

# eRecruitment

## 1. Contact Information

<p><b>A/GIS/IPS Director</b>          Bureau of Administration          Global Information Services          Office of Information Programs and Services</p>
--

## 2. System Information

- (a) Name of system: eRecruitment
- (b) Bureau: NEA-SCA/EX
- (c) System acronym: eRecruitment
- (d) [iMatrix Asset ID Number](#): 167747
- (e) Reason for performing PIA:
  - 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
  - No - Contact IRM/IA at [IASolutionCenter@state.gov](mailto:IASolutionCenter@state.gov) for assistance.
- (b) What is the security Assessment and Authorization (A&A) status of the system?
  - A&A in progress, estimated complete date: July 2015
- (c) Describe the purpose of the system:
  - eRecruitment allows HR personnel at NEA-SCA posts to manage and track employment application data for Locally Employed Staff or Family Member during the recruitment process.
- (d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
  - Name
  - DOB
  - SSN

- Address (Home/Work)
- Phone Number (Mobile/Home/Work)
- E-Mail Address (Personal/Professional)
- Educational History
- Job Experience
- Military Status
- Citizenship

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

22 U.S.C. 2581 (General Authority of Secretary of State)  
 22 U.S.C. 3901 et seq. (Foreign Service Act of 1980)  
 22 U.S.C. 3921 (Management of the Foreign Service)  
 5 U.S.C. 301-302 (Management of the Department of State)

(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 2013

No, explain how the information is retrieved without a personal identifier (*if you do not have a SORN, contact [Privacy@state.gov](mailto:Privacy@state.gov)*).

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

Yes  No

If yes, please notify the Privacy Division at [Privacy@state.gov](mailto:Privacy@state.gov).

(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): [A-04-002-01b](#)
- Length of time the information is retained in the system: Delete within 180 days after recordkeeping copy has been produced.
- Type of information retained in the system: Electronic version of records created by electronic mail and word processing applications.
- DispAuthNo: N1-059-00-07, item 1b

#### 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

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

Yes  No

- If yes, under what authorization?  
Executive Order 9397

(c) How is the information collected?

Individuals apply for a position within the Department of State using DS Form 174 and provides the Department with their personal information which is used in the evaluation of their qualifications.

(d) Where is the information housed?

Department-owned equipment  
 FEDRAMP-certified cloud  
 Other Federal agency equipment or cloud  
 Other

- If you did not select "Department-owned equipment," please specify.

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

Applicants are responsible for ensuring the accuracy of their submission. Any errors or omissions can impact their consideration for a vacancy.

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

- Yes. Information is current at the time of submission but does not need to be maintained afterward.

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

- The system does not use any commercial information, publicly available information, or information from other Federal agency databases. All of the information in the system is supplied by the applicants.

(h) Is notice provided to the individual prior to the collection of his or her information?

- Notice of the purpose, use and authority for collection of information submitted are available in the Privacy Act Statement on the DS Form 174.

(i) 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 information on the application is voluntary, however the application will not be processed if an individual fails to disclose any information (including SSN). Before divulging information via the telephone (Land-Line, Mobile, or Internet), the individual is informed of the Privacy Act statement; whereby, the acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information.

-If no, why are individuals not allowed to provide consent?

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

- The least amount of personal information necessary to verify personal identity and qualification is collected and provided only to those necessary for the approval process.

## 5. Use of Information

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

- The information is collected to determine the knowledge, skills and abilities of applicants seeking employment and to select the successful candidate. The PII will be use to verify citizenship, military service, to conduct investigation and determine employment suitability. The social security number is used to verify identify.

- (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

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

If yes:

(1) What types of methods are used to analyze the information? *(Include any analysis other than standard reporting requirements.)*

(2) Does the analysis result in new information? *(If the system creates or makes available new or previously unutilized information about an individual, describe the new information.)*

(3) Will the new information be placed in the individual's record?  Yes  No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without 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 submitted to eRecruitment by potential employees is used internally by Human Resources (HR) departments of local posts within the Department of State.

- (b) What information will be shared?

- All information submitted by applicant.

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

- The information which is shared between the departments is limited to only what is necessary in order to track the progress of the potential employee's candidacy into a position with the Department of State.

- (d) The information to be shared is transmitted or disclosed by what methods?
- Electronically within eRecruitment or viaPDF
- (e) What safeguards are in place for each internal or external sharing arrangement?
- The information is hand carried from one HR department to the other by a HR employee who has been trained on the handling procedures consistent with information of this level of sensitivity.
- Moreover, numerous management, operational and technical controls are in place to reduce and mitigate the risks associate with internal sharing and disclosure including, but not limited to annual security training, separation of duties, least privilege and personnel screening.
- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?
- Unauthorized and/or unintentional disclosure of privacy information from personnel can result from social engineering, phishing, abuse or elevated privileges or general lack of training. Transmission of privacy data in an unencrypted form (plan text), and over an un-trusted communications link can also pose a significant risk. Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with unauthorized external sharing and unintentional disclosure including, but not limited to formal Memorandums of Agreement. Understandings (MOA/MOU), services level agreements (SLA) annual security training, separation of duties, least privilege and personnel screening.

## 7. Redress and Notification

- (a) What procedures allow individuals to gain access to their information?
- For each application filed, eRecruitment generates an email to the user which contains a random password and the record ID of the entry. Users will gain access to eRecruitment with registered email and password.
- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
- Yes No
- If yes, explain the procedures.
- Prior to final submission, user may update information using step specified in section 7a.
- (c) By what means are individuals notified of the procedures to correct their information?
- Email

## 8. Security Controls

- (a) How is the information in the system secured?
- IRM uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the Internet-connected systems that host IRM's major and minor applications, including the eRecruitment components, for changes to the DoS mandated security controls.
- (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 administrators and HR managers, who are Department of State direct hire or contractor employees, can manage the application given proper authorization.
- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
  - None
- (d) Explain the privacy training provided to authorized users of the system.
  - Standard training required by all State department employees as well as daily “Tip of the day” messages.
- (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.
- (f) How were the security measures above influenced by the type of information collected?
  - All security measures were implemented as a direct result of the information collected.

## 9. Data Access

- (a) Who has access to data in the system?
  - System Owners: all data
  - NEA-SCA/HR, HR staff at post: access only to those to their post
  - Local hiring managers: access to only those they need to approve
  - Users (access to only those items they have entered).
- (b) How is access to data in the system determined?
  - Respective approving authority security group managers
- (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?
  - Access will be limited according to role-based restriction.
- (e) What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?
  - There are no systems controls. Rather the system relies on the Department’s Rules of Behavior for Protecting Personally Identifiable Information which instructs users to only access information in the performance of their official duties.