

DOD PRIVACY IMPACT ASSESSMENT

1. Department of Defense (DoD) Component:
Defense Security Cooperation Agency (DSCA)

2. Name of Information Technology (IT) System:
Regional International Outreach (RIO) Federated Network

3. Budget System Identification Number (SNAP-IT Initiative Number):
PE 0605127T

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):
DITPR ID: 7526

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable):
N/A

6. Privacy Act System of Records Notice Identifier (if applicable):
Privacy Act Identifier: DOD-2007-OS-0018

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date:
N/A

8. Type of authority to collect information (statutory or otherwise):
DoD Directive 5105.65 Defense Security Cooperation Agency (DSCA); Pages 35 and 36 of Program Budget Decision (PBD) 704 December 2003 Signed by Ryan Henry, Principal Deputy Undersecretary of Defense for Policy and reinforced by Info Memo I-05/010987-STRAT, RIO Operational Requirements and Implementation Guidance signed by Principal Deputy Undersecretary of Defense for Policy.

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup):

The RIO federated network improves international outreach efforts (with students, graduates and subject matter experts) and collaboration among the Regional Centers for Security Studies, School of International Graduate Studies, and the Defense Security Cooperation Agency. The users are DoD Military and civilian employees, students, alumni, contractors, who interact with the Regional Centers for Security Studies, and subject matter experts of the Department of Defense's Regional Centers for Security Studies, and the School of International Graduate Studies.

The system of records will provide the capability to compile statistical information. The information technology is located at Space and Naval Warfare Systems Center Charleston—Europe Offices, Kelley Barracks, Bldg. 3315, 70567 Stuttgart-Moeringen, Germany, Space and Naval Warfare Systems Center Charleston, One Innovation Drive, Hanahan, SC 29406–4200, and the Naval Postgraduate School, Information Technology (ITACS), Monterey, CA 93943–5216. Because it is a distributed, federated system of nodes, the predominant users are graduates from the Africa Center for Strategic Studies (National Defense University, 300 5th Avenue, Bldg. 62, Fort McNair, Washington, DC 20319–5066), the Asia-Pacific Center for Security Studies (2058 Maluhia Rd., Honolulu, HI 96815–1949), the Center for Hemispheric Defense Studies (National Defense University at Coast Guard Headquarters building, 2100 Second Street SW., Suite 4118, Washington, DC 20593–0001), the George C. Marshall European Center for Security Studies (Gernackerstrasse 2, Gebaude 101, D–82467 Garmsch-Partenkirchen, Germany), and the Near East South Asia Center for Security Studies (National Defense University at Coast Guard Headquarters building, 2100 Second Street SW., Suite 4308, Washington, DC 20593–0001).

The system is currently operational, with continued updates and upgrades based on developmental and operational requirements. The system will be backed up using a Storage Area Network (SAN) at the Naval Postgraduate School. It will also be backed up offsite at SPAWAR Systems Center Charleston.

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.):

The system will have the capability to store name, e-mail address, address, organization, phone number, and biographic information such as expertise, background, and education.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.):

The intent of the system is to provide a social networking tool available on the World Wide Web. The user has the ability to either display or not display the any collected personal element to the users of the system.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.):

RIO supports policy established in DOD Directive 5200.41 (30 Jul 2004) and statute at 10 US Code Section 184. The information is to be used to allow

graduates and students of the regional centers the ability to maintain contact with class members and faculty. It also allows users to share their subject matter expertise so other users can find people of similar interests and backgrounds to form communities of practice.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.):

Users may search their classmates or the entire federation to find classmates or other users who share similar interests or backgrounds or subject matter expertise. Once a user has been identified or his expertise/interest has been identified, a user may view his contact information, given the user has granted other users the ability to view his profile.

14. Describe whether the system derives or creates new data about individuals through aggregation:

The system compiles usage data about an individual through aggregation of its federated nodes.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.):

The information is shared with members of the federation when voluntarily published into the RIO federation. It is not shared with any other systems or members of the DSCA or any additional DoD components.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent:

Users of the system have the ability to contact the regional center or school to remove them from the Federation. As an additional measure, the users can choose which information to populate and which information to share and the roles to which the information may be shared.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form:

A user is prompted to view the Terms of Use which shall include the Privacy Act Statement when logging into the system which states:

Title 5 U.S.C. 301, Departmental Regulations and 10 U.S.C. Chapter 2, Secretary of Defense authorizes collection of this information. The primary use of this information is to improve international outreach efforts (with students, graduates and subject matter experts) and collaboration among the DoD designated educational institutions. Submission of information is voluntary and all authorized users may view the information provided. The information is collected under OSD Privacy Act Systems Notice DOD-2007-OS-0018, Regional International Outreach System (RIO).

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form:

The information is maintained in secure information systems which are located in secure facilities. The federation administrators and the regional center administrators have access to the data to do outreach but the role based access controls do not allow unauthorized users to view this information. A user may intentionally allow viewing of each element, depending on the options he selects, to certain groups. He may also remove any identifiable information as well as by writing to the administrator remove himself entirely from the system. The system is secure, using best commercial practices (user name and password protected). Accounts are provisioned by the sponsoring institution.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur:

DSCA published a notice in the Federal Register / Volume 72, Number 44, Wednesday March 7, 2007 Page 10180-10181. The specific reference is DOD-2007-OS-0018.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures:

This system is located in the .edu DMZ located at the Naval Postgraduate School. This system is internet accessible and as such is subject to intrusions and mal use of any other systems accessible to the Internet. Best industry standards are being used but there exists the possibility of intrusion and theft of records. This threat is low due to compliance with all DoD Security

Technical Implementation Guides (STIG), intrusion detection systems, and perpetual monitoring. SPAWAR Systems Center Charleston is providing the security analysis, the SSAA package, and technical implementation.

There is the possibility a user may enter all personal information and not understand that he needs to use the select box to not display his information into the federation. This is a low priority as the user can clearly see the default state as well as help tutorials and training sessions, where available, will stress this point.

There is also the possibility of the insider threat. Federation and regional center administrators have access to the information and could publish this information against policy. By limiting this role and monitoring the system use, this threat would be mitigated.

Users have the ultimate control of their data. If users choose not to provide information other than email and name, they will not experience system degradation. If they choose to share personal information, they can control with whom the information is shared. The information is stored on secure hardware and software located in secure facilities. The potential for privacy risks are low.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form:

This is Unclassified and should be published.