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: DSCA nn2, entitled "Defense Institute of Security Assistance Management (DISAM) Information System Mission (DISM)"

2. Responsible official: Donald J. McCormick, Director of Academic Support, Defense Institute of Security Management, 2475 K Street, Wright-Patterson AFB, Ohio 45433, telephone (937) 713-3340.

3. Purpose of establishing the system: The DISAM Information Mission System is a web based portal designed to hold several applications for the purposes of efficient administration of U.S. and internal students, and the effective management of DISAM personnel and guest lecturers. The portal also provides DISAM personnel the ability to submit travel requests and travel arrangements. Finally, the web based portal uses a relational database to record, manage and report information about students, personnel, and travel, including reports of annual training for foreign nationals. Records are also used as a management tool for statistical analysis, tracking, reporting to Congress, evaluating program effectiveness, and conducting research.

4. Authority for the *maintenance (maintained, collected, used, or disseminated) of the system: 10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA); DoD Directive 5105.38-M, Security Assistance Management Manual, Chapter 10; DoD Directive 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 ; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; E. O. 9397, SSN, as amended.

5. Provide the agency's evaluation on the probable or potential effect on the privacy of individuals: In reviewing this SORN, the Defense Security Cooperation Agency 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 DSCA 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, (maintained, collected, used or disseminated) by a contractor? Yes.

7. Steps taken to minimize risk of unauthorized access: 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 Common Access Cards (CACs), passwords (which are changed periodically), file permissions, and audit logs.

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

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.

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.

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.

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.

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.

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 set forth at the beginning of the Office of the Secretary of Defense/ Joint Staff (OSD/JS) Privacy Office’s compilation of systems of records notices may apply to this system. The complete list of DoD blanket routine uses can be found online at:

http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

9. OMB public information collection requirements:
    OMB collection required: YES

OMB Control Number (if approved): Pending
Expiration Date (if approved) or Data Submitted to OMB:

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

1) DISM Collection comprising of:
2) DISAM Form GSI-001
3) Student Registration Form

If collecting on members of the public and no OMB approval is required, state the applicable exception(s): N/A

10. Name of IT system (state NONE if paper records only):
DISAM Information System Mission (DISM)

DSCA nn2

System name:
Defense Institute of Security Assistance Management Information System Mission (DISM)

System location:
Defense Institute of Security Assistance Management (DISAM), 2475 K. Street, Bldg 52, Wright-Patterson AFB, OH 45433-7641.

Categories of individuals covered by the system:
DoD civilian, military, and contractor personnel, U.S. Federal agency employees, Foreign Service nationals and industry students, and guest speakers.

Categories of records in the system:
DISAM Personnel data: Full name, DoD ID number, gender, date of birth, home address, personal cell phone and work numbers, domain name, email address, arrival and departure dates, duty hours, emergency name and 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, arrival date, 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.

DISAM Personnel Travel data: Traveler’s name, government point of contact information, request number, 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 Identification Number (DoD ID Number), 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, email address, 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), DoD Identification Number (DoD ID Number), home, cell phone, and work numbers, fax number, email and mailing address, employment status, security clearance type, military rank, civilian grade, course information, honorarium, DISAM host name, and funding information.

Authority for maintenance of the system:
10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA); DoD Directive 5105.38-M, Security Assistance Management Manual, Chapter 10; DoD Directive 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 ; Public Law 97-195, Foreign Assistance and Arms Export Act of 1961, as amended; E. O. 9397, SSN, as amended.

Purpose(s):
The DISAM Information Mission System is a web based portal designed to hold several applications for the purposes of efficient administration of U.S. and internal students, and the effective management of DISAM personnel and guest lecturers. The portal also provides DISAM personnel the ability to submit travel requests and travel arrangements. Finally, the web based portal uses a relational database to record, manage and report information about students, personnel, and travel, including reports of annual training for foreign nationals. Records are also used as a management tool for statistical analysis, tracking, reporting to Congress, evaluating program effectiveness, and conducting research.

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

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

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.

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.

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.

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.

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.

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 set forth at the beginning of the Office of the Secretary of Defense/ Joint Staff (OSD/JS) Privacy Office's compilation of systems of records notices may apply to this system. The complete list of DoD blanket routine uses can be found online at:

http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

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

Storage:
Paper and electronic storage media.

Retrievability:
By name of individual, DoD ID number, student ID, or SSN.

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 Common Access Cards (CACs), passwords (which are changed periodically), file permissions, and audit logs.

Retention and disposal:
Records are cut off annually, destroy when 25 years old.

System manager(s) and address:
DISM System Administrator; Defense Institute of Security Assistance Management, 2475 K. Street, Bldg. 52, Wright-Patterson AFB, OH 45433-7641.

Notification procedure:
Individuals seeking to determine whether information about themselves is contained in this system of records should address

written inquiries to Defense Institute of Security Assistance Management, ATTN: Director of Academic Support, 2475 K Street, Wright-Patterson AFB, OH 45433-7641.

Signed, written requests should include the full name, SSN (last four digits) or DoD ID number, current address and telephone number, and the number of this system of records notice.

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 Services, 1155 Defense Pentagon, Washington DC 20301-1155.

Signed, written requests should include the full name, SSN (last four digits) or DoD ID number, current address and telephone number, and the number of the 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:
From the individual

Exemptions claimed for the system:
None