

***Human Resources Network (HRNet)***  
***(iMATRIX NUMBER 866)***

**Privacy Impact Assessment 2017**

**1. Contact Information**

<p><b>A/GIS Deputy Assistant Secretary</b> Bureau of Administration Global Information Services</p>
---

**2. System Information**

- (a) Name of system: Human Resources Network
- (b) Bureau: Human Resources (HR)
- (c) System acronym: HRNET
- (d) iMatrix Asset ID Number: 866
- (e) Reason for performing PIA: For security reauthorization of the system. Some information has changed in HRNET since the last PIA conducted in 2014.
  - New system
  - Significant modification to an existing system
  - To update existing PIA for a triennial security reauthorization
- (f) Explanation of modification (if applicable): Since the last authorization there has been an update to the Point of Contact and server information, and the removal of the Civilian Response Corps (CRC) System, Gateway to State (GTS) and Connect systems.

**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?  
Authorization to Operate (ATO) expires January 31, 2018
- (c) 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 both Civil Service and Foreign Service employees 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 NGOs. 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.
- 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.

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

The RNet website (a static informational website), a 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	NSDD-38	EOD	HR Surveys
Full Name	X	X	
Date of Birth		X	
SSN		X	
Work/Home Address	X	X	
E-mail Address	X	X	X

Telephone	X	X	
Emergency Contact Information		X	
Diplomatic/Official Passport Numbers		X	
Visa Number		X	
Medical Clearance Level		X	
Family Members		X	
Educational Information		X	
Insurance Information		X	
Individual Bank Account Information		X	

(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 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)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- SORN Name and Number:  
Human Resources Records, State-31, July 19, 2013  
Office for the Coordinator of Reconstruction and Stabilization Records, State-68, August 27, 2010.
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): July 19, 2013; August 27, 2010

No, explain how the information is retrieved without a personal identifier.

[Click here to enter text.](#)

(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 uncertain about this question, please contact the Department's Records Officer at [records@state.gov](mailto:records@state.gov).)

If yes provide:

Schedule Number: A-04-004-03b

Length of time information retained in system: TEMPORARY. Destroy when active agency use ceases. (NC1-59-83-4, item 25b)

Type of information retained in system: Personnel Records

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.
- 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

- 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.

- (c) How is the information collected?

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

- NSDD-38 information is collected from the requester who represents the external Executive Branch agency or Non-Governmental Organization (NGO), through the NSDD-38 web form.
- EOD information is collected through the EOD web form by the applicant user.
- Offices within HR have business requirements to gather survey information from their internal (OpenNet users) and external (non OpenNet users) customers. HR

Surveys receives e-mail address lists from the organization requesting the survey and HR survey system sends the electronic survey to the email addresses provided.

(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.

[Click here to enter text.](#)

(e) 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.
- 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.
- 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.

(f) 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.
- 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.
- HR Surveys: The organization requesting the survey is responsible for providing a current e-mail address set at the start of the survey process.

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

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

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

- A system use notification that includes a Privacy Act Statement is presented at the logon screen of the two HRNet applications that collect PII from employees (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.

- HR Surveys only maintains e-mail addresses obtained from organizations. Since the information is not collected directly from the individual, notice is not provided at this stage.

(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?

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?

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

[Click here to enter text.](#)

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

Privacy concerns were considerations. However information collected are requirements of the business processes for the system. As such only the minimum amount of information required to perform these functions is collected.

## **5. Use of information**

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

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.

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, and 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.

(b) 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.

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

There is no analysis other than the standard reporting requirements.

If yes:

(1) What types of methods are used to analyze the information?

[Click here to enter text.](#)

(2) Does the analysis result in new information?

[Click here to enter text.](#)

(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.

- 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.
- EOD data is directly transferred to HR's GEMS and eOPF child applications of Integrated Personnel Management System (IPMS). The IPMS PIA details the requirements, collection, and security of personal data shared by GEMS and eOPF

with other Department bureaus and Office of Personnel Management (OPM). Other Department Bureaus include:

- Foreign Service Institute (FSI)
- Bureau of the Comptroller and Global Financial Services (CGFS)
- Bureau of Diplomatic Security (DS)
- Administration (A) Bureau
- HR Surveys' personal e-mail address lists are managed by the HR organization requesting the survey.

**(b) What information will be shared?**

Information collected through EOD and transferred to IPMS, and its GEMS and EAPS child applications, may be shared with 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.

In addition to the position request, NSDD-38 shares information (name, email address and phone number) about the requester and point of contact with M/PRI using Transport Layer Security (TLS) for confidentiality.

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

- The purpose of HRNet information shared with internal Bureaus is the following:
  - FSI – Supports the employee training process.
  - CGFS – Supports the payroll process.
  - DS – Supports the security clearance process.
  - A – Supports the employee travel, logistics, and parking processes.

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

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) v1.2. Data from HRNet is first transferred via OpenNet to 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 the Bureau of Information Resource Management (IRM) managed OpenNet. Methods of data sharing include Oracle database sockets, flat text file transfer, SQL table transfer, XML file transfer, and secure ftp.

**(e) What safeguards are in place for each internal or external 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, 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 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. EOD application administration is performed by HR/EX/ESD.

**(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?**

Privacy concerns identified include access to PII including name, email address and phone numbers. 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. 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. 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 are 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 his/her 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.

## **7. Redress and Notification**

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

EOD Administrator sends a link to EOD user to submit their information. EOD user can only access their information through the link sent by EOD Administrator.

HRNET user accounts are deleted from DMZ after submission. HRNet users may only amend contact information and personal identification information they believe to be incorrect using the link sent to them by EOD Administrator.

Administrators are the only users that have access to NSDD-38. Administrators can edit their information in the system.

- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes  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 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

If no, explain why not.

Click here to enter text.

- (c) By what means are individuals 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.

## **8. Security Controls**

- (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. 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 Cyber Security Awareness Course (PS 800) provided by DS/SI, 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 Cyber Security Awareness Course yearly. Additionally all Department employees are required to take PA459-Protecting Personally Identifiable Information.

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 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.

Transmission of data from the Internet for web (https) sessions uses encryption through TLS protocols for all HRNET systems. Two-factor authentication through an out-of-band token and password is in place for the EOD application.

- (f) 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 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.

9. Data 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 and EOD also have database administrators from HR/EX/ESD with elevated privileges to maintain the databases.

NSDD-38

System Users	Roles and Responsibilities
<b>System Administrator</b>	The System Administrator has complete access throughout the NSDD-38 website, including user administration permissions.
<b>Individuals (Requesters) who work for other USG agencies and NGOs</b>	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.

**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, EFM's (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>

**HR Surveys**

System Users	Roles and Responsibilities
Web Application Administrators	<p>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</p>

	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) How is access to data in the system determined?

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 Chief of Mission (COM) at posts for their representative USG or NGO.
- 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.
- 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  No

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

Users have restricted data access 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 for full breakdown of access restrictions based on roles.

(e) What controls are in place to prevent the misuse (e.g. 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 by a least privilege and need-to-know restriction for each role. End users in EOD are limited to viewing their own personal information.