

**WHAFRCeRecruit**

**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: Florida Regional Center (FRC) Regional Online Recruitment Platform
- (b) Bureau: WHA/EX/FRC
- (c) System acronym: WHAFRCeRecruit
- (d) IT Asset Baseline (iMatrix) number: 171206
- (e) Reason for performing PIA:
  - New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security re-certification
- (f) Explanation of modification (if applicable):N/A

**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: TBD
- (c) Describe the purpose of the system: WHAFRCeRecruit allows HR personnel at WHA posts to electronically screen employment applications for publicly announced local staff positions.
- (d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
  - Name
  - Nationality

- POB
- DOB
- Address (Home/Work)
- Phone Number (Mobile/Home/Work)
- USA Veteran Status
- E-Mail Address (Personal/Professional)
- Education
- Job Experience
- Citizenship
- Spouse Info if working at post
- IP Address

(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?

- (c) How is the information collected?

Information is collected directly from individuals applying for a position within the Mission through the use of the Online Recruitment website and completing the information requested.

- (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. Due to the purpose of the system, the accuracy of the information and does not need to be current 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?

- Individuals are provided an approved Privacy Act statement on the WHAFRCeRecruit website.

- (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. 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 pre-screen applicants seeking employment and to select potential candidates for further review. The PII will be used to verify employability within the host nation, prior military service, and determine suitability for the position advertised.

- (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 WHAFRCeRecruit by potential employees is used internally by Human Resources (HR) departments of local posts along with those in the hiring process (e.g., selecting official) as appropriate within WHA.

- (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 departments is limited to only what is necessary to determine a potential employee's qualifications for a position within the post.

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

- Electronically within WHAFRCeRecruit or via printed PDF.

- (e) What safeguards are in place for each internal or external sharing arrangement?

- The hard-copy PDF form 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 (plain 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, WHAFRCeRecruit generates an email to the user which contains a random password and the record ID of the entry. Users will gain access to their own information in WHAFRCeRecruit with their 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 their access to the system.

(c) By what means are individuals notified of the procedures to correct their information?

- Emails are sent to the applicant which provides instructions on updating their information up to the time of final submission.

## 8. Security Controls

(a) How is the information in the system secured?

- WHAFRCeRecruit resides within a DMZ behind a secure firewall. Administrative access is restricted using Personal Identification Verification (PIV) technology.

(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 with proper authorization and permission, can manage the data within the application.

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

- IP addresses of persons visiting the site are recorded to assist with investigation of unusual activity on the website. System logs and audits are managed and reviewed by WHA\EX\FRC IRM personnel.

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

- Standard training (i.e., Annual CyberSecurity and Protecting Personally Identifiable Information Online Training courses through FSI) is 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.

- Administrative access is restricted using PIV technology. Access to the physical servers is restricted to WHA\EX\FRC IRM personnel only using combination locks and alarms.

- (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 type information collected and as directed by IRM/IA.

## 9. Data Access

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

- System Owners: all data  
- WHA Post HR: HR staff at post: access only to their WHAFRCeRecruit site.  
- 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?

- On a need to know basis as determined and approved by the Post HRO and FRC IMO.

- (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?

- 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.