

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

2. System Information

- a. **Date PIA was completed:** July 31, 2008
- b. **Name of system:** Human Resources Network
- c. **System acronym:** HR Net
- d. **IT Asset Baseline (ITAB) number:** 866
- e. **System description (Briefly describe scope, purpose, and major functions):** The Human Resources Network (HRNet) serves as the Bureau of Human Resources' main web portal for providing internet-based services, including the Retirement Network (RNet). RNet provides the ability for Department of State retirees to enroll on a mailing list to receive information provided by the Director General, complete an Employee Profile Plus (EP+), review employment opportunities, and receive information about the Standby Response Corps.

Note: RNet users will be authenticated against Foreign Affairs Retirement and Disability System (FARADS) data provided by IRM. The fields used to validate users during the registration process are last name, first initial of the first name, birthday month and day, and last four (4) digits of the social security number. Retirees will be able to enter and retrieve data pertaining to their self-assessed skills in countries, organizations, professions, languages, and competencies.

f. Reason for performing PIA:

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

g. Explanation of modification (if applicable):

h. Date of previous PIA (if applicable): 07/31/2005

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? The fields used to validate users during the registration process are last name, first initial of the first name, birthday month and day, and last four (4) digits of the social security number. HRNet users are authenticated against Department of State data sourced

from the Foreign Affairs Retirement and Disability System (FARADS) and the Integrated Personnel Management System (IPMS).

b. How is the information collected? The information is collected from the individual during the registration process using a web form.

c. Why is the information collected and maintained? The data is used to verify potential user's identity during the registration process and manage access and other administrative purposes.

d. How will the information be checked for accuracy? The individual is responsible for the accuracy of the information they provide.

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

22 U.S.C. 2581 General Authority of Secretary of State
22 U.S.C. 2651a Organization of the Department of State

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated. The system collects last 4 digits of a user's social security number, last name, and middle initial. This information is use to authenticate the user's identity. No other personal data is collected or stored in HRNet.

4. Uses of the Information

a. Describe all uses of the information. For retirees to indicate their willingness to be considered for reemployment. In addition, they can update their EP+ and sign up for Standby Response Corps.

b. What types of methods are used to analyze the data? What new information may be produced? HR Net does not create new, derived, or aggregate information about individuals.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used. Not applicable.

d. Is the system a contractor used and owned system? Contractors are involved in the development and maintenance of this system. All contractors are required to have completed and keep up-to-date security awareness training.

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. Appropriate use of the system is regulated by automated controls in the system and by instruction information published on the website.

5. Retention

a. How long is information retained? Per the Department's record disposition schedule, records are maintained until their use is no longer required then are destroyed immediately thereafter.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated. Risk is mitigated by retaining the data for the minimal time necessary.

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? Information is shared with the program office for managing the Standby Response Corps.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement? Information is available only to approved authorized users. The users are briefed on the rules of behavior before the account is created and/or use is authorized. The account is cancelled immediately after it is no longer required.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated. Access to data is only available to authorized users who are cleared government employees/contractors. The information is used in accordance with its stated authority and purpose, and is restricted to only those individuals with a "need-to-know."

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? HRNet does not interface or share data with any external organizations or other U.S. government systems.

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.
Provide number and name of each applicable systems of records.
(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? The purpose, use and authority for collection of information submitted are described in the System of Records Notice, STATE-31, titled Human Resource Records. A website Privacy Policy is also available on the public-facing website.

b. Do individuals have the opportunity and/or right to decline to provide information? Yes, retirees may decline to provide the information, thereby preventing his/her access to the system.

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? No other special uses of the information are permitted. Users are advised on the use of the information being collected.

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. Notice about collection of personal information is provided on the website and in the System of Record Notice. The notice is specific to the system's purpose and sensitivity of the PII collected.

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? When a user's identity is authenticated by the system, individuals are able to access the system and update their account information as needed.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated. There is minimal/no privacy risks associated with this system. However, individuals can update their accounts as needed or follow the notification and redress procedures stated in the System of Record Notice, STATE-31, that is published in the *Federal Register*.

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? User access is restricted. The network operating system access controls and limits who can logon, what resources will be available, what each user can do with these resources, and when and from where access is available. System managers, key security, and user personnel cooperate closely to implement access controls.

b. What privacy orientation or training for the system is provided authorized users? The Department of State's use policy and rules of behavior are the general terms under which retirees and other federal employees use the system. No special privacy orientation is needed since only partial PII data is used to authenticate authorized users. Access to data is limited to cleared U.S. Government employees/contractors administering the system with an "official" need-to-know.

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. No residual risk is identified.

11. Technologies

a. What technologies are used in the system that involves privacy risk? None.

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? HR Net was last certified on 7/31/2005, with recertification in process and expected to complete on or before 8/31/2008

Certifying Officials' Signatures

Rueben Torres

System Owner

Dan Stapula

Program Manager

William Griffin

Information Security Manager

Email the completed PIA in MSWord format to “PIA Team”. Upon signing, please send this signature page to the same group email box in the form of a scanned PDF, or send as paper via interoffice mail to “A/ISS/IPS/PRV”.

TO BE COMPLETED BY A/ISS/IPS/PRV:

Reviewer: Essie L. Bell

Higher-Lever Reviewer: Paula Ferguson