PRIVACY IMPACT ASSESSMENT (PIA)

For the

DAU STUDENT INFORMATION SYSTEM
Defense Acquisition University

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	12971
☐	**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 Pending

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 pending

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. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; DoD Directive 5000.57, Defense Acquisition University.

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.

To manage administrative and academic functions related to student registration, courses attempted, and completed. Records are also used to verify attendance and grades; and as a management tool for statistical analysis, tracking, and reporting.

Categories of records in the system:
Name; DAU ID Number; date of birth; citizenship; home address; personal home telephone number, personal cell telephone number; personal email address; ; education information (college transcripts); employment information (job series; rank; pay grade; service; user type (i.e., DoD, military, civilian, etc.), business address, business telephone number, business email address, supervisor's name; supervisor's telephone number; supervisor's email address); emergency contact; Temporary Duty (TDY) address; TDY telephone number; registration information (i.e., registered, waitlisted, graduated, etc.); course information (i. e., course name, class or section number, dates, etc.); instructor information; DAU grades; and special accommodation (yes/no only).

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

The primary risk is that should the system be compromised there would be disclosure of PII to an unauthorized source. DAU has addressed this risk in two ways, 1) By limiting the number and type of required PII within the system, particularly the absence of social security numbers. 2) The system is being safeguarded with the physical, technical and administrative controls addressed in part 3 of the PIA Questionnaire and via the DIACAP certification and accreditation of the system.

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. ATLAS (DAU Learning Management System), DAU Data Warehouse, FAI Data Mart, AT&L Data Mart (Note: not all PII is shared with each of the listed systems. Only limited data elements are shared)

☒ **Other DoD Components.**

Specify. Career Acquisition Personnel & Position Management Information System (CAPPMIS - Army system), Defense Civilian Personnel Data System (DCPDS), Acquisition Career Management System (ACMS - Air force system), Management Information System (MIS II - Navy system), Army Training Requirements and Resources System (ATRRS - Army system), Defense Manpower Data Center (DMDC), Defense Travel System (DTS)

☐ **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.

For those students considered the public, federal contractors, foreign nationals and industry members, they can object to the collection of PII by not creating an account in the SIS. If they desire to take a DAU course, they must provide the minimum fields necessary to create an account in the SIS.

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

Members of the DoD acquisition workforce, who are required by law to take DAU courses, do not have an opportunity to object to the collection of their PII in the student information system. Their data will be fed over by their component (Army, Navy, Air Force or other DoD agencies). PII is required for reporting on Defense Acquisition Workforce Improvement Act (DAWIA) training to Department of Defense (DoD).

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 resident in the SIS is used to provide training management services for the individual and components DoD wide. If an acquisition workforce member were given the opportunity to exclude their PII, it would prevent them from meeting the qualifications for their position. This would also prevent DAU from reporting to Congress regarding Defense Acquisition Workforce (DAWIA) training data.

For those students considered the public, federal contractors, foreign nationals and industry members, by creating an account in the SIS and registering for a course, they are consenting to the use by DAU, of their information for reporting and course management purposes.

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.

PRIVACY ACT STATEMENT
Authorities: 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; and DoD Directive 5000.57, Defense Acquisition University.

Purpose: To manage administrative and academic functions related to student registration and courses attempted and completed. Records are also used to verify attendance and grades, and as a management tool for statistical analysis, tracking, and reporting. These records are covered by Privacy Act System of Records Notice DAU 08 [WILL NEED TO ADD LINK TO THE SORN].

Routine Use(s): 1. Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

2. Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

3. Disclosures Required by International Agreements Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

4. Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

5. Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

6. Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

The DoD Blanket Routine Uses are set forth at http://dpclo.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

Disclosure: Voluntary. However, if you do not provide the information required to identify and register you for courses, your application for attendance at DAU may be rejected or you may not receive credit for a course you attended.

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.