DISM

SUPPORTING STATEMENT – PART A

A. JUSTIFICATION

1. Need for the Information Collection

The Defense Institute of Security Assistance Management (DISAM) Information Technology Mission System (DISM): Is a web based portal designed to hold several web applications for the purposes of efficient administration of U.S. and international students, and the effective management of DISAM personnel and guest lecturers. The portal provides DISAM personnel the ability to submit travel request and travel arrangements. Finally, the web based portal uses a relational database to record, manage and report information about students, personnel, and travel.

Legal or administrative requirements that mandate the collection of data are;

22 U.S. CODE § 2394 (Foreign Assistance Act (FAA)) and 22 U.S. CODE § 2770A (Arms Export Control Act (AECA)) the Joint Security Cooperation Education and Training Regulation, 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347; 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, DSCA Manual, Chapter 10; DoD Directive 5101.1, DoD Executive Agent; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; DoD Directive 5105.38-M, DSCA Manual; Joint Security Cooperation Education and Training (JSCET) regulation, (AR12-1, SECNAVINST 4950.4B, AFI 16-105); Foreign Assistance and Arms Export Act §548; Executive Order 9397, as amended by Executive Order 13478.

2. Use of the Information

The information collected in DISM is used by DISAM to provide an efficient management of DISAM resources in support of U.S. and international students that attend DISAM courses on-site or overseas. The information is used to manage personnel actions to include the validation and reconciliation of travel orders, time off, course instruction schedules, recall roster, academic rank & degree and emergency POCs. The management of student/participant activities including all events and courses attended at DISAM or at DISAM offsite courses both CONUS and OCONUS, we can provide the students with their academic achievement at DISAM along with a record of completion. Further the student information is used to verify the qualifications of individuals in the Security Cooperation workforce database on the SAN. The site maintains all the forms that are used within the DISAM organization such as Credit Hours, Out-processing Checklist and GPC Request forms. Finally the DISM portal provides both personnel and class scheduling throughout the Fiscal/Calendar Year. To sum up the DISM portal is a collaborative work tool for all of DISAM.

3. Use of Information Technology

Potential students input their information through the DISAM registration form or manually send the registration forms to the registrar's office at disam_registrars@us.af.mil. Once the student's information is uploaded into the DISM database and approved the student is assigned to the class. Faculty submit travel request on DISM which provides for future planning of the courses and budgetary management within DISAM. Visiting guest speaker information is loaded into the database by the administrators for tax purposes and as part of the course management. The DISM portal provides an overview of the courses and compiles reports on DISAM resources for management of the programs.

4. Non-duplication

There are no duplicates to the DISM Forms.

5. Burden on Small Business

This is not applicable for this information collection.

6. Less Frequent Collection

The collection information is voluntary; however failure to provide the information could result in the individual not being accepted into a DISAM course.

7. Paperwork Reduction Act Guidelines

No special circumstances exist that would not adhere to the guidelines in 5 CFR 1320.5(b)(2).

8. Consultation and Public Comments

60-day Federal Register Notice was published on 27 February 2015 (80 FR 10073). Public comments ended on 04/27/2015 with no comments received.

30-Day Federal Register Notice was published on 4 September 2015 (80 FR 53504).

9. Gifts or Payment

This is not applicable for this information collection.

10. Confidentiality

Confidentiality ensures that only those personnel with the appropriate security clearance and the need-to-know shall be allowed access to data processed, handled or stored on

system components. Confidentiality targets the protection of information from unauthorized access. Personnel, physical and administrative security mechanisms applied to the system shall minimize risks of unauthorized disclosure of command and control information.

DISM policy references are:

- DoDD 5205.02E, DoD Operations Security (OPSEC) Program, 20 June 2012.
- DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007
- DoDI 8500.01, Cybersecurity, 14 March 2014
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014

The DISM System Security Policy implements Department of Defense (DoD) security publications. This security policy applies to all personnel involved with the development, maintenance and operation of an automated information system Users shall ensure sensitive-but-unclassified materials, which require special marking and handling such as For Official Use Only (FOUO), mandated by the Freedom of Information Act (FOIA) or Privacy Act (PA), are marked in accordance with DoDM 5200.01-V4, DoD Information Security Program: Controlled Unclassified Information (CUI).

DoDI 8500.01, enclosure 3, paragraph 8 states that access to all DoD information systems (i.e., workstations, computers, servers, etc.) ensure strong identification and authentication so that entities' access and access behavior are visible, traceable, and enable continuous monitoring for law enforcement and cybersecurity. DODI 8500.01 paragraph 3i(1) also states the cybersecurity workforce functions must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened in accordance with this instruction and adherence to DoD 5200.2-R, paragraph 3.6.15 and Federal Information Processing Standards (FIPS) Publication 201-1 which further implements Homeland Security Presidential Directive (HSPD) 12 for specific clearance/investigation requirements. The minimum investigation required for DISM access is a National Agency Check with Inquiries (NACI) or host nation equivalent of a NACI.

DoDI 8500.01, enclosure 3, paragraph 11c(2) states that access must be strictly limited to information that has been cleared for release. DISM data is considered For Official Use Only (FOUO). DISM implements role-based security controls for user access deemed necessary to meet their mission. Interface partners require approved written requirements for specified data only.

DoDI 8500.01, enclosure 3, paragraph 10 requires all users of DoD information systems must be adequately trained to perform their information assurance responsibilities. Information Assurance Training shall be accomplished and documented for all personnel prior to their obtaining system access. Training will consist of the applicable requirements contained as stated above and local security procedures. DoDD 8570.01-M, Information Assurance Training,

Certification, and Workforce Management, shall be met by all DISM users with privileged access.

DoDI 8500.1, enclosure 3, paragraph 7e, requires data must be protected in accordance with DoDI 8582.01 when processed or stored. Users are responsible for protecting and safeguarding all sensitive information under their control. Sensitive information includes, but is not limited to, privacy act data, privileged data, proprietary data, logistics records, procurement data, financial data, investigative data, auditor records, For Official Use Only data, scientific and technical data (which has national security related implications), unit mobility or deployment information. The computing facility where data is stored enforces restrictive access features. The DISAM facility located on Wright-Patterson AFB, OH does not require privileged keycard entry. Access to facilities require authentication of identification documents for review by security officers for entry.

Users are responsible for protecting and safeguarding all sensitive information under their control. Sensitive information includes, but is not limited to, privacy act data, privileged data, proprietary data, logistics records, procurement data, financial data, investigative data, auditor records, For Official Use Only data, scientific and technical data (which has national security related implications), unit mobility or deployment information, and classified information. Also, the aggregation of unclassified information may result in the creation of sensitive data. Use the following guidelines on how to protect sensitive information.

- Do remove compact disc containing sensitive information from your computer and properly store them when they are no longer being used.
- Do store compact disc containing sensitive-but-unclassified information in locked offices or in a locked storage container during non-duty hours.
- Do properly safeguard, store and dispose of sensitive information.
- Do ensure all classified papers contain the date of creation, the highest classification level of the data contained in the document, the downgrading instructions or review date, and the name of the originator.
- Do when possible; use internal markings on files to indicate the type of sensitive data contained in the file and any special handling instructions.
- Do dispose of computer products containing sensitive-but-unclassified information in accordance with the records disposition schedule.
- Do not place sensitive-but-unclassified data on diskettes used for general correspondence.
- Do not provide sensitive information to an individual until you have determined he or she has a valid need-to-know requirement for the information as part of their official duties.

Information Assurance Training shall be accomplished and documented for all personnel prior to their obtaining system access. Training will consist of the applicable requirements contained in DoDD 8570.01, this policy and local security procedures.

The DISM Privacy Impact Assessment dated 30 April 2015 is included as a supplementary document.

In accordance with DoDD 5400.11 there is no violation of the DoD Privacy Program.

Delete when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.

11. Sensitive Questions

The justification for use of the social security number (SSN) is dated 26 March 2015. Guest speakers need to provide their full name, SSN, honorarium, course information and their position in order to receive funding for their services as speaker/ instructor.

The minimum data needed for the student to register is their full name, email, student type (includes service branch and grade/rank), DoD Identification Number (DoD ID Number) and Information Assurance (IA) Cyber Awareness training completion date. Students are allowed to input information related to any special needs or requirements (i.e., food, disability, etc.). This is done to assist the registrar office in advising the student where they can find food per their religious dietary requirements, places of worship or to make special arrangements the student may require during their training.

For DISAM personnel the information collected; such as full name, DoD ID number, gender, date of birth, home address, personal cell phone and work numbers, duty hours, emergency name contact, funding source, directorate and office names, employment status, academic rank and degree, salary, job series, civilian grade, military; is used for human resources, TDY and emergency contact purposes.

5 U.S.C. § 552a(b)(3) (routine uses) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D).

12. Respondent Burden, and its Labor Costs

a. Estimation of Respondent Burden.

DISAM STUDENT REGISTRATION FORM:

ANNUAL BURDEN HOURS: 2388 hours

NUMBER OF RESPONDENTS: 4775

RESPONSES PER RESPONDENT: 2

ANNUAL RESPONSES: 9551

AVERAGE BURDEN PER RESPONSE: 15 minutes

DISAM GUEST SPEAKER FORM: (Still in development)

ANNUAL BURDEN HOURS: 62.25

NUMBER OF RESPONDENTS: 249

RESPONSES PER RESPONDENT: 1

ANNUAL RESPONSES: 249

AVERAGE BURDEN PER RESPONSE: 15 min

ANNUAL TOTALS:

ANNUAL BURDEN HOURS: 2450 hours

b. Labor Cost of Respondent Burden

Estimated hourly rate: 21.02
Rate Per Response: 5.255
Total Labor Cost: $51,499

13. Respondent Costs Other Than Burden Hour Costs

$0

14. Cost to the Federal Government

Although DISM funding for individuals is provided through the Foreign Military Sales Program, Software development costs incurred for the collection of the data is $201K. Annual operations and maintenance costs are $10K

Estimated hourly rate: 14.17
Average burden per response: 15 mins
Total Cost to Gov't: 106,808

TOTAL ANNUAL COST TO GOVT: $116,808

15. Reasons for Change in Burden

This is an existing collection in use without an OMB Control Number. Therefore, burden increase for this collection is due to the enforcement of compliance with the Paperwork Reduction Act.

16. Publication of Results

This is not applicable for this information collection.

17. Non-Display of OMB Expiration Date

This is not applicable for this information collection.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

This is not applicable for this information collection.