

DEPARTMENT OF DEFENSE

BILLING CODE: 5001-06

Office of the Secretary

Docket ID:

Privacy Act of 1974; System of Records

AGENCY: Defense Acquisition University, DoD.

ACTION: Notice of a Modified System of Records.

SUMMARY: The Office of the Secretary of Defense proposes to modify a system of records entitled “Defense Acquisition University Student Files, “DSMC 02”. DSMC 02 is consolidating its current system of records DAU 07, “Acquisition Community Connection (ACC)”, DAU 08, “Student Information System (SIS)” and DSMC 02 in to one system of records DAU 02, “Data Services Management (DSM)” and SORN ID. This is being done to reduce the number of individual SORNs, bring the SORN up to date with the new learning management system and cancel SORNs that are associated with legacy systems that are no longer being used.

DATES: Comments will be accepted on or before 27 Apr 2020. This proposed action will be effective the date following the end of the comment period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <http://www.regulations.gov>.

Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mrs. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPDD), 1155 Defense Pentagon, Washington, D.C. 20311-1155, or by phone at (571) 372-0478.

SUPPLEMENTARY INFORMATION:

DAU is responsible for providing a global learning environment to develop qualified acquisition, requirements and contingency professionals who deliver and sustain effective and affordable warfighting capabilities per Congressional Mandate (NDAA FY2007, Section 801). By not consolidating and updating DAU 02 DSM, DAU cannot collect essential information on our student population that is used to ensure workforce training and certification. DAU will also be

unable to provide the necessary information to the Services and 4th Estate Director, Acquisition Career Management (DACM) offices.

The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974, as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at <http://dpcl.d.defense.gov/privacy>.

Dated:

Aaron Siegel

OSD Federal Register Liaison Officer, Department of Defense

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

1. System and number: Defense Acquisition University Student Files, DSMC 02.
2. Nature of proposed modifications for the system: The DSM supports institutional acquisition training missions for the Department of Defense, in accordance with 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Sustainment; and DoD Directive 5000.57, Defense Acquisition University. The DSM provides administrative and academic capabilities and functions related to student registrations, account requests, courses attempted, and completed, and graduation notifications to DoD training systems. The DSM includes multiple environments associated with the Defense Acquisition University (DAU) Learning Management Systems (LMSs). Respondents are university applicants and instructors who willingly provide personal information to take courses administered by the DAU or access DAU training, knowledge sharing and collaboration systems. This alteration is combining three systems of records notices, DSMC 02, Defense Acquisition Student Files, DAU 07, Acquisition Community Connection (ACC) Member Records, and DAU 08, Defense Acquisition University Student Information System (SIS).
3. Authority for the maintenance of the system: 10 U.S.C. 133, Under Secretary of Defense for Acquisition and Sustainment; DoD Instruction 5000.57, Defense Acquisition University (DAU); and E.O. 9397 (SSN), as amended.
4. Provide the agency's evaluation on the probably or potential effects on the privacy of individuals: The potential impacts on the privacy of individuals is minimal because the information collected is essential to providing the individual students credit for course completions and annotating of their professional records for DAWIA Certification.
5. Routine use compatibility: The routine uses are consistent with the purpose for which the information is collected and have been determined to be necessary and proper.

Routine use (a) is compatible with the purpose of the collection because it allows for DoD DAU to share student's information with other Federal, DoD and Industry partners.

Routine uses (b) through (h) are standard routine uses commonly listed in DoD and other Federal agency System of Records Notices.

Routine uses (g) and (h) are in response to the Office of Management and Budget (OMB) requirement in OMB M-17-12 to respond appropriately to a breach of personally identifiable information in this system of records or, as appropriate, to assist another Federal agency or entity in its response to a breach.

- (a.) To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.
- (b.) To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.
- (c.) To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
- (d.) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- (e.) To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
- (f.) To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- (g.) To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- (h.) To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

6. OMB information collection requirements:

OMB collection required: Yes.

OMB Control Number: 0704-AAKD.

Title of collection if other than #10: N/A
Date Approved or Submitted: 27 Mar 2020
Expiration Date: 30 Apr 2023

Provide titles of any information collection requests (e.g., forms and number, surveys, interviews scripts, etc.) contained in the system of records.

7. Name of IT system (state NONE if paper records only): DAU Data Service Management, DITPR #19833.

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

SYSTEM NAME AND NUMBER: Defense Acquisition University Data Services Management (DSM), DAU 02.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Office of the Registrar, Defense Acquisition University, 9820 Belvoir Road, Fort Belvoir, VA 22060-5565.

SYSTEM MANAGER(S): Data Integration Manager, Defense Acquisition University, 9820 Belvoir Road, Building 231, Fort Belvoir, VA 22060-5565. Contact email: Chris.Johnson@dau.edu.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 133, Under Secretary of Defense for Acquisition, Technology and Logistics; DoD Instruction 5000.57, Defense Acquisition University (DAU); and E.O. 9397 (SSN), as amended.

PURPOSE(S): To manage administrative and academic functions related to students; enables students to interact; share resources, ideas and experiences to support job performance, and avoid duplication of professional effort; and to issue student identification and create single sign-on accounts. To provide a professional forum for the defense acquisition workforce to connect with others in their field on acquisition-related topics, and form professional networks. These social interactions allow for the sharing of resources, ideas, and experiences to enhance job performance; promote social learning and foster a culture that continuously learns, shares learning, and acts upon that learning. Records are also used as a management tool for statistical analysis, tracking, and reporting.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: All current, former, and nominated students of the Defense Acquisition University (DAU). DoD Acquisition Workforce which includes Active Duty Military, Reservists, National Guardsman, and DoD civilians. Students may also include other Federal Agency Acquisition employees, international military and civilian fellows, members of supporting defense industries, and program office sponsored contractor employees applying for or attending Defense Acquisition University courses.

CATEGORIES OF RECORDS IN THE SYSTEM: Name, Social Security Number (SSN), DoD ID Number, DAU student ID, date of birth, current address, work or personal email address, temporary duty address and telephone number, disability (yes/no only), citizenship type, designation (Military, civilian, or contractor), organization, employment information (job series; rank; pay grade; service); supervisor information (name, work email, code and phone number), security clearance, course information (i.e., course name, class or section number, dates); college transcripts, correspondence, DAU grades, instructor and advisor evaluations, education reports, official orders, individual's photograph, about me (interests, hobbies, skills and job related experience), and emergency point of contact name and phone number, acquisition discipline and specialty area (auditing, business, contracting, engineering, facilities engineering, industrial/contract property management, information technology, life cycle logistics, program management, purchasing, production/quality/manufacturing, science/technology manager,

test/evaluation), Office of Government Ethics (OGE) Form 50 filer (yes/no), student record (active or inactive).

RECORD SOURCE CATEGORIES: Individual, supervisors, employers, instructors, advisors, examinations, official military records, and the Army Training Requirements and Resources System (ATRRS).

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:

- a. To support Acquisition Workforce Certifications and graduation, data will be shared with the Services and Corporate Partners of DoD sponsored students.
- b. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.
- c. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.
- d. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
- e. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- f. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
- g. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- h. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD

(including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

i. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Paper and electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Name, SSN, DAU ID number, DoD ID (EDIPI) or email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Student registration records are destroyed 50 years after graduation, transfer, withdrawal, or death (GTWD) of student. All other records are destroyed 5 years after GTWD of student.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records are housed in the data center, which is an electronically controlled entry 24/7 and accessed only by authorized personnel having an official need-to-know. DoD mandated intrusion detection and monitoring systems in place, providing 24/7 protection. Secure Socket Layers are used for transactions to and from the system. Internally, Defense Acquisition University employs a two-factor authentication, Common Access Card login, role-based profiles and access is granted on a need-to-know basis. Data at rest is protected through access controls including role-based permissions based on need-to-know. Annual Cyber Awareness Challenge training and completion of Privacy Act training is required annually. Records are maintained in locked cabinets, in an area accessible only to authorized personnel. Building is locked during non-business hours. Only individuals designated as having a need for access to files by the system manager are authorized access to information. The site is FedRAMP certified and is compliance with DoD Risk Management Framework (RMF).

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 for information should contain the name and number of this system of records notice, your full name, SSN, current address and telephone number, course attended, class to which assigned, and include the number and name of this system of records notice.

In addition, the requester must provide a notarized statement or an unsworn declaration made in

accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)”.

CONTESTING RECORD PROCEDURES: The Office of the Secretary of Defense (OSD) rules for accessing records, for contesting contents, and for appealing initial agency determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Help Desk, Defense Acquisition University, 9820 Belvoir Road, Building 231, Fort Belvoir, VA 22060-5565.

Signed, written requests for information should contain full name, SSN, current address and telephone number, course attended and class to which assigned.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)”.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: March 27, 2003, 68 FR 14950.