1. Contact Information

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

2. System Information

(a) Date PIA was completed: March 30 , 2011

(b) Name of system: Human Resources Network

(c) System acronym: HRNet

(d) IT Asset Baseline (ITAB number): 866

(e) System description:

The Human Resources Network (HRNet) serves as the HR Bureau's main portal to provide Internet-based HR services to the Department of State's and other Executive Branch agencies' user communities. Users include employees of the Departments of Commerce, Agriculture, Homeland Security, Justice, Energy, Transportation, and Health and Human Services, the U.S. Agency for International Development, Broadcasting Board of Governors, Peace Corps, as well as retirees and annuitants from all the foreign affairs agencies. The HRNet portal is comprised of five applications:

- National Security Decision Directive 38 (NSDD-38)
- Civilian Response Corps (CRC)
- Post Personnel Lite (PSLite) Web Service
- Post Personnel Lite (PSLite) BizTalk Service
- Connect:Direct Client Subsystem

(f) Reason for performing Privacy Impact Assessment (PIA):

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

(g) Explanation of modification:

The last PIA for HRNet was published in 2008. Since that time, several modifications to HRNet were made and the following applications were incorporated:

Civilian Response Corps. CRC maintains records for the Office of the Coordinator for Reconstruction and Stabilization (S/CRS) of registered CRC members. Members are a pool of qualified, specially trained professionals occupying active and standby roles who are equipped and ready to deploy rapidly to prevent conflict or provide

post-conflict and stabilization assistance to countries in crisis or emerging from conflict. CRC contains PII on current and former Federal employees and contractors.

Connect:Direct. This subsystem permits data exchange between the Department of Labor and Department of State related to Federal employee workers' compensation (FECA) claims.

PSLite Web and BizTalk Services. Post Personnel, an application component of the WebPASS suite, collects and stores locally a post's personnel data. Data is transmitted nightly to a consolidated database in Washington, DC. PSLite provides a subset of this consolidated post personnel data to subscribing systems via the PSLite Web and BizTalk Service. PSLite compiles a file transmitted daily from the Executive Agency Personnel Support (EAPS) system. PSLite presents these data to the WebPass subscribing system called eServices. eServices receives a subset of the post personnel contact information, specifically name, office phone number, and office location.

Until April 2008, HRNet hosted another application called the Post Personnel Global Access System (PSGAS) that provided other Executive Branch agency users with reports on position-related information maintained in Post Personnel. PSGAS functions were replaced by the Executive Agency Personnel Support (EAPS) system. Functions of Employee Profile Plus (EP+) and the When Actually Employed (WAE) Global Registry in HRNet have been discontinued. Because of the nature of the new applications added to HRNet, its security categorization was increased to Moderate.

(h) Date of previous PIA: July 31, 2008

3. Characterization of the Information

The system:

☐ Does NOT contain PII.

☒ Does contain PII.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The elements of PII collected and maintained by HRNet include the following types:

PII Elements	CRC	NSDD-38	PSLite	Connect:Direct
Full Name	X	X	X	X
Gender	X			X
Date of Birth	X			X
Grade and Step	X		X	
Department/Agency	X	X	X	X
SSN	X			X
Work/Home Address	X	X	X	
Emergency Contact Information	X		X	

Contact Information	X	X	X	
Diplomatic/Official passport numbers	X			
Visa Number	X			
Medical Clearance level, date of issue, country cleared	X			
Security Clearance Level	X			
Department of State Badge Number	X			

b. How is the information collected?

PII about members of the Federal workforce is originally compiled and collected as a condition of employment by the Department of State or another Executive Branch agency using a variety of separate Federal government systems supporting recruitment and career-long maintenance of the workforce. Information compiled by HRNet supports HR's mission of providing Internet-based HR services to the Department of State community, and other Executive Branch 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 diplomatic agencies. The information is used specifically for the following purposes:

(1) Provides authorized users the ability to enroll on a mailing list to receive information provided by the Director General and about the Civilian Response Corp.

(2) Provides information pertinent to retirement planning to include retirement planning guides, links to retiree/annuitant information and forms, and retirement contact information for the Thrift Savings Plan and Social Security Administration.

(3) HRNet provides support for the Civilian Response Corp by providing automation for the purpose of contact, training, medical clearances, and property issuance to CRC members and their missions outside of the Department of State, including agencies such as Health and Human Services, Department of Agriculture, and the United States Agency for International Development.

c. Why is the information collected and maintained?

HR Net supports the following mission and program objectives:

- To ensure the Chief of Mission has control of the size, composition, and mandate of overseas full-time mission staffing for all U.S. Government agencies.
- 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.
- To improve the operational effectiveness and efficiency of overseas post personnel and position management.
- To support Department of State obligations under the Department of Labor’s Workers’ Compensation Programs.

d. How will the information be checked for accuracy?

M/PRI is the business owner for NSDD-38 and interacts directly with posts to validate the information. S/CRS validates information pertinent to CRC members through interaction with the member's parent Executive Branch agency. PSLite depends on data originating in the Post Personnel application of WebPASS. Post HR personnel use the data quality assurance features of WebPASS to ensure that the data entered is correct. Further detail is provided in a separate PIA for WebPASS.

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

- 22 U.S.C. 2669
- 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. 3901 et seq. (Foreign Service Act of 1980)
- 22 U.S.C. 3921 (Management of the Foreign Service)
- 5 U.S.C. 301-302 (Management of the Department of State)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy risks are mitigated through adherence to Department policy and guidelines. HRNet collects the absolute minimum amount of PII required to satisfy the statutory purposes of HRNet and the mission of the HR Bureau. Using Federal Information Processing Standards Publication 199 (FIPS 199), the sensitivity of PII elements, individually and as an aggregate, are classified as having a moderate risk because the combination of name, date of birth, and SSN may be used as means of identification for commission of identity theft.

The loss of confidentiality, integrity, or availability of PII may have a serious adverse effect on organizational operations, organizational assets, or the individuals. Depending on the information lost, the potential harm suffered may include social, economic, or physical harm. If the information lost is sufficient to be exploited by an identity thief, an employee can suffer from financial loss, damage to credit, a compromise of medical records, threats and/or harassment. An individual may lose time and money to repair the damage.

Other types of harm that may occur to individuals include denial of government benefits, blackmail, discrimination, and physical harm. The potential harm of compromised PII may also lead to the compromise of the safety of Department employees from organized crime groups or hostile foreign governments. If PII is misused, the Department may suffer financial losses in compensating individuals, assisting them in monitoring their credit ratings, and addressing administrative concerns. In addition, recovering from a major breach would be costly to the Department in terms of time spent by key staff in coordinating and executing appropriate responses.

HR has adopted the Department-wide Rules of Behavior for Protecting PII (hereinafter called "Rules") that lists the privacy rules applicable to Department records, regardless of format. All employees and contractors with access to PII in the performance of their official duties are required to comply with these rules. Procedural and technical security controls are in place to protect information in transit and at rest. The use of encryption, audit log

review, non-PII database primary keys, data masking, and separation of duties are among the controls in place to mitigate the risk of information exposure.

Access to information is granted to systems administrators, helpdesk agents, HR specialists, and hiring managers at a level commensurate with their need to know and responsibilities. In addition, prior to system access, all Department employees (including contractors) involved in the design, development, operation, or maintenance of HRNet undergo training to include the Rules and penalties for noncompliance. Users are trained through the mandatory Computer Security Awareness Training (CSAT) to report suspicious activities.

4. Uses of the Information

a. Describe all uses of the information.

HRNet collects and maintains information in support of HR's mission. As a logical suite of applications, HRNet collects the PII (listed in section 3.a.) in the following subsystems:

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. External to the Department of State, NSDD-38 web application users include direct hires, cleared contractors, and un-cleared contractors who are from other Executive Branch agencies as well as some NGOs.

CRC. The Civilian Response Corps (CRC) system is used by the Office of the Coordinator for Reconstruction and Stabilization (S/CRS) in Washington 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.

PSLite Web Service. The PSLite Web Service provides position information to eService on demand. PSLite is a web service that maintains a system-to-system connection with eServices, and provides a subset of post personnel data collected in Washington, DC to subscribing systems via a web service.

PSLite BizTalk Service. The purpose of the PSLite BizTalk Service is to provide position and employee information to those posts that do not have Post Personnel system installed locally.

Connect:Direct Client Subsystem. The Department of State utilizes data provided by Office of Workers' Compensation Programs (OWCP) to trend, report, and manage the performance of its worker safety and health program under the Department of Labor's Safety, Health, and Return-to-Employment (SHARE) Initiative. Connect:Direct performs a secure transfer of data from Labor. The OWCP data is then securely transferred from HRNet and stored in the Department of State's Workers Compensation Database, a component application of IPMS.

b. What types of methods are used to analyze the data? What new information may be produced?

No data mining activities or methods are utilized by the system. New information that may be produced includes reports pertaining to workforce planning. Reports are created on a need-to-know basis for statistical purposes, skills inventories, data quality reviews, internal management controls, and for official reporting both inside and outside of the Department. Access to reports is limited to authorized users as identified by the system owner.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

HRNet does not use commercial, publicly available information, or information from other Federal agency databases.

d. Are contractors involved in the uses of the PII?

Contractors are involved in the design, development, and maintenance of HRNet, and are required to complete, and repeat when appropriate, the Department's Cyber Security Awareness Training (CSAT). All contracts include Federal Acquisition Regulation Privacy Act clauses.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Access authorizations and permissions are granted only to systems administrators, helpdesk agents, and hiring managers at a level commensurate with their need to know and responsibilities. HRNet relies on security safeguards implemented by the Department of State. Only users granted access to OpenNet may connect directly to and administer the HRNet servers. Other Executive Branch agency users are required to complete an access request form to gain access to the CRC and NSDD-38 applications.

HRNet adheres to the rules stipulated in the system security plan (SSP). The SSP delineates responsibilities and expected behavior of all individuals who access information collected by HRNet. All components and sub-components adhere to the Rules applicable to all employees and contractors and covering all Department records that include PII, regardless of format. The security protections in place include: controlled access, authorization, and permission controls, reducing the overall risk to a low level.

5. Retention

a. How long is information retained?

PII records are maintained until they become inactive, at which time they are retired or destroyed in accordance with published Department records schedules as approved by the National Archives and Records Administration (NARA) and administered by Information Programs and Services (A/GIS/IPS).

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The risk associated with the retention of information pertains to continued viability of the media and whether it can be supported by current technologies. To mitigate the risk, HR has the practice of converting information to a government-wide standard.

Technology risks aside, the risks associated with the duration that information is retained are minimal. As stated in Section 5.a. above, information is retired or destroyed in accordance with published Department records disposition schedules. Any residual risk is mitigated through the use of security controls, such as allowing only authorized personnel access to the system and the use of OpenNet, the Department's Sensitive But Unclassified (SBU) network.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

HRNet is not directly connected to any external networks. However the NSDD-38 and CRC portions of HRNet interface with IPMS, via Executive Agency Personnel Support (EAPS). Information is available only to authorized users within the Department for the purpose of executing their official duties. Within the Department, information is shared as follows:

- M/PRI is the business owner of NSDD-38 and is responsible for the administration and authentication of user accounts. In addition, M/PRI manages the requests by other agencies for additions, deletions, and changes to their staffing abroad.
- CRC is used by the Office of the Coordinator for Reconstruction and Stabilization (S/CRS) in Washington, DC for tracking and reporting on members and their missions.
- The PSLite web site is used only by the eService system and is not directly accessible by users. PSLite is an extract from the NSDD-38 database, located inside the Department's network perimeter. PSLite BizTalk is an inter-system interface with no user interaction. Post personnel data extracted from EAPS database is copied to a secure network directory where it is used by PSLite.
- Connect:Direct exchanges data between the Department of Labor's Integrated Federal Employees' Compensation System (iFECS) and the Department of State's IPMS for the purposes of FECA administration. An Interconnection Security Agreement (ISA) was executed between the two agencies for this purpose in October 2009.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is shared by secure network transmission methods permitted under Department policy for the handling and transmission of SBU information.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

HRNet adheres to the rules stipulated in the system security plan, which delineates responsibilities and expected behavior of all individuals who access HRNet. In addition, the Department has implemented Rules applicable to all employees and contractors and covering all Department records that include PII, regardless of format.

Internal access to data is only available to authorized users who are cleared government employees and 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 layered technical controls to prevent the misuse or improper disclosure or access to PII. HRNet is hosted within the Department of State which is an accredited network. Log records of all user activity are maintained.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

All external organizations accessing HRNet are granted an authorization level to manage information within their scope of responsibility. HRNet shares information with Washington-based Executive Branch agencies as well as other agencies with an overseas presence.

NSDD-38 information is provided to designated personnel managers within their respective agency. Agencies are not able to view employee information outside their own organization. Disclosed information includes home phone, cell phone, emergency phone, work number, and e-mail. Sharing is required to enable administrative personnel the ability to validate position and employee data. This includes the ability to review, validate, audit, and continuously manage personnel, assignment, and position data. HRNet shares information with authorized users of the following external entities:

S/CRS discloses CRC records to entities outside the Department such as to the designated Response Corps Coordinators of:

- The United Nations, NATO, or similar international organizations for the purpose of coordinating personnel engaged in specific reconstruction and stabilization activities.
- A U.S. and NATO military installation for the purpose of security checks and to obtain access to military facilities, including manifesting on military aircraft.
- Other Executive Branch agencies regarding information needed in the performance of their official duties to support the functions for which the records were compiled about their employees accepted as members of the Corps.
- Other Executive Branch agencies, state governments, foreign governments, and international organizations where employees are being considered for detail, assignment, or secondment within the Corps.
- Officials of foreign governments and other Executive Branch agencies for clearance before an employee is assigned to that country, as well as for the procurement of necessary services for personnel assigned overseas, such as permits of free entry and identity cards.
- Attorneys, union representatives, or other persons designated in writing by those employees, who are the subject of the information, to represent them in complaints or grievances.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

HRNet PII is disclosed only to authorize users. HRNet relies on the security control safeguards implemented by OpenNet. External agency representatives that require access to HRNet must comply with the application access process. Users who are granted access are only allowed to view or edit information to which they are assigned sufficient access rights. Agencies are not able to view employee information outside their own organization.

Information transmitted across a network not under the control of the Department of State is protected by encryption.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Privacy risks from external sharing of information contained in HRNet is mitigated by maintaining strict access controls. Representatives of agencies are only able to view employee information of those persons within their agency. This provides a limit on the flow of information within HRNet and among agencies, mitigating privacy risks.

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Depending on its use, PII maintained in HRNet is subject to the provisions of the Privacy Act, and is described in the following Privacy Act systems of records:

- State-25, Overseas Records
- State-31, Human Resource Records
- State 68, Office of the Coordination for Reconstruction and Stabilization Records

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

The authority, purpose, and use for the PII in the HRNet applications are described in the Privacy Act systems of records (SORNs) listed above. A website privacy policy, compliant with both Section 208 of the E-Government Act and the Privacy Act, is posted on any sites that provide self-service to record subjects or authorized Executive Branch agency staff.

b. Do individuals have the opportunity and/or right to decline to provide information?

Individuals may decline to provide some or all information; however, refusal may interfere with the provision of HR services to the individual.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No other special uses of the information are permitted. Employees are advised of the uses of the information being collected.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

A system use notification (“warning banner”) is presented at the logon screen of applications that collect PII from employees. Risks associated with individuals not being aware of the collection of PII are further mitigated by the applicable Privacy Act notices described above.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

As explained in Section 8, HRNet users may amend contact information they believe to be incorrect. With respect to the source systems from which HRNet records are compiled, access and amendment procedures are available and are described in the applicable Privacy Act SORNs listed in Section 8.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Notification and redress mechanisms offered to individuals are reasonable and adequate. Department of State employees may request the HR Bureau to update information they consider to be incorrect. Employees of other Executive Branch agencies may follow notification and redress procedures in the Privacy Act SORNs described in Section 8.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Only authorized Department active employees and contractors are provided direct access to the HROnline. To gain access to the HROnline a user must maintain at least a SECRET security clearance. To access records, the individual must first be an authorized user of OpenNet. Each prospective authorized user must also sign a user access agreement before being given an OpenNet user account. The user access agreement includes the Rules describing the individual's responsibility to safeguard information and lists prohibited activities (e.g. curiosity browsing). Internet users are required to complete an access request form to gain access to CRC and NSDD-38 applications. External agency representatives accessing NSDD-38 and CRC are responsible for supervising the use of the system by that agency's staff.

Each time a user logs on to HRNet, a Federal-standard system use notification ("warning banner") is presented. Users who are granted access to HRNet are only allowed to view or edit information to which they are assigned sufficient access rights. All HRNet user access is regulated through the use of role-based access controls.

Audit logs are maintained to record system and user activity including invalid logon attempts and access to data. The HR Information System Security Officer monitors audit logs monthly for atypical activity. System managers and key security and user personnel cooperate and work closely to implement access controls. Endpoint devices used to access HRNet complete with the Federal Desktop Core Configuration (FDCC) standard.

HRNet is accessed by other Executive Branch agencies across external networks not under the control of the Federal government. Security is provided by approved encryption technologies and logon processes.

b. What privacy orientation or training for the system is provided authorized users?

The Department's appropriate use policy and Rules are the general terms under which Federal employees and contractors use the system. The Department requires all new

employees and contractors to attend Cyber Security awareness training before or immediately after the employment start date and prior to being granted access to the system. In addition, the account request form signed by all employees and contractors to access OpenNet includes a requirement for the individual to successfully complete a Cyber Security awareness learning course. To retain access, all Department personnel must complete annual refresher training. Access to data is limited to cleared Federal employees and contractors administering the system who meet official need-to-know criteria. The HRNet System Security Plan and the Department Rules delineate the responsibilities and expected behavior of the individuals.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Safeguards for access are commensurate for a system having a Moderate security categorization. The safeguards reduce privacy risk related to user access to a negligible level. The HR Bureau places great emphasis on the security of the data under its purview through adherence to best security practices and compliance with Department directives and Federal laws. The NIST security controls required by the Federal Information Security Management Act (FISMA) include continuous monitoring of account access and least privilege, monitoring of event log activities related to object access and transactions, and appropriate internal user training to include the Rules and security awareness. These controls are reassessed and certified annually to maintain security standards.

11. Technologies

a. What technologies are used in the system that involves privacy risk?

HRNet relies on standards-based commercial software products for which configuration standards have been established by the Bureau of Diplomatic Security.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

HRNet utilizes technologies approved by the Department of State IT Configuration Control Board and the HR Bureau's internal Configuration Control Board. HRNet leverages the OpenNet hosting environment for secure network connectivity. HRNet software is configured in accordance with Department configuration standards and is annually tested for configuration vulnerabilities according to Department security policy.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The last authorization to operate HRNet in accordance with the Federal Information Security Management Act (FISMA) was issued on August 15, 2008. HRNet is authorized to operate until August 2011; however, with the inclusion of the Civilian Response Corps, Connect Direct, and PSLite applications and the change in security categorization from Low to Moderate, HRNet received an earlier authorization March 1, 2011.