

INTERNational Connections Privacy Impact Assessment

1. Contact Information

Department of State Privacy Coordinator

Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: September 30, 2009

(b) Name of system: INTERNational Connections

(c) System acronym: IC

(d) IT Asset Baseline (ITAB) number: 4669

(e) System description (Briefly describe scope, purpose, and major functions):

The Department's student internship programs provide a key source of potential candidates who have an interest in, and are qualified, to become future Department employees. Naturally, HR/REE wants to strengthen and maintain its connections to this group, fostering and mentoring a pool of candidates from which to obtain successful recruits. HR/REE developed an intern engagement strategy to assist in maintaining these connections. The foundation of this strategy is INTERNational Connections, a web-based career networking site for current and former interns that collects pertinent information about them, their experiences and their career goals.

The benefits include:

- Streamlined communications between Executive Offices and Hiring Offices and between Bureau Coordinators and Bureau Interns who are serving domestically and overseas;
- Web-based application that can be accessed from anywhere in the world at any time without having to access the Department system;
- Makes it easier to stay connected with interns for mentoring and career networking;
- Facilitates encouraging communications between bureau offices and interns with an end goal of promoting their future in the Department; and
- Executive Offices and Bureau Coordinator will be able to submit appropriate intern communications to HR/REE Student Programs for distribution through the system or upload relevant documents to the Intern Assistance Center in the Knowledge Corner.

(f) Reason for performing PIA:

- New system
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable):

(h) Date of previous PIA (if applicable):

3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

International Connection collects name, email address, username and password, where you're from, university name, major/minor, where you traveled to during your internship or employment with Department of State, program name, program start date, program end date, your field of study and resume or curriculum vitae (CV). The sources of information are current, former and future interns.

b. How is the information collected?

Information is collected by web form and resume or CV is uploaded by the user.

c. Why is the information collected and maintained?

INTERNational Connections collects data in order to keep track of the participants of its student programs. The U.S. Department of State must justify to the U.S. Congress the importance of its student programs and tracking its participants' activities is one way to do just that. The Bureau of Human Resources wants to maintain a connection with student program participants after they have completed a specific program. The primary goal is to assist in encouraging, motivating and inspiring these potential candidates to pursue a career with the U.S. Department of State. Additionally, the collected data is used to fine-tune the design and functionality of the site.

d. How will the information be checked for accuracy?

INTERNational Connection depends completely upon the participants for the accuracy of the information.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

Foreign Service Act of 1980;
22 U.S.C. § 2651a Organization of the Department of State;
22 U.S.C. § 3901 Congressional Findings and Objectives; and
22 U.S.C. § 4141a Foreign Service Internship Program.

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

INTERNational Connections collects the absolute minimum amount of PII required to satisfy the statutory purposes of this system and the mission of the Bureau of Human Resources.

4. Uses of the Information

a. Describe all uses of the information.

The information will be used to stay connected with interns for mentoring and career networking in order to obtain successful recruits. Additional uses of information are described above in 3c.

b. What types of methods are used to analyze the data? What new information may be produced?

The U.S. Department of State use data to perform statistical analyses of the collective characteristics, interests, and behaviors of registered users.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Not applicable. INTERNational Connections does not use commercial information or publicly available information, or information from other Federal agency databases.

d. Are contractors involved in the uses of the PII?

Contractors are involved in the design, development and maintenance of the system. All contractors are required to complete and renew when appropriate, security awareness training. In addition, Privacy Act clauses are present in the contracts and in the Statements of Work of each contractor company hired. All contractor personnel are required to pass a National agency check prior to being awarded contract work.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

INTERNational Connections stores all user information in a secure database protected by a variety of access controls. For site security purposes and to ensure that this service remains available to all users, the government computer system employs commercial software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Retention

a. How long is information retained?

Information is retained as long as the user is active on the system. Any user account that has been inactive for more than 18 months is deactivated and purged from the system. All users have the ability to deactivate their accounts whenever they want.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The information is only retained for the amount of time that is required to perform the system's purpose. There are minimal risks with unauthorized use or exposure. The

risks are mitigated by limiting access to the data only to those authorized through a formal approval process with the need to know.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The information may be shared with current student program participants to connect participants with one another. Information is shared with Department employees to perform their official duties.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Participants must be registered users of the website. All users must have a user ID and password to access the site. System authentication is based upon role-based control and session management. All actions performed within the system are audited by controls configured for the operating system and database management.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

INTERNational Connections stores all user information in a secure database protected by a variety of access controls. This information is accessed only for the purposes specified in section 2e above. The government computer system employs commercial software programs to monitor network traffic that will identify unauthorized attempts to upload or change information.

In addition, DoS employees are required to undergo computer security and privacy awareness training and must complete refresher training yearly in order to retain access.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

INTERNational Connections information is NOT shared with external organizations.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Not Applicable.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Not Applicable.

8. Notice

The system:

- contains information covered by the Privacy Act.
Human Resources Records, State-31
(visit www.state.gov/m/a/ips/c25533.htm for list of all published systems):
- does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice of the purpose, use and authority for collection of information is described in the System of Records Notices titled Human Resources Records State-31. Notice is given when accessing the website.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes. Providing the information is strictly voluntary and only required if you desire to participate in the student program.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Data such as username, password, first and last name, email address, college/university, major/minor, program status and elementary school name, is necessary to process your request for participation in INTERNational Connections. Providing optional data such as year graduated, degree, photos, career goals, professional experience, areas of interest, resume, achievements, department bureau, student program information, internship experience, home and work information, interesting links and world location is totally at discretion of the individual. Data is clearly marked as required or optional.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice offered is reasonable and adequate in relation to the system's purposes and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Participants can update and edit their personal information by logging into the site and clicking Update Your Profile. Participants may also request their INTERNational Connections account be deactivated by sending an email to internconnect@state.gov.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses. Individuals can update their accounts as needed.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

INTERNational Connections stores all user information in a secure database protected by a variety of access controls. This information is accessed only for the purposes specified in section 2e above. The government computer system employs commercial software programs to monitor network traffic that will identify unauthorized attempts to upload or change information.

The system uses a secure shell key encryption for access to the server, meaning you have to have a valid key to even connect to the server. Root level access to the server and the database content and structure is limited to two system administrators. Application access to data is limited to two content developers, and three Site Content Managers. Connectivity to the server is done via secure socket layer, all access requires an authorized user account, including multi-tier access levels differentiating area and level of access.

b. What privacy orientation or training for the system is provided authorized users?

DoS employees and contractors are required to undergo computer security and privacy awareness training and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

There is no expected residual risk.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

There are no technologies used in the system that involve privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Not applicable.

12. Security

What is the security certification and accreditation (C&A) status of the system?

IC is a system that is not reportable per the Federal Information Security Management Act, because it is categorized as a Low impact system, per the Federal Information Processing Standards Publication, Standards for Security Categorization of Federal Information and Information Systems 199.