

SYSTEM NAME AND NUMBER: Defense Institute of Security Assistance Management (DISAM) Information System Mission (DISM), DSCA 05. (November 21, 2019; 84 FR 64281)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Defense Institute of Security Cooperation Studies (DISCS), 2475 K. Street, Bldg. 52, Wright-Patterson AFB, OH 45433-7641.

SYSTEM MANAGER(S): DISM System Administrator; Defense Institute of Security Cooperation Studies, 2475 K. Street, Bldg. 52, Wright-Patterson AFB, OH 45433-7641; email: dsca.ncr.lmo.mbx.info@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 134, Under Secretary of Defense for Policy; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; DoD Directive (DoDD) 5105.65, Defense Security Cooperation Agency (DSCA); DSCA Security Assistance Management Manual, Chapter 10, International Training; DoDD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, SECNAVINST 4950.4B, AFI 16-105, Joint Security Cooperation Education and Training; and E.O. 9397, (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: The DISCS DISM contains several applications to efficiently manage the administrative activities of U.S. and international students, DISCS personnel and guest lecturers. Also, the system allows personnel to submit requests and make arrangements for travel. Finally, the system uses a relational database to record, manage and report information about students, personnel, and travel, including reports of annual training. Records are also used as a management tool for statistical analysis, tracking, reporting to Congress, evaluating program effectiveness, and conducting research.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DISCS civilian, military, and contractor personnel, U.S. Federal agency employees, students, and guest speakers.

CATEGORIES OF RECORDS IN THE SYSTEM: DISCS Personnel data: Full name, DoD Identification Number (DoD ID), gender, date of birth, home address, personal cell phone and work numbers, work domain name, work email address, arrival and departure dates, duty hours, emergency point of contact information, position title, funding source, directorate and office names, employment status, academic rank and degree, salary, job series, civilian grade, military Joint Manpower Program rank and number, date of rank, service branch, occupational specialty code and description, military evaluation dates, tour completion date, recall order, DoD billet manning document number, height and weight, security clearance type, issue and expiration dates, investigation type and date, IT level, supervisor name, list of DoD annual training requirements, training completion dates and year required, faculty member, function and program type;

DISCS Personnel Travel data: Traveler's name, government point of contact information, request number, agency directorate, priority and requirement types, purpose of travel, group and class type, order and voucher numbers, voucher check and Military Interdepartmental Purchase Request (MIPR) dates, funding source, source organization, departure and arrival information,

travel location cost information, DoD status of travel request, administrative notes and comments.

Student data: Full name, student and DoD ID, gender, date of birth, nationality, organization and mailing addresses, work number, position title, hotel confirmation number, country name, combatant command, student type, area of expertise and duty type, civilian grade, service branch, military rank, diploma, test scores, supervisor name, personal and work email addresses, and work number, course type, registration date, level and status, certificates, student and registrar comments, administrative notes and emergency point of contact information.

Guest Speaker data: Full name, position title, gender, Social Security Number (SSN) (for non-DoD guest speakers only), DoD ID, home, cell phone, and work numbers, fax number, email and mailing address, employment status, security clearance type, military rank, civilian grade, course information, honorarium, DISCS host name, and funding information.

RECORD SOURCE CATEGORIES: Information contained in this system is obtained from the DISCS personnel, individuals via DISCS student registration and guest speaker forms, and travel request forms, including by administrators with access to DoD personnel and security related databases.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND 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):

- a. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the DoD 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 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 confirms a breach of the system of records; (2) the DoD determines 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 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: The records are stored in electronic format on secure servers with access restricted by the use of Common Access Cards (CACs), pin numbers, and/or card swipe protocols. Physical access is limited through the use of locks, guards, card swipe, and other administrative procedures.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: These records may be retrieved by name of individual, DoD ID, student ID, or SSN.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: These records are cut off on closure of study or event and destroyed 25 years after cut off.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, and is accessible only to authorized personnel. Access to records is also limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to electronic data is restricted by centralized access control to include the use of CAC, pin numbers (which are changed periodically), file permissions, and audit logs.

RECORD ACCESS PROCEDURES: Individuals seeking access to records 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 should include the full name, current address and telephone number, and the name and number of this system of records notice. In addition, the requester must provide either 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 DoD rule for accessing records, contesting contents, and appealing initial agency determinations are published 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 of records should address written inquiries to Defense Institute of Security Cooperation Studies, ATTN: Director of Organizational Support, 2475 K Street, Wright-Patterson AFB, OH 45433-7641. Signed, written requests should include the full name, current address and telephone number, and the name and number of this system of records notice. In addition, the requester must provide either 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: June 7, 2016, 81 FR 36526.