Security Assistance Network (SAN)

SUPPORTING STATEMENT – PART A

A. JUSTIFICATION

1. Need for the Information Collection

The Security Cooperation Training Management System portion of the Security Assistance Network (SAN) collects International Student Information (IMSI) that is used by the Defense Security Cooperation Agency (DSCA), military departments and others within the security cooperation community. This data is collected on non U.S. citizens that have been selected by their government to attend various training through the Department of Defense (DoD) schools and DoD-contracted facilities. The IMSI is also used by the receiving organization to provide background information on the student assisting in the student's arrival and stay in the United States. The SAN also includes the Security Cooperation Workforce Database (SCWD) and International Affairs Certification Database (IACD) which tracks and provides the status of training for the Security Cooperation workforce certification levels.

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

10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA); DSCA Security Assistance Management Manual, Chapter 10, International Training; DoD Directive 5101.1, DoD Executive Agent; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Joint Security Cooperation Education and Training (JSCET) regulation, (AR12-1, SECNAVINST 4950.4B, AFI 16-105); Foreign Assistance and Arms Export Act § 548.

Use of the Information

The IMSI that is collected on the SAN is used by the International Military Student Officer (IMSO) assigned to each training installation to prepare for the arrival and stay in the United States of the international training student. The collection of this information, in addition to the above, is for the issuance of invitational travel orders, student screening purposes, and to determine the student's likes and dislikes; his/her recreation activities; dietary restrictions; etc. Using the Web-based Training Management System (TMS), the Security Assistance Organization (Office or Officer) enters the IMSI data via an automated copy of the DD Form 2339. Users may access the system via username and password or if they are active DoD (civilian, military or contractor) members through CAC and pin. Data may also be collected from automated uploads from the RCPAMS and DSAMS DoD systems.

3. Use of Information Technology

Once information is input through the DoD 2339 the IMSI data is then uploaded to the SAN and distributed to training activities via interfacing with MILDEP and other DSCA systems for processing. Ninety-eight percent of the data within the SAN is collected electronically.

4. Non-duplication

There are no duplicates to the DD Form 2339, *International Military Student Information or any other collection forms or tools that are used by other agencies*.

5. Burden on Small Business

Not applicable.

6. Less Frequent Collection

The collection of this information at its current rate of frequency is necessary so that the IMSO knows any specified general requirements of the international student before their arrival resulting in less of a workload for the IMSO and efficiency of processing the student.

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 6 March 2015 (80 FR 16364). Public comment to end on 26 March 2015 with no public comments received. No outside experts were consulted by the Defense Institute of Security Cooperation (DISAM) through these processes.

A 30-day Federal Register Notice was published on 29 March 2016 (81 FR 17449).

9. Gifts or Payment

Not applicable.

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.

SAN 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 SAN 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 SAN 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. SAN data is considered For Official Use Only (FOUO). SAN 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 SAN 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 Institute for Defense Analysis (IDA) Facility located in Alexandria, VA requires privileged keycard entry. Access to both 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 SAN Privacy Impact Assessment dated 24 August 2015 resides at URL - https://www.dsca.mil/sites/default/files/san_pia_8-24-2015.pdf.

The SORN for the SAN system is currently undergoing revision and will be provided upon its finalization. A copy of the DRAFT SORN is included as a supplementary document.

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

Records are cut off annually and destroyed 25 years after cut off.

11. Sensitive Questions

The SAN does not collect social security numbers. International student are allowed to input information related to educational and employment information, academic evaluation, religious affiliation and preferences (i.e., food, entertainment, etc.). This is done to assist the International Military Student Officer (IMSO) in advising the student where they can find food per their religious dietary ay and places of worship during their training. .

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.

Number of respondents: 43,980
Number of responses per respondents: 1
Total Annual Responses: 43,980
Annual burden hours: 10,995
Average burden per response: 15 minutes

b. Labor Cost of Respondent Burden

Estimated hourly rate: $21.02
Rate Per Response: $5.255
Total Labor Cost: $231,115

Costs were determined through the DoD Cost Guidance Portal at URL
`https://www.cape.osd.mil/CGPortal/?source=collection`

13. Respondent Costs Other than Burden Hour Costs

$0

14. Cost to the Federal Government

Although the SAN funding is provided through the Foreign Military Sales Program, Software development costs incurred for the collection of the data is $100K. Annual operations and maintenance costs are $90K.

Estimated hourly rate: $14.17
Average processing time per response: 15 mins
Average processing Cost per 1 response: $3.54 ($14.17x .25)
Annual Processing Cost: $155,800 (43,980 x $3.54)

TOTAL ANNUAL COST TO GOVT: $345,800 ($100k + 90k + $155,800)

Costs were determined through the DoD Cost Guidance Portal.

15. Reasons for Change in Burden

This is an existing collection in use without an OMB control number.

16. Publication of Results

Not applicable.

17. Non-Display of OMB Expiration Date

Not applicable.

18. Exceptions to "Certification for Paperwork Reduction Submissions"

Not applicable.