



# **Privacy Impact Assessment**

***FY 2014***

***Human Resources Network (HRNet)***

***(iMATRIX NUMBER 866)***

## 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: Human Resources Network
- (b) Bureau: HR
- (c) System acronym: HRNet
- (d) iMatrix Asset ID Number: 866
- (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): Addition of Entrance On Duty (EOD), iMatrix #66451, and HR Surveys, iMatrix #67982, as child systems of HRNet.
- (g) Date of previous PIA (if applicable): March 30, 2011

## 3. General Information

- (a) Describe the purpose of the system:

HRNet serves as the Bureau of Human Resources' main web portal for providing Internet-based human resources services to the Department of State community, and other agency users to include retired or retiring Foreign Service employees of the Departments of Commerce, Agriculture, the Agency for International Development, the Broadcasting Board of Governors and Peace Corps, as well as retirees and annuitants from all the Foreign Affairs agencies. The HRNet web portal infrastructure is comprised of the following.

- Retirement Network Alumni Organization Site (RNet): RNet is a static internet web site that provides information to Foreign and Civil Service retirees from the Department of State and other foreign affairs agencies. It provides information about the services we offer to active employees and annuitants. Provides detailed information and helps the employee both Civil Service and Foreign Service plan for retirement.
- National Security Decision Directive (NSDD-38) System: The Department of State provides workspace and a variety of services at Posts to individuals who work for other USG agencies as well as some NGO's. National Security Decision Directive 38 (NSDD-38) documents this relationship and the process governing the request,

approval, establishment, and management of those positions at Post. The NSDD-38 application is a web-based application designed to allow approved and authorized USG agency or NGO users to request that a position be established at Post

- Civilian Response Corps (CRC) System: CRC application is used by the Bureau of Conflict and Stabilization Operations (CSO) in Washington for tracking and reporting on CRC members and their missions overseas. The CRC system permits CRC members and partner agencies to input required personnel and deployment information into an HRNet-based interface
- Gateway to State (GTS) – Monster Government Solutions (MGS) File Transfer Tool: HR/EX/ESD technical staff manually initiate unidirectional sftp file transfers from Gateway to State (aka, Monster Hiring Management Enterprise) to HRNet on request from the Office of Recruitments, Examination, and Employment (HR/REE). Gateway to State is a web-based job candidate assessment tool that is accessible via the Internet from the USA Jobs site. Gateway to State interfaces with OPM's USA Jobs recruitment tool and serves as the automated mechanism for applicants to apply for all DoS Civil Service and most Foreign Service jobs. Gateway to State is part of the Hiring Management Enterprise Suite system that is managed and serviced by Monster Government Solutions (MGS).
- Connect:Direct Client Tool for Department of Labor (DoL) Data Sharing: Connect:Direct is a point-to-point file-based integration middleware used by HR in the DMZ on a dedicated server to perform file transfers with the DoL. Connect:Direct is a COTS software tool hosted within the HRNet system boundary though it is not an application.
- Entrance on Duty (EOD) System: EOD automates the employee onboarding process. The EOD system provides easy data entry, standardized routing and processing in order to create a seamless user experience for DoS applicants and to avoid excess data entry for all participants involved.
- HR Surveys: Offices within HR have business requirements to gather survey information from their internal (OpenNet users) and external (non OpenNet users) customers. The survey sponsor (respective HR Office) is responsible for identifying and providing the targeted audience list for emailing out the surveys. HR Surveys does not include the notification messaging. HR Surveys consists of the management of question presentation and response data.

(b) What are the specific legal authorities, arrangements, and/or agreements that allow the information to be collected (e.g., statutory and regulatory authorities, Executive Orders, and Memorandums of Understanding (MOUs) authorizing the collection, maintenance, use and dissemination of PII).

- 22 U.S.C. 2581 (General Authority of Secretary of State)
- 22 U.S.C 2651a (Organization of the Department of State)
- 22 U.S.C 2901 et seq. (Foreign Service Act of 1980)
- 22 U.S.C. 3921 (Management of the Foreign Service)
- 22 U.S.C 4041 (Administration of the Foreign Service Retirement and Disability System)
- 5 U.S.C. 301-302 (Management of the Department of State)

- Executive Order 9397, as amended (Numbering System for Federal Accounts Relating to Individual Persons)
- Executive Order 9830 (Amending the Civil Service Rules and Providing for Federal Personnel Administration)
- Executive Order 12107 (Relating to the Civil Service Commission and Labor-Management in the Federal Service)

(c) Is the information searchable by a personal identifier (e.g., name or Social Security number)?  
Yes X No \_\_\_

If yes, provide:

- HRNet Applicable SORNs
  - Human Resources Records, State-31, July 19, 2013
  - Office for the Coordinator of Reconstruction and Stabilization Records, State-68, August 27, 2010.

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

(e) If no SORN is required, explain how the information is retrieved without a personal identifier?  
HRNet requires a SORN.

(f) Is there a records retention schedule approved by the National Archives and Records Administration (NARA) for this system? Yes X No \_\_\_  
(If uncertain about this question, please contact the Department's Records Officer at [records-dl@state.gov](mailto:records-dl@state.gov).)

The records in HRNet are subject to specific records disposition schedules published by the Records Management Division (A/GIS/IPS/RA) and OPM. The schedule for record disposition varies with record type. Retention and disposal of HRNet record types are specified in Domestic Records Disposition Schedule, Chapter A-04, Personnel and Foreign Records Disposition Schedule, Chapter B-07, Personnel. A/GIS/IPS/RA maintains the schedule including records in HRNet at the following url:

<http://infoaccess.state.gov/recordsmgmt/recdispsched.asp?cat=records#search>

The Department also follows the National Archives and Records Administration (NARA) General Records Schedule 1 (GRS-1) for Civilian personnel records supplemented as necessary to meet the specialized records management needs of the Department.

#### 4. Characterization of the Information

- (a) What entities below are the original sources of the information in the system? Please check all that apply.
- Individuals (U.S. citizens or legal permanent residents (LPRs))

- U.S. Government employees/Contractor employees/FSN
- Other

(b) Does the system collect, store, disseminate, or maintain PII? Yes X No \_\_\_\_

(c) If yes, what type of PII elements does the system use, collect, contain, maintain and/or disseminate?

The RNet website child application of HRNet does **not** use, collect, contain, maintain, or disseminate PII.

The following table addresses child systems or tools under HRNet that use, collect, maintain, and/or disseminate PII.

PII Elements	CRC	NSDD-38	Connect: Direct	EOD	GTS	HR Surveys
Full Name	X	X	X	X	X	
Date of Birth	X		X	X	X	
SSN	X		X	X	X	
Work/Home Address	X	X		X	X	
E-mail Address	X	X		X	X	X
Telephone	X	X		X	X	
Emergency Contact Information	X			X		
Diplomatic/Official Passport Numbers	X			X		
Visa Number	X			X		
Medical Clearance Level	X			X		
Department of State Badge Number	X					
Family Members	X			X		
Educational Information				X	X	
Insurance Information				X		
Individual Bank Account Information				X		

(d) If the system contains SSNs is the collection necessary? Yes X No \_\_\_\_

If yes, under what authorization?

Authorization for the Department to perform SSN collection comes from the following:

- 26 CFR 301.6109, Taxpayer identification;
- Executive Order 9397, Federal employment; and
- 20 CFR 10.100, Federal Workers' Compensation allow the Department to collect SSN for employment, payroll, tax identification and benefit purposes.

(e) How is the information collected?

Information is collected directly from applicants and members of the Federal workforce as a condition of employment by the Department of State or another Executive Branch agency.

- CRC is provided through the CRC interface by the CRC member, Response Corps Coordinator, or Corporate Staff.
- NSDD-38 information is collected from the requester who represents the external Executive Branch agency or Non-Governmental Organization (NGO), through the NSDD-38 interface.
- EOD information is collected through the EOD interface by the applicant user.
- Connect:Direct information is collected in the Department of Labor's Integrated Federal Employees' Compensation System (iFECS), which transfers data into HRNet.
- The GTS-MGS file transfer tool stores PII that is collected outside of HRNet in the source system USA Jobs website, which feeds into GTS.
- HR Surveys receives e-mail address lists including personal e-mail addresses from the organization requesting the survey.

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

- NSDD-38: M/PRI is the business owner for NSDD-38 and interacts directly with posts to validate information collected from the individuals.
- CRC: CSO validates information pertinent to CRC members through interaction with the member's parent Executive Branch agency.
- EOD: The applicant user has the opportunity and responsibility to verify his/her personal and demographic information in the EOD process and as needed to make changes to his/her profile. For eligible family members, as defined by 5 FAM 784-785, the employee is responsible for ensuring the accuracy of information.
- Connect:Direct: Accuracy is dependent on DoL which compiles the information.
- GTS – MGS file transfer: There is no user interface with GTS - MGS file transfer tool data. Accuracy is based on the user submission through USA Jobs and GTS.
- HR Surveys: E-mail address accuracy is dependent on the source of the individual providing the e-mail address. Accuracy is dependent on communication from the survey respondent or their organization affiliated with DoS to the organization issuing the survey.

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

- NSDD-38 information is kept current through M/PRI data management.
- CRC information is kept current through review by CSO.

- EOD applicant user information is kept current by the applicant and is maintained in HRNet until the applicant has completed the EOD process at which point it is purged from the system.
- Connect:Direct: DoL compiles information and is responsible for it remaining current.
- GTS – MGS file transfer: There is no user interface with GTS - MGS file transfer tool data. The user candidate is responsible for keeping their data current through USA Jobs and GTS.
- HR Surveys: The organization requesting the survey is responsible for providing a current e-mail address set at the start of the survey process.

(h) Does the system use information from commercial sources or is it publicly available information?

The system does not use information from commercial sources or publicly available information.

(i) Is notice provided to the individual prior to the collection of their information?

- A system use notification that includes a Privacy Act Statement is presented at the logon screen of the three HRNet applications that collect PII from employees (CSC, NSDD-38, EOD). Individuals may decline to provide some or all information; however, refusal may interfere with the provision of HR services or employment for the individual.
- Connect:Direct and the GTS-MGS file transfer are not the source of collection of PII from individuals.
- HR Surveys only maintains e-mail addresses and does not collect PII information.

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

- If yes, how are individuals granted consent?

Individuals may decline to provide some or all information; however, refusal may interfere with the provision of HR services to the individual. Though EOD will be the preferred method for provision of personal data required for HR records immediately prior to starting employment, the individual who has accepted an offer of an employment with DoS may opt for completion of handwritten paper forms to collect data. Refusal by a new user to provide minimally required data to HR may result in the employment offer being rescinded.

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

Individuals are granted consent to uses of the information.

(k) Did privacy concerns influence the determination of which information would be collected by the system?

Privacy concerns were considerations. However information collected are requirements of the business processes for the system.

## 5. Sharing and Use of information

(a) The purpose of collecting the information in this system is to:

HRNet supports the following mission and program objectives:

- CSC Application: To provide for a U.S. Government civilian capacity to prevent or prepare for post-conflict situations, and to help stabilize and reconstruct societies in transition from conflict or civil strife.
- NSDD-38 Application: To ensure the COM has control of the size, composition, and mandate of overseas full-time mission staffing for all U.S. Government agencies.
- Connect:Direct Client Tool: To support Department of State obligations under the DoL Worker's Compensation Programs.
- GTS – MGS File Transfer Tool: To support recruitment and employment of civil service applicants for DoS.
- EOD Application: To provide the new applicant with an automated means to provide required personal information and form completion to enable a more efficient in-processing on starting at DoS.
- HR Surveys: To provide a means to measure feedback from individuals affiliated with the State Department without access to a State e-mail address.

(b) The intended use for the information is:

CRC: The CRC system is used by CSO for tracking and reporting on CRC members and their missions. CRC members are a pool of qualified, trained, and ready-to-deploy civilian professionals who support overseas reconstruction and stabilization operations. The CRC system permits CRC members and partner agencies to input personnel and deployment information via a web-based interface

NSDD-38: The National Security Decision Directive 38 (NSDD-38), Staffing at Diplomatic Missions and their constituent Posts, dated June 2, 1982, gives the Chief of Mission (COM) control of the size, composition, and mandate of overseas full-time mission staffing for all Executive Branch agencies. The Under Secretary for Management's Office of Policy, Rightsizing, and Innovation (M/PRI) has the lead in managing requests by agencies for additions, deletions, and changes to their staffing overseas. The NSDD-38 application allows an external Executive Branch agency or Non-Governmental Organization (NGO) to request that a position be established at post. PII collected by NSDD-38 is limited to basic contact information of the requester including name, telephone, e-mail address, and office address to enable the requester to manage their agency's requests.

Connect:Direct Client Tool: The Connect:Direct Client Tool does not collect the information from the individual. The HRNet Connect:Direct client functions as a conduit to receive data from DoL. The data is then manually retrieved from HRNet, decrypted, and then uploaded into the integrated Personnel Management System (IPMS).

GTS – MGS File Transfer Tool: The GTS File Transfer Tool does not collect the information from the individual. HRNet functions as a conduit to receive data from Monster Government Solutions. The data is then manually retrieved from HRNet, decrypted, and then uploaded into IPMS.

EOD: The EOD system will provide easy data entry, standardized routing and processing in order to create a seamless user experience for DoS applicants and to avoid excess data entry for all participants involved. Each form appointee packet, as a standalone entity, requires a large amount of duplicate entry that is eliminated with the EOD system. EOD data will enable applicants for positions to complete required locator forms, benefit elections, direct deposit. Completion can be done remotely prior to the applicant's orientation and start date as a federal employee with DoS.

HR Surveys: Offices within HR have business requirements to gather survey information from their internal (OpenNet users) and external (non OpenNet users) customers. Personal e-mail addresses are resident in the HR Surveys database to enable contact and response from the survey sample.

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

The use of information is relevant to the purpose for which HRNet applications were designed. There are no collateral uses of the information outside the scope of the system.

- (d) Types of methods used to analyze the information are:

There is no analysis other than the standard reporting requirements.

- (e) Does the analysis result in new information? The new information is:

Standard reporting requirements are the only form of analysis. There is no analysis which produces new information.

- (f) Will the new information be placed in the individual's record? Yes \_\_\_ No  X

Standard reporting requirements are the only form of analysis. There is no analysis which produces new information.

- (g) 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  X

Standard reporting requirements are the only form of analysis. There is no analysis which produces new information.

- (h) With whom will the information be shared? Please identify the recipients of the information. Information internal to the Department is used by the following.

- NSDD-38 is used by M/PRI. M/PRI is the business owner of NSDD-38 and responsible for the administration and authentication of user accounts. M/PRI manages requests by other U.S.

government agencies for additions, deletions, and changes to their staffing abroad. Data is hosted on the HR maintained infrastructure and not shared outside HR systems.

- CRC is used by the Bureau of Conflict and Stabilization Operations (CSO). For tracking and reporting on members. Data is hosted on the HR maintained infrastructure and not shared outside HR systems.
- Connect:Direct Client Information is shared with the HR Office of Employee Relations (HR/ER).
- GTS information is shared with the HR Office of Recruitment, Examination, and Employment (HR/REE).
- EOD data is directly transferred to HR's GEMS and eOPF child applications of IPMS. The IPMS PIA details the requirements, collection, and security of personal data shared by GEMS and eOPF with other Department bureaus and U.S. government agency.
- HR Surveys personal e-mail address lists are managed by the organization requesting the survey.

(i) What information will be shared?

Information collected through HRNet and transferred to IPMS and its GEMS and EAPS child applications where it may be shared to the following Bureaus through GEMS and EAPS:

- Foreign Service Institute (FSI)
  - IPMS shares employee, position, salary, location, and organization data.
- Bureau of the Comptroller and Global Financial Services (CGFS)
  - IPMS shares employee salary and benefits information.
- Bureau of Diplomatic Security (DS)
  - IPMS shares employee and applicant information.
- Administration (A) Bureau
  - IPMS shares employee information.

Information transferred to HR/REE includes personal data related to employment qualifications, background, and contact information of the individual.

Information transferred to HR/ER includes personal data related to job-related injury and associated worker's compensation claims.

(j) The purpose for sharing the information is:

- The purpose of HRNet information shared with internal Bureaus is the following:
  - FSI – supporting the employee training process.
  - CGFS – supporting the payroll process.
  - DS – supporting the security clearance process.
  - A – Supporting the employee travel, logistics, and parking processes.
- The purpose of HRNet information shared with HR/ER is to support the Office of Workers' Compensation Programs (OWCP) to trend, report, and manage the performance of its worker

safety and health program under the Secretary of Labor's, Safety, Health and Return-to-Employment (SHARE) Initiative.

- The purpose of HRNet information shared with HR/REE is to evaluate the application for efficiency in the process of identification and selection of qualified candidates to fill recruitment and staffing needs for the DoS mission.

(k) The information to be shared is transmitted or disclosed by:

Information is shared by secure network transmission methods permitted under Department policy for the handling and transmission of SBU information including Transport Layer Security (TLS) v1.0 and Secure Sockets Layer (SSL) v3.1. Data from HRNet is first transferred to OpenNet and the IPMS system before sharing with other bureaus. OpenNet is also a dedicated Department network for the secure transmission of Sensitive But Unclassified information among Department of State component offices, domestic and overseas. All passwords for HRNet comply with DS security guidelines. All IT systems on OpenNet must be fully certified and accredited as required by the Federal Information Security Management Act (FISMA).

Data sharing is fully explained in the HRNet System Security Plan (SSP), Section 2.9.3, System Data Sharing. Most connections are automated between servers with other Department bureaus within IRM managed OpenNet. Methods of data sharing include Oracle database sockets, flat text file transfer, SQL table transfer, XML file transfer, and secure ftp.

(l) What safeguards are in place for each sharing arrangement?

HRNet PII is disclosed only to authorized users based on their roles as defined in the HRNet SSP. External agency representatives who require access to HRNet must comply with the application access process to request an account. Users who are granted access are only allowed to view or edit information which they are assigned sufficient access rights based on a need to know. Need-to-know is determined based on a decision of the business owning organization (M/PRI for NSDD-38, CSO for CRC, HR for EOD and file transfers).

HRNet relies on network security control through IRM/ENM operation and restrictions in a Demilitarized Zone (DMZ) infrastructure. Users external to the department are only permitted access to the web servers based on internal account management. NSDD-38, CRC, and EOD applications include databases separated through network and firewall segmentation into a database DMZ from the web servers. Authorized users for each HRNet application do not have access to these databases. Application servers make calls to these databases, and only privileged system administrators and database administrators have direct access.

Other HRNet infrastructure including application servers and databases are restricted to access through network and firewall isolation in a private application DMZ and a database DMZ controlled by IRM/ENM. Application servers and database servers contain only privileged accounts for HR/EX/ESD system and database administrators. Application administrators for

NSDD-38 are limited to authorized M/PRI staff. Application administrators for CRC are limited to authorized CSO staff. EOD application administration is performed by HR/EX/ESD.

(m) What privacy concerns were identified regarding the sharing of the information? How did the Department address these concerns?

The HRNet System Security Plan delineates responsibilities and expected behavior of all individuals who access HRNet applications. In addition, the Department of State has implemented the “Rules of Behavior for Protecting Personally Identifiable Information” policy, dated October 6, 2008. The Department of State Rules of Behavior are applicable to all employees and contractors, and cover all Department of State records, regardless of format that include PII, in addition to Department of State Components.

In addition HRNet only utilizes authorized technology approved by the Department of State IT Configuration Control Board or HR’s internal bureau Configuration Control Board. Internal access to data is only available to authorized users who are cleared government employees/contractors. The information is used in accordance with the stated authority and purpose. Minimum risks to privacy are mitigated by granting access only to authorized persons with a need-to-know.

HR employs a significant number of layered technical controls to prevent the misuse or improper disclosure or access to PII data. These controls include but are not limited to:

- HRNet is hosted in the IRM managed DMZs for boundary protection in restrictions on network accessibility and connections between servers. Web servers are hosted in the Public Web DMZ. Application servers are not accessible from the Internet and are segregated in a Private Application DMZ. Database servers are not accessible from the Internet and segregated in the Database DMZ.
- Operational and Technical controls include a predefined number of failed attempts and lockout, and server event logging.
- Identification and authenticator restriction with documented need-to-know privileges assigned to roles based on application and position.

The EOD application specifically enforces the separation of duty whereby the Applicant User may only access their own information. The Applicant User is able to create and access only their individual personal information in required forms for the EOD process. They will be able to save incomplete forms and return to complete the forms. Once the Applicant User submits the EOD package and their package is accepted, their data is purged from the DMZ database and the Applicant User access to EOD is revoked.

## **6. Redress and Notification**

(a) What procedures allow individuals to gain access to their information?

HRNet users may amend contact information and personal identification information they believe to be incorrect.

(b) Are there procedures in place to allow an individual to correct inaccurate or erroneous information? Yes X No \_\_\_\_\_

If yes, explain the procedures.

System of Records Notices STATE-31 and STATE-68 provide guidance for record access and amendment procedures. Individuals who wish to gain access to or amend records pertaining to themselves, should write to the Director General of the Foreign Service and Director of Human Resources; Department of State; 2201 C Street, NW; Washington, DC 20520. Additionally, the HR Help Desk may be contacted by phone or e-mail as an initial step if an individual finds incorrect information in their personnel record in an HRNet application. The HR Help Desk may be contacted by phone at (202) 663-2000 or e-mail at [hrhelpdesk@state.gov](mailto:hrhelpdesk@state.gov).

EOD users may correct their own PII in data fields within the application while completing forms for the EOD process. If they notice inaccurate or erroneous information, they may correct this before submitting their information

Pursuant to 5 U.S.C. 552a (k)(5) and (k)(7), certain records contained within this system contain confidential source information and are exempt from 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). Pursuant to 5 U.S.C. 552a (k)(6), records that contain testing or examination material the release of which may compromise testing or examination procedures are also exempt from 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (H) and (I), and (f). See Department of State Rules published in the Federal Register.

(c) By what means is an individual notified of the procedures to correct their information?

The individual is notified of the procedures to correct their information through response from the contacts in the SORN as stated in section 6b above.

## 7. Security

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

The information in HRNet is secured through implementation of the minimum baseline of controls for a Moderate impact system for confidentiality, integrity, and availability. Security controls are specific to HRNet control descriptions in NIST SP 800-53. Access to the application from an end user and user with elevated privileges are controlled by the application administrators. Application identifiers and authenticators are provisioned based on the NIST SP 800-53 and State requirements. The server operating system, web servers, applications, and databases are configured according to State DS Secure Configuration Standards and best practices. Account privileges are based on roles with the concept of least-privilege and need-to-know. IRM/ENM manages DMZs for increasing levels of restrictions for access and visibility over the network for each of the web servers, application servers, and database servers. Full details of security control implementation are found in the HRNet System Security Plan.

(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.

Full information on assignment of users to roles is documented in the HRNet System Security Plan. Role assignment is controlled based on application. NSDD-38 user account applications are assessed and granted by M/PRI analysts. CRC user account application and role assignment are assessed and granted by CSO. External access to EOD is granted by HR Specialists for new user applicants. HR Specialist roles are required as part of the job function to manage the EOD process.

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

Each server in HRNet is configured with DS issued secure configuration standard or equivalent auditing of system and database activity including successful and failed logins, account creation, and account modification. Audit logs are reviewed monthly by the ISSO. The ISSO and System Administrators regularly review and analyze audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, and report findings per 12 FAM 621. HRNet servers as hosted in the IRM/ENM DMZ rely on firewall network access control and network intrusion detection.

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

The Department of State's appropriate use policy and rules of behavior are the general terms under which federal employees and contractors use HRNet. The Department of State requires all new employees and contractors to complete Computer Security Awareness and Training (CSAT) provided by DS/SI, before or immediately after the employment start date and prior to being granted access to the system. In addition, the OpenNet account request form signed by all employees and contractors who will also have access to HRNet includes a "Computer Security Awareness Form" that includes privacy orientation. All Department of State personnel must complete refresher training yearly. Access to data is limited to cleared U.S. Government employees/contractors administering the system who meet "official" need-to-know criteria. As future State employees, EOD Applicant Users do not have accessibility to complete Privacy training. However, Applicant User accounts are only granted access to their individual information, which conveys negligible risk as authorized users of their own information.

(e) Are there any security controls such as encryption, strong authentication procedures, or other controls in place making the information unusable to unauthorized users? Yes  No

Transmission of data from the Internet for web (https) sessions uses encryption through SSL and/or TLS protocols. Files transferred into HRNet through the Connect:Direct are encrypted using TLS and remain encrypted at rest until pulled into IPMS by an Connect:Direct user. Two-factor authentication through an out-of-band token and password is in place for the EOD application.

(f) Can this system be accessed remotely? Yes  No

- Is two-factor authentication used? Yes  No

- Is the remote access accomplished via a virtual private network (VPN)? Yes  No

(g) How were the security measures above influenced by the type of information collected?

The security measures above were influenced by the baseline requirements for a system with moderate impact rating for confidentiality, integrity, and availability. HRNet followed the data categorization procedures for confidentiality, integrity, and availability based on Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. Additionally, the DoS IRM/IA Security Categorization Form (SCF) and eAuthentication Risk Assessment guides were used to determine the overall impact and eAuthentication levels of each HRNet application. NIST SP 800-53 security controls for a moderate system were included in the design and operation of HRNet. In particular, the PII data influenced the application of the controls from the following families: access control, audit and accountability, identification and authentication, system and communications protection, and system and information integrity control families.

**8. Access**

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

The following system user definitions describe the roles and access. User access is specific to each child application or component of HRNet with independent application identification and authentication controls. All HRNet systems have system administrators with privileges to maintain the servers. System administrators are authorized as HR/EX/ESD system support. NSDD-38, CRC, and EOD also have database administrators from HR/EX/ESD with elevated privileges to maintain the databases.

**NSDD-38**

System Users	Roles and Responsibilities
Individuals (Requesters) who work for other USG agencies and NGOs	This user role will have access to data for their specific agency and all its Posts. Once a request is approved, an authorized user can then create position requests at Post.

**CRC**

System Users	Roles and Responsibilities
CRC System Administrator	This role permits a user from the CSO to administer data and user permissions. The system admin user role has access to all data and is responsible for reviewing, creating and generating report and query functions. Other responsibilities include the review of data for consistency and validation, and the use of data elements to populate training, medical and personnel forms as required.
CSO Administrator (limited)	This role permits a CSO user to report, track and mobilize CRC personnel across all partner agencies for deployment. Responsible for generating formal reports for upper management, Congress and other government agencies. Review records for data integrity and set enhancements for future reporting requirements. Responsible for setting standards and requirements for automated e-mail generation for CRC member tasks (medical, passport, training and other administrative updates as required). This role has

System Users	Roles and Responsibilities
	access to all partner agency, employee, deployment and regular data and historical data. Access to edit training, medical and deployment forms as required.
Response Corps Coordinator (RCC)	This role is assigned to a partner agency representative to manage their CRC employee data. The user role is responsible for administrative review and process flow for CRC members from their respective agency. The RCC also approves training requests and performs other administrative tasks for agency CRC members. The RCC user role does not have access rights to private data but is able to review employee data (such as country and language experience) in a CRC member's record. Access to edit training, medical and personnel forms as required. RCCs are required to notify the Director of CRO of a non-CRC deployment (TDY).
CRC Employee	This user role permits a CRC employee to add, edit, and view their personal CRC data. This user role is currently limited to employees of the partner agencies or retirees (re-employed annuitants) who are in the Standby component and may only have a private email address and not a USG account. However, eventually Reserve CRC members may be from the private sector. The CRC Employee user role has the ability to edit training, medical and personnel forms as required.
Corporate staff	This role is for corporate employees from any partner agency who frequently deploy but are not in the CRC. Corporate staff should have the same permissions as a CRC employee in order to edit their own data. Corporate staff may or may not be direct USG employees. They could also be private sector contractors or Personal Service Contractors (PSCs) (which are often used at USAID).
Travel Coordinators	This user role is for travel coordinators in Mission Support, CSO's Travel Unit and the Civilian Deployment Center, who will make travel arrangements for CRC members and need access to the database in order to gather information for the e-country clearances or booking flight tickets. They would need read-only permissions to PII, such as DOB, SSNs, Passport Numbers, and Emergency Contacts.
Mission Support/Civilian Deployment Center staff	This user role is for deployment liaisons who manage active deployments either through CSO's Mission Support or through USAID's Civilian Deployment Center (CDC). This user role is to have permissions to view and edit all deployment-mission non Personally Identifiable Information (non-PII) to include as sizing information.
Training Department Administrators	This user role is for persons who need access to the system to approve training requests and requires access to OpenNet. They shall have view access to the data for CRC Members. This role permits a training department CSO user to view the essential "training" elements of CRC personnel, but not more than needed. Relevant training information that is to be viable by this user role, includes a person's name, contact information, availability, agency, CRC component, technical skills, country and language experience, status of training application, and completed and planned training information. Training Department Administrators are also responsible for executing ad hoc reports of current attendance lists, past attendance lists, statistics on training. If needed, this user role is also able to execute database queries to search for available people to take future courses.

**EOD**

System Users	Roles and Responsibilities
Applicant User	<p>This role permits a DoS applicant user to access the applicant interface from the Internet. The Applicant User is a person selected for a position in any one of the various programs offered by the Department of State including: Foreign Service Specialist, Foreign Service Generalist, Student, Civil Service, Presidential Appointments, Re-employed annuitants, EFMs (Eligible Family Members), SES (Senior Executive Service), LES (Locally Employed Staff), EPAP (Expanded Professional Associates Program), and Limited Non-Career Appointments.</p> <p>The Applicant User is able to create and access only their individual personal information in required forms for the Entrance on Duty process. They will be able to save incomplete forms and return to complete the forms. Once the Applicant User submits the EOD package and their package is accepted, their data is purged from the DMZ database and the Applicant User access to EOD is revoked.</p>
EOD Administrator	<p>This role is only granted to HR DoS employees. The EOD administrator refers to an application administrator. EOD administrators may perform account management functions at the highest level. EOD Administrators will be able to restore archived data into the EOD database for analysis. The EOD administrator authenticates to the Global Employment Management System (GEMS) system through their OpenNet Active Directory account.</p> <p>This role is responsible for granting and removing the HR Specialist and the Benefits Processor User roles in the EOD system.</p>
HR Specialist	<p>This role is only granted to HR Specialist DoS employees. The HR Specialist role initiates and manages the process to create an invitation and account for the Applicant User. The HR Specialist authenticates to the Global Employment Management System (GEMS) system through their OpenNet Active Directory account. The HR Specialist is allowed to view, modify, and delete forms for new applicants and is the approver of the EOD package. The HR Specialist user is able verify, send to Payroll, the eOPF and print all necessary information being done or submitted by EOD User.</p> <p>The HR user can send back the selected core/benefits information submitted by the Applicant User to be corrected if the Applicant has not completed the forms properly. The HR Specialist may terminate an EOD process and disable an account of a specific Applicant. The HR Specialist initiates the purge process which transfers the EOD package onto the GEMS system and deactivates the Applicant User account.</p>
Benefits Processor	<p>The Benefits Processor user is able to view, verify, send to Payroll, eOPF, and print all necessary information being done or submitted by the Applicant User. The Benefits Processor user can send back the selected benefits information submitted by the Applicant User to be corrected if the employee has not completed the forms properly. The Benefits Processor user authenticates to the GEMS system through their OpenNet Active Directory account.</p>

**Connect:Direct Client Tool**

System Users	Roles and Responsibilities
--------------	----------------------------

Connect:Direct System Administrators	This role permits a user to administer data and user permissions, as well as to restrict privileges. The system admin user role has access to all data, and is responsible for reviewing, creating and generating report and query functions. This user role issues the Copy Receive, Copy Send, Run Job, and Run Task processes. For a complete list of default privileges, refer to page 9 of the <i>Connect:Direct for Windows, System Guide</i> Version 4.5.01.
General Users	This role permits a user to access data to which permission has been granted. General users are responsible for reviewing, creating and generating report and query functions. This user role issues the Issue the Copy Receive, Copy Send, Run Job, and Run Task processes. For a complete list of default privileges, refer to page 9 of the <i>Connect:Direct for Windows, System Guide</i> Version 4.5.01.

**Gateway to State - MGS File Transfer Tool**

System Users	Roles and Responsibilities
System Administrators	This role permits a user to administer data and user permissions, as well as to restrict privileges at the OS level. The System Administrator has complete access to the MGS server. MGS does not have other non-privileged users. The system administrator is responsible for download of files sent via secure ftp to this server from MGS.

**HR Surveys**

System Users	Roles and Responsibilities
Web Application Administrators	This is a privileged role granted only to the HR/EX/ESD/CSB Web Operations Team Administrators. The function of this role is to create survey questions from HR customer requirements and manage the survey response file.
System Administrators	This role permits a user to administer data and user permissions, as well as to restrict privileges at the OS level. The System Administrator has complete access to the HR Surveys servers, including user administration permissions.

(b) Access to data in the system is determined by the individual’s organization, role and authorized responsibility.

- Access to data is determined by roles as defined in the HRNet SSP. Privileged system administration and database administration roles are assigned within HR/EX/ESD in line with job function. Application specific access is determined by organization membership.
- NSDD-38 users must have the role of requesting positions under COM at posts for their representative USG or NGO.
- CRC users must be members of the CRC or have a role in preparing for and executing the activation of CRC deployment.
- EOD users are external New Applicants awaiting start of employment or internal Department HR specialists in charge of the EOD process from initiation to approval of the EOD package.
- Connect:Direct and GTS users are limited to those HR/EX/ESD system administrators who control file transfers and are necessary tasks for their position.

- HR Surveys users only view a web page with the survey information. They do not access the database which contains survey respondent e-mail addresses.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

Yes X No \_\_\_\_\_

(d) Will all users have access to all data in the system or will user access be restricted? Please explain.

Users have access restricted to data based on their individual role and privileges granted. Each application has application specific identifiers and authenticators not recognized by the other HRNet applications. See section 8a above and the HRNet System Security Plan for full breakdown of access restrictions based on roles.

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

Access is restricted by application and roles within each application. Full description of roles and permissions for each HRNet application with end user access is provided in Section 8a above. Data access is limited on a least privilege and need-to-know restriction for each role. End users in CRC and EOD are limited to viewing their own personal information.