PRIVACY IMPACT ASSESSMENT

Human Resource Network (HRNet) PIA

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Date of completion of this PIA: July 2021
(b) Name of system: Human Resources Network
(c) System acronym: HRNet
(d) Bureau: Global Talent Management (GTM/EX)
(e) iMatrix Asset ID Number: 866
(f) Child systems (if applicable) and iMatrix Asset ID Number:

Entrance of Duty (EOD) - 66451
National Security Decision Directive (NSDD-38) - 165
Retirement Network Alumni Organization Site (RNET) - 2166
Candidate Tool (CT) Survey - 318750

(g) Reason for performing PIA:

☐ New system
☐ Significant modification to an existing system
☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒ Yes ☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒ Yes ☐ No

If yes, has the privacy questionnaire in Xacta been completed?
☒ Yes ☐ No

(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 and 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 child systems:

- **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 the Department offers to active employees and annuitants. RNet 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 a workspace and a variety of services at posts to individuals who work for other USG agencies as well as some non-governmental organizations (NGOs). 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. While NSD-38 is a child system of HRNET, the business owner of the system is the Office of Management Strategy and Solutions (M/SS).
- **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.
- **Candidate Tool (CT) Survey**: CT is an electronic survey system that allows peers, subordinates, and supervisors of Chief of Mission (COM), Deputy Chief of Mission (DCM), and Principal Officer (PO) candidates to complete a questionnaire about that candidate's leadership qualities, management abilities and policy skills. The CT Survey is used to support the Deputy and DCM committee selection processes for COM/DCM/PO and Minister Counselor-level Office of the Coordinator of the Foreign Policy Advisor Program (PM/POLAD) positions during the assignment cycles. Questionnaire responses are confidential, and the information in the resulting reports is not attributable to any single participant.

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

The HRNet web portal infrastructure does not collect PII directly. Rather, it either provides information or collects information via the following:

The RNet website (a static informational website), a child application of HRNet does not use, collect, contain, maintain, or disseminate PII.

The NSDD-38 system collects full name, work address, home address, government email address, and either personal or work telephone number.

The EOD system collects full name, date of birth, social security number (SSN), work address, home address, personal and government email address, either personal or work telephone number, emergency contact information, diplomatic/official passport numbers, visa number, medical clearance level, family members' information, educational information, insurance information, and individual bank account information.

The CT Survey system collects full name and personal and government email address.

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

- 22 U.S.C. 2581 (General Authority of Secretary of State)
- 22 U.S.C 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, etc.)?

☒ Yes, provide:

- SORN Name and Number:

- Human Resources Records, STATE-31
- Office for the Coordinator of Reconstruction and Stabilization Records, STATE-68

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

- STATE-31, July 19, 2013
- STATE-68, August 27, 2010

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

(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 Office at 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.)

If yes provide (Consolidate as much as possible):
- Schedule number (e.g., (XX-587-XX-XXX)): A-04-004-03b
- Disposition Authority Number: N1-059-00-08 item 4b, NC1-59-83-4, item 25b
- Length of time the information is retained in the system:
  Temporary. Destroy when active agency use ceases.
- Type of information retained in the system:
  Personnel records. The Department also follows the National Archives and Records Administration (NARA) General Records Schedule 2 (GRS-2.2) Employee Management 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) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒ Yes ☐ No ☐ N/A

- If yes, under what authorization?
  - 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.

(d) How is the PII 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 NGO, through the NSDD-38 User Registration web form.
- EOD information is collected through the EOD User Registration web form by the applicant.
- CT Survey – The candidate/bidder enters the names and email addresses of the individuals they would like to assess them into CT Survey. A standardized email is then generated and sent to each of the assessors. The assessors log into the system and answer the questions about the candidate. The answers and the reference's name and email are collected in the application.

(e) 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.

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

- NSDD-38: The Office of Management Strategy and Solutions (M/SS) is the business owner for NSDD-38 and interacts directly with posts to validate information collected from the individuals.
- EOD: The applicant 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 Foreign Affairs Manual chapter 5 FAM 784-785, the employee is responsible for ensuring the accuracy of information.
- CT Survey - The accuracy of the name and email is the responsibility of the candidate.

(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/SS data management.
- EOD: Applicant 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.
- CT Survey – The candidate/bidder is responsible for keeping their information current.

(h) 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.

(i) How was the minimization of PII in the system considered?

The system owner, HR specialist and system ISSO work together to review the fields collected from applicants. All efforts are made to ensure that only the necessary PII elements are collected and stored by the system. These elements include PII needed to verify the applicant's identity, ensure no duplication of applicant records in the system, verify eligibility of applicants, contact applicants throughout the hiring process, and initiate on-boarding activities.

5. Use of information

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

NSDD-38: NSDD-38 application allows an external Executive Branch agency or NGO to request that a position be established at post. PII collected by NSDD-38 is limited to basic contact information of the requester, as listed in 3d, that enables the requester to manage their agency's requests.

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

CT Survey – The Candidate Tool (CT) is an electronic survey system that allows peers, subordinates, and supervisors of COM/DCM/PO candidates to complete a questionnaire about that candidate's leadership qualities, management abilities and policy skills. The candidate/bidder enters the name and email of the references. The reference email is used to send the questionnaire to the reference for additional information.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes. 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 PII stored in it? ☐ Yes ☒ No

If yes:

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

(2) Does the analysis result in new information?

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

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

(d) If the system will use test data, will it include real PII?

☒Yes ☐No ☐N/A

If yes, please provide additional details.

NSDD-38 - User-provided registration data (including name, email, phone number, fax, and organization title) are accessible to testers through an administration screen to test system administrator functionality. The testers assess the functionalities that will approve user access to the system and are able to add, remove, and update the user registration data. The test results do not change production access, and production is overwritten monthly.

EOD – The EOD testing environment contains data fields that are required for HR Specialist to accurately test their information, including name, address, benefits, email, phone number, fax, and organization title. The EOD test data are accessible to GEMS Security testers so they can perform system administrator functionality by logging in as different employees. The functional testers add or update information in the hire templates, review tax forms, and send out offer letters.

CT Survey –User-provided data (including name and email) are accessible to testers through administration screens where testers can test system administrator functionality. The testers may create candidate and/or assessor users. The assessors fill out survey about the candidates.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:

- NSDD-38: While GTM is the system owner for NSDD-38, M/SS is the business owner. M/SS directly accesses the data in NSDD-38, which is maintained by GTM . As the business owner M/SS, administers and authenticates user accounts. M/SS also

manages requests by other U.S. government agencies for additions, deletions, and changes to their staffing abroad. This internal sharing is between Bureaus at the Department of State, and not between systems. Data hosted on GTM-maintained infrastructure are not shared outside GTM systems.
- EOD: Data are shared with GTM's Integrated Personnel Management System's (IPMS) child applications: Global Employment Management System (GEMS) and Electronic Official Personnel File (eOPF).
- CT Survey: The Office of Organization and Talent Analytics (OTA) within GTM does not share PII data in CT Survey internally or externally.

External:
N/A

(b) What information will be shared?

Internal:
- NSDD-38 shares information (name, email address and phone number) about the requester and point of contact with M/SS. Position request may also be shared.
- EOD shares employee information such as position, salary, location, benefits information, organization data as well as applicant information with IPMS.

External:
N/A

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

Internal:
- NSDD-38: Information is shared to support staffing changes at U.S. missions abroad.
- EOD: Information is shared to support the employee training, payroll, security clearance, employee travel, logistics, and parking processes.

External:
N/A

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

Internal:
- NSDD-38: Information is shared with M/SS by secure network transmission methods permitted under Department policy for the handling and transmission of SBU information including Transport Layer Security (TLS) v1.2.
- EOD - Data from EOD are transferred via OpenNet to IPMS and its child applications. There are custom app engine processes in GEMS that push or pull data from GEMS to/from the EOD instance in the Demilitarized Zone (DMZ). This is done via Oracle DB link, using the encryption and security for Oracle DB link.

External:
N/A

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

Internal:

- NSDD-38 – NSDD-38 has front end – website or user interface – installed on both DMZ and OpenNet. Both interfaces read and write data to the same database but M/SS can only accesses the data using the OpenNet front end. The PII data are accessed on demand one record at time and the transmitted data are not stored on OpenNet. The data transmission process is electronic, fully automated, and encrypted. Only a few individuals have privileges to access PII data. M/SS system administrators control the access. Application administrators for NSDD-38 are limited to authorized M/SS staff.
- EOD - Using the encryption and security for Oracle DB link, GEMS automatically pushes or pulls data from GEMS to/from the EOD instance in the DMZ. EOD application administration is performed by GTM/EX/ESD.

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

HRNet relies on network security control through IRM/Enterprise Network Management (ENM) operations and restrictions in a Demilitarized Zone (DMZ) infrastructure.

External:
N/A

7. Redress and Notification

(a) Is notice provided to the record subject 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 NSDD-38 and EOD, the two HRNet applications that collect PII from employees. Individuals may decline to provide some or all information; however, refusal may interfere with the provision of HR services or employment for the individual. CT Surveys does not collect personal email addresses directly from the public or individuals. Rather, personal email addresses are provided for proposed assessors or references by individuals who are being evaluated through the CT survey process. For this reason, a Privacy Act statement or notice prior to collection of information is not required.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☒ Yes ☐ No

If yes, how do record subjects grant consent?

By completing the registration forms, users consent to the collection and storage of their PII.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

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

NSDD-38 users can access their own information by logging directly into the system. Administrators are the only users that have access to everyone's information in NSDD-38.

Record subjects are not able to gain access to their information within CT Survey.

(d) Are procedures in place to allow a record subject 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 Global Talent Management; Department of State; 2201 C Street, NW; Washington, DC 20520.

Additionally, the GTM 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 the HRNet application. The GTM Help Desk may be contacted by phone at (202) 663-2000 or e-mail at hrhelpdesk@state.gov.

NSDD-38 users may correct their own PII via User Information link within the system.

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.

(e) By what means are record subjects notified of the procedures to correct their information?

Individuals are notified of procedures to correct their information by contacting their HR Specialist within the HR Service Center (HRSC) via email.

8. Security Controls

(a) How is all of 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 DoS requirements. The server operating system, web servers, applications, and databases are configured according to DoS 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) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

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 GTM/EX/ESD system support. NSDD-38 and EOD also have database administrators from GTM/EX/ESD with elevated privileges to maintain the databases.

There are no roles created to provide access to RNet.

NSDD-38

- System Administrator – The System Administrator has complete access throughout the NSDD-38 website, including user administration permissions.
- Requester – Individuals 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.

EOD

- Applicant User - 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.
- EOD Administrator - This role is only granted to GTM 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. This role is responsible for granting and removing the HR Specialist and the Benefits Processor roles in the EOD system.
- HR Specialist - 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 user can send back information submitted by the applicant user to be corrected and may terminate an EOD process and disable an account of a specific Applicant User. The HR Specialist initiates the purge process which transfers the EOD package to the GEMS system and deactivates the applicant user account.
- Benefits Processor – The Benefits Processor user can view, verify, send to Payroll, eOPF, and print all necessary information 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. They notify carriers of coverage and ensure members have designated coverages established.

CT Survey

- Candidate/Bidder – This role is responsible for contacting references, submitting questionnaires to preferred references, and seeking additional feedback from current or former colleagues.
- Assessor - Assessors are responsible for completing and responding to the questionnaire once it's received from the candidate.
- GTM/RMA (Admin) – This role is responsible for reviewing and validating questionnaire results prior to sending results to the committee and representatives.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

The procedures to limit system and data access vary by system and role assignment:

- NSDD-38 user account applications are assessed and granted by M/SS analysts.

- HR Specialists are granted access to EOD based on the position and role requested on the EOD User Registration web form. The form is submitted to Application Support for approval. Once granted approval. the HR Specialist can then initiate and manage the process to create an invitation and account for the applicant user. The applicant user is a person selected for a position in any one of the various programs offered by the Department of State.

(d) How is access to data in the system determined for each role identified above?

Access to data in the system is determined by the individual's organization, role, and authorized responsibility. Privileged system administration and database administration roles are assigned within GTM/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.

NSDD-38

- System Administrator – The system administrator has complete access throughout the NSDD-38 website, including user administration permissions.
- Requester – This user role will have access to data for their specific agency and all its posts.

EOD

- Applicant User - The applicant user can create and access only their individual personal information in required forms for the Entrance on Duty process. 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.
- EOD Administrator – The administrator has full access to the data and the ability to assess and assist when errors and issues prevent the completion of any packet. They can cancel, resend, or move packets as required during the process.
- HR Specialist - The HR specialist can view, modify, and delete forms for new applicants and is the approver of the EOD package.
- Benefits Processor – The benefits processor user can view, verify, send to payroll, eOPF, and print all necessary information submitted by the applicant user.

CT Survey

- Candidate/Bidder – Is the user who creates the survey and has access only to their data.
- Assessor – This role only has access to update the candidates survey.
- GTM/RMA (Admin) – The administrator can update and review everything.

(e) What monitoring, recording, auditing safeguards, and other controls 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 are hosted in the IRM/ENM DMZ and rely on firewall network access control and network intrusion detection.

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

☒ Yes ☐ No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

There is no specific role-based training provided. 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 (PS800), prior to being granted access to the system and annually thereafter. 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. Finally, all Department employees are required to take the biennial mandatory PII Training, PA318 - Protecting Personally Identifiable Information.