PRIVACY IMPACT ASSESSMENT (PIA)

For the

GlobalNET Outreach and Collaboration Platform
Defense Security Cooperation Agency

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐ **New DoD Information System** ☐ **New Electronic Collection**

☒ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒ **Yes, DITPR** Enter DITPR System Identification Number | 7526

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number |

☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐ Yes ☒ No

If "Yes," enter UPI |

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ Yes ☐ No

If "Yes," enter Privacy Act SORN Identifier | DSCA 02

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. |

e. Does this DoD information system or electronic collection have an OMB Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

> **Enter OMB Control Number** | Pending Review |
>
> **Enter Expiration Date** | |

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 134, Under Secretary of Defense for Policy; DoD Directive 5101.1, DoD Executive Agent, Section 5.2.7; DoD Directive 5105.65, Defense Security Cooperation Agency (DSCA), Section 5.n; DoD Directive 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; and DoD Directive 5200.41, DoD Centers for Regional Security Studies, Section 3.1.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

    (1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The purpose of GlobalNET platform is to provide a collaborative social networking environment/capability where students, alumni, faculty, partners, and other community members and subject matter experts can find relevant and timely information about pertinent subject matter experts.

The system will have the capability to store name, citizenship, home and email addresses, personal telephone numbers, organization, gender, date of birth, month/year of attendance and course subjects, and biographic information such as subject matter expertise, background, and education.

    (2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

This system is currently located in a shared hosting facility ("Cloud") operated by Amazon and managed by the commercial entity Acquia. 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, including data encryption at both rest and in-motion, are being used but there exists the possibility of intrusion and theft of records. This threat is low due to compliance with industry best practices and information assurance controls, intrusion detection systems, and perpetual monitoring.

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 of his information into the federation (i.e., federated system which supports DoD's information sharing and collaboration efforts). 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 is 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.

The information is maintained in secure information systems which are located in secure facilities. The 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 the administrator to 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 community

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒   **Within the DoD Component.**

    Specify. | Regional Center Personnel Activity Management System (RCPAMS) |

☐   **Other DoD Components.**

    Specify. | |

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

This effort has multiple contractors on the integration and support teams in addition to any contractors each institute retains for its general support. Each contract DSCA manages contains provisions to ensure the confidentiality and security of PII and safeguards are in place to manage PII in the workplace.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. **Do individuals have the opportunity to object to the collection of their PII?**

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Users of the system have the ability to contact the sponsoring institution and have all PII removed from the system.

(2) If "No," state the reason why individuals cannot object.

j. **Do individuals have the opportunity to consent to the specific uses of their PII?**

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Users can choose which information to populate and which information to share and the roles to which the information may be shared.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☐	**None**

Describe each applicable format.

By logging into this system, you are confirming you have read and understand the following Terms of Use. The primary use of this system is to foster communities of practice in support of international outreach efforts between students, graduates and subject matter experts of the regional centers for security studies, and other defense related educational institutions, as directed. The system will aid and facilitate collaboration among the aforementioned individuals and activities. With the exception of name and email address, submission of information is voluntary without any degradation of functionality for incomplete information.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.