DEPARTMENT OF DEFENSE
Office of the Secretary of Defense
Narrative Statement on a New System of Records
Under the Privacy Act of 1974

1. System identifier and name: DAU 08, entitled "Defense Acquisition University Student Information System (SIS)".

2. Responsible officials: Ms. Brenda Sedlacek, Program Manager Defense Acquisition University (DAU) Student Information System, 9820 Belvoir Road, Fort Belvoir, VA 20602, telephone (703)805-4970.

3. Purpose of establishing the system: The Office of the Secretary of Defense proposes to establish a new System of Records to support the Defense Acquisition University Student Information System which will 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.

4. Authority for the maintenance of the system: 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; and DoD Directive 5000.57, Defense Acquisition University.

5. Provide the agency's evaluation on the probable or potential effects on the privacy of individuals: In developing this system of records notice, the Defense Acquisition University program manager carefully reviewed the safeguards established for the system to ensure they are compliant with DoD requirements and are appropriate to the sensitivity of the information stored within this system. Any specific routine uses have been established to ensure the minimum amount of personally identifiable information is provided. The DAU recognizes the sensitive nature of the information collected and stored within this System of Records and has considered this in developing the system and implemented ways to minimize any potential effects to the individuals on whom records might be retained.

6. Is the system, in whole or in part, being maintained, collected, used or disseminated by a contractor? Yes.

7. Steps taken to minimize risk of unauthorized access: Physical controls include: security guards, identification badges, and key cards. Building is located on a federal installation with around-the-clock gate guards. Building is locked during non-business hours. Only individuals with the need to know are authorized access to files. Personally Identifiable Information (PII) fields are not exposed to users who have not been properly cleared and trained. Reports containing PII may only be created by those with specific role based access. Any reports generated with PII are appropriately marked per regulations. System is contained in a DAU enclave with boundary defense mechanisms in place.

Technical controls include: user identification, passwords, intrusion detection system (IDS), data is encrypted at rest and in transit, firewalls, virtual private network (VPN), access to records requires the use of DoD Public Key Infrastructure Certificates or Common Access Card (CAC) and Personnel Identification Number (PIN).

Administrative controls include: periodic security audits, regular monitoring of users' security practices, methods to ensure only authorized personnel access to PII, encryption of backups containing sensitive data.

8. Routine use compatibility: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

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.

9. OMB information collection requirements:
OMB collection required: Yes
OMB Control Number: pending
Title of collection if other than #10:
Date Approved or Submitted:
Expiration Date:

If No, then state reason:

10. Name of IT system (state NONE if paper records only): DAU Student Identification System (DITPR 12971).

DAU 08

System name:
Defense Acquisition University Student Information System (SIS).

System location:
Defense Acquisition University (DAU), 9820 Belvoir Road, Fort Belvoir, VA 22060-5565.

Categories of individuals covered by the system:
All current and former students of the DAU to include contractors and foreign nationals.

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).

Authority for maintenance of the system:
10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology, and Logistics; and DoD Directive 5000.57, Defense Acquisition University.

Purpose(s):
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.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

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.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Electronic storage media.

Retrievability:
Individual's name, DAU ID number, date of birth, course name, and class or section number.

Safeguards:
Physical controls include: security guards, identification badges, and key cards. Building is located on a federal installation with around-the-clock gate guards. Building is locked during non-business hours. Only individuals with the need to know are authorized access to files. Personally Identifiable Information (PII) fields are not exposed to users who have not been properly cleared and trained. Reports containing PII may only be created by those with specific role based access. Any reports generated with PII are appropriately marked per regulations. System is contained in a DAU enclave with boundary defense mechanisms in place.

Technical controls include: user identification, passwords, intrusion detection system (IDS), data is encrypted at rest and in transit, firewalls, virtual private network (VPN), access to records requires the use of DoD Public Key Infrastructure Certificates or Common Access Card (CAC) and Personnel Identification Number (PIN).

Administrative controls include: periodic security audits, regular monitoring of users' security practices, methods to ensure only authorized personnel access to PII, encryption of backups containing sensitive data.

Retention and disposal: Records are destroyed when 50 years old.

System manager's address:
Center Director, Defense Acquisition University, Scheduling and Student Support, Performance and Resource Management, 9820 Belvoir Road, Fort Belvoir, VA 22060-5565.

Notification procedure:
Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Center Director, Defense Acquisition University, Performance and Resource Management, 9820 Belvoir Road, Fort Belvoir, VA 22060-5565.

Signed, written requests should contain full name, DAU ID number, date of birth, current address, and telephone number

Record access procedures:
Individuals seeking access to information about themselves contained in this system, should address written inquiries to the Office of the Secretary of Defense/Joint Staff Freedom of Information Act Requester Service Center, 1155 Defense Pentagon, Washington DC 20301-1155.

Signed, written requests must contain full name, DAU ID number, date of birth, current address, telephone number, and the name and number of this system of records notice.

Contesting record procedures:
The OSD rules for accessing records, for contesting contents, and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager.

Record source categories:
The individual, the DAU Data Center, 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 acquisition career management system), and Defense Manpower Data Center (DMDC).

Exemptions claimed for the system:
None.