

INTERNational Connections

1. Contact Information

A/GIS/IPS Director

Bureau of Administration

Global Information Services

Office of Information Programs and Services

2. System Information

(a) Name of system: INTERNational Connections

(b) Bureau: HR/REE

(c) System acronym: IC

(d) iMatrix Asset ID Number: 4669

(e) Reason for performing PIA: Click here to enter text.

New system

Significant modification to an existing system

To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

Yes

(b) What is the security Assessment and Authorization (A&A) status of the system?
INTERNational Connections (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. The categorization of this system is a low risk impact level, low confidentiality, integrity, low availability and low cost and is non FISMA-reportable application

(c) Describe the purpose of the system:

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. HR/REE strengthens and maintains its connections to this group by 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;
- A web-based application that can be accessed from anywhere in the world at any time without having to access the Department system;
- Making it easier to stay connected with interns for mentoring and career networking;
- Facilitating and encouraging communications between bureau offices and interns with an end goal of promoting their future in the Department; and
- Enabling Executive Offices and Bureau Coordinator 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.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

- Last Name
- First Name
- Hometown
- Personal Email Address
- University Name
- Major/Minor
- Degree
- Year Graduated (or anticipated graduation)
- Career tracks of interest
- Professional Experience
- Current Post
- Job Title
- Bureau

(e) What are the specific legal authorities and/or agreements that allow the information to be collected? 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) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- SORN Name and Number: Human Resource Records State-31
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): July 19, 2013

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes No

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes No

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): GRS 4.3, item 031 (DAA-GRS-2013-0001-0006)
- Length of time the information is retained in the system: Undetermined
- Type of information retained in the system:
: Data intern data maintained in REETA (Disposable under N1-059-007, Item 8)

4. Characterization of the Information

- (a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
 U.S. Government employees/Contractor employees
 Other (people who are not U.S. Citizens or LPRs)

- (b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes No

- (c) How is the information collected?

Information is collected directly from the individuals who voluntarily register for an account on the INTERNational Connections website. Once individuals receive a security clearance for their internship, they are sent an email giving them information about the website. Individuals are told to create an online profile, login ID, and password at <https://internconnect.careers.state.gov/register/>. After they create their profile, individuals are verified through REETA (Recruitment, Examination, and Employment Tracking) that they work or intern for the Department of State before being granted access to the website.

- (d) Where is the information housed?

- Department-owned equipment
 FEDRAMP-certified cloud
 Other Federal agency equipment or cloud
 Other The data is stored offsite at Softlayer

- (e) What process is used to determine if the information is accurate?

Internship participants are manually verified through REETA (Recruitment, Examination, and Employment Tracking). INTERNational Connections depends completely upon the participants for the accuracy of member's personal information.

- (f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

INTERNational Connections depends completely upon the participants to keep information current.

- (g) Does the system use information from commercial sources? Is the information publicly available?

No. INTERNational Connection does not use information from commercial sources and is not publicly available or accessible.

- (h) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes No

- If yes, how do individuals grant consent?

Providing the information is strictly voluntary and only required if individuals choose to participate in the career networking platform

- (i) How did privacy concerns influence the determination of what information would be collected by the system?

Privacy concerns were considered. Profile security was a privacy concern, and we limited the profile information to be career specific, while still providing information which will assist the Department and the users to determine where their academic experience align with potential career tracks. The Risk's to privacy were determined to be of low risk. However, the information collected is limited to that which will assist the Department and the users to determine where their academic experiences align with potential career tracks.

5. Use of information

- (a) What is/are the intended use(s) for the information?

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. The information will be used to engage interns in career networking and convert some into full-time employees. INTERNational Connections collects data to keep track of participants of its student programs. Tracking interns' activities allows the Department to justify the importance of its student programs to Congress. The Bureau of Human Resources wants to maintain a connection with student program participants after they have completed a specific program.

- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes. INTERNational Connection allows for the Bureau of Human Resources to maintain engagement with its internship program participants.

- (c) Does the system analyze the information stored in it? Yes No

6. Sharing of Information

- (a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The information may be shared with current student program participants to connect participants with one another. Information is shared with Diplomats-in-Residence and recruiters to assist with maintaining engagement between the Department and program participants.

- (b) What information will be shared?

Only the volunteered information that was referenced in 3(d), except for email addresses.

- (c) What is the purpose for sharing the information?

HR/REE recruiters and Diplomats in Residence use the system to identify those in their regions with whom they can connect and provide guidance for future employment possibilities. IC participants can learn from one another's experiences and find commonalities like universities, locations, languages, etc.

- (d) The information to be shared is transmitted or disclosed by what methods?

Participants must be registered users of the website. All users, including student participants, must have a user ID and password to access the site.

- (e) What safeguards are in place for each internal or external sharing arrangement?
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.
- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed? Profile privacy is a concern regarding the sharing of information. This risk is mitigated through the use of data security for each profile field has user based access controls installed that allows them to limit the sharing of their profile data at the field level. Sharing of data is limited strictly to mission activities

7. Redress and Notification

- (a) What procedures allow individuals to gain access to their information?
Individuals are able to access and edit their profiles on the site.
- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
 Yes No
If yes, explain the procedures.
Participants can update and edit their personal information by logging into the site and clicking Edit Your Profile. Participants may also request their INTERNational Connections account be deactivated by sending an email to internconnect@state.gov.
- (c) By what means are individuals notified of the procedures to correct their information?
By creating an online account, individuals have the ability to edit and update their own information by logging on to the system using their assigned username and password.

8. Security Controls

- (a) How is the information in the system secured?
Only users who have been issued a username and password to the site may access/change their own password. INTERNational Connections uses sender email address to validate password resets. User needs access to the email account they used to set up the system to change their password or issue and complete a password reset.

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 above. The government computer system employs commercial software programs to monitor network traffic that will identify unauthorized attempts to upload or change information. IC uses WordPress BuddyPress software. All login attempts are captured in the system logs, which are monitored routinely for abnormal traffic/failed login attempts.

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

Only the site's webmaster, a backup from the Marketing Department, and select members of the technology consulting company who helped develop the website have access to the site.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Audit logs are maintained to record system and user activity including invalid logon attempts and access to data. The INTERNational Connection site regularly goes through the Department's Compliance & Vulnerabilities scan. E&V Scanning runs McAfee vulnerability scans every 6 months, and DS helps analyze for remediation.

- (d) Explain the privacy training provided to authorized users of the system.

The Department's user policy and rules of behavior are the general terms under which federal employees and contractors use the system. The Department requires all new employees and contractors to attend Cyber Security Awareness training before or immediately after the employment start date and prior to being granted access to the system along with the completion of online course PA-459, Protecting Personally Identifiable Information (PII). In addition, the OpenNet account request form signed by all employees and contractors includes a "Computer Security Awareness Form" that provides privacy orientation. To retain access, all Department personnel must complete annual refresher training. Access to data is limited to cleared U.S. Government employees.

- (e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? Yes No
If yes, please explain.

INTERNational Connections uses https, is not Google-searchable, and only people who have been verified through REETA as Department employees or interns are granted access to this password protected website.

- (f) How were the security measures above influenced by the type of information collected? Because of the PII submitted by users on the site in conjunction with the fact that following HTTPS protocol is now a mandated practice, HR/REE has secured the site with an HTTPS certificate. Although there was no mandate in place at the time of startup, There was no current mandate in place at the time of startup to use https. The decision was made to use HTTPS. The use of HTTPS provides an extra level of security measures.

9. Data Access

- (a) Who has access to data in the system?

- **System administrators** are limited to authorized contractor company personnel. Administrative accesses to the servers are reviewed on a monthly basis to ensure access is restricted to authorized personnel.
- **Database administrators** are limited to authorized contractor company personnel. Access to key databases (DBA and direct access) is reviewed on a quarterly basis
- **Students and Department of State employees** have access the volunteered profile information from fellow users. This does not include email addresses

- **Subscribers:** Students and recruiters can access the data they submit to the site and manage his/her profile

(b) How is access to data in the system determined?

To gain Access to the system, users are required to fill out profile information to create an account. After creating their profile, users are verified through REETA (Recruitment, Examination, and Employment Tracking) to validate that the user works or interns for the Department of State before being granted access to the website.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? Yes No

(d) Will all users have access to all data in the system, or will user access be restricted? Users will have access to select information, while the Administrators will have access to all of the information.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Field level security and password protection has been implemented to limit users from accessing data outside their areas, whether logged in to the system or not. Each account also has user level permissions: Administrator, Author, Editor, Subscriber, Keymaster, or Participant. 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 (SSL), all access requires an authorized user account, including multi-tier access levels differentiating area and level of access.