Integrated Personnel Management System (IPMS)

1. Contact Information

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

2. System Information

(a) Name of system: Integrated Personnel Management System

(b) Bureau: Human Resources (HR)

(c) System acronym: IPMS

(d) iMatrix Asset ID Number: 951

(e) Reason for performing PIA:

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

(f) Explanation of modification (if applicable): Since the last authorization there has been an update to the HR Points of Contact, network architecture and addition of two new sub systems namely Overseas Personnel System (OPS) and HR Customer Assistance Support Environment (HRCASE).

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 for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
Authorization to Operate (ATO) expires October 30, 2018.

(c) Describe the purpose of the system:
The HR IPMS is a multi-year, mixed-lifecycle program initiative that incorporates the underlying technical architecture for all the applications managed by the HR Executive Office (HR/EX). The IPMS is used to manage personnel information for Department of State (DoS) Civil Service (CS) and Foreign Service (FS) direct-hire employees, Locally Employed Staff (LES), contractor employees, dependents, FS Consular Agents, applicants for CS and FS employment, other United States Government (USG) Agency

employees under Chief of Mission (COM) authority, and resident US citizens employed by US missions abroad.

The core applications within the IPMS umbrella include the PeopleSoft Based Global Employment Management System (GEMS- iMatrix 135), HR Knowledge Center (KC - iMatrix 729), the Overseas Personnel System (OPS - iMatrix 7305), HR Customer Assistance Support Environment (HRCASE - iMatrix 257500), the Human Resources Online (HROnline - iMatrix 728) system, and the Executive Agency Personnel Support (EAPS - iMatrix 2738) system. The core applications receive data from Global Employment Management System (GEMS).

Together, all IPMS components reduce transaction processing overhead, enhance enterprise-wide data sharing, improve data integrity and quality, and empower employees and supervisors with the ability to independently manage their personal information though online seamless workflow processes.

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

- SSN
- Employee System ID
- First Name
- Last name
- Birth Date
- Birth Country
- Birth Place
- Age
- Legal Residence
- Marital Status
- Gender
- Race and National Origin Code
- Known Traveler Number
- Handicap Code
- Med Clearance Code
- Med Clearance Date
- Med Exam Date
- Employee Benefits
- Employee Review Data

- Education
- Email Address (Gov't and Personal)
- Military Status
- Veteran Code &Veteran Description
- Security Clearance Case Open Date & Grant Date, Security Clearance Level
- Requested Security Clearance Level
- Dependents
- Name and Location of Position's Organization
- Position title and number
- Retirement Plan, Citizenship
- Evacuee Contact Information
- Passport Number Information
- Address: Street number, street name, City or Town, State, Zip Code
- Telephone number
- Selection of one of the following:
  - Citizen of the U.S
  - Noncitizen national of the U.S
  - Lawful permanent resident: Alien Registration Number/USCIS Number
  - Alien authorized to work until (expiration date)
- Alien Registration Number/USCIS Number OR
- Form I-94 Admission Number OR
- Foreign Passport Number and Country of Issuance
- If Driver's License used: State is entered in E-Verify
- Visa Number (when applicable)

(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. 3901 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 13478 (Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers
- Executive Order 9830 (Amending the Civil Service Rules and Providing for Federal Personnel Administration)

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

☒Yes, provide:

- SORN Name and Number: Medical Records, State-24
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): February 11, 2015

- SORN Name and Number: Human Resources Records, State-31
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): July 19, 2013

- SORN Name and Number: Overseas Citizens Services Records and Other Overseas Records, State-05
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): September 8, 2016

- SORN Name and Number: Security Records, State-36
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): June 15, 2018

☐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 Division 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 .)

HR is reaching out to Records Management to create new schedules and to update the existing ones.

If yes provide:

- Schedule numbers: A-04-003-01a through A-04-003-20 and A-04-004-18
  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.
- Length of time the information is retained in the system: When records have reached their retention period (see below), they are immediately retired or destroyed in accordance with the National Archive and Records Administration
- Type of information retained in the system: Documents pertaining to the Foreign Service Examination and to all phases of the Foreign Service personnel assignment and travel process.

Schedules: A-04-003-01a; A-04-003-02a; A-04-003-02b; A-04-003-03a; A-04-003-03b; A-04-003-04; A-04-003-05; A-04-003-06; A-04-003-07a; A-04-003-07b; A-04-003-08a; A-04-003-08b; A-04-003-09a(1); A-04-003-09a(2); A-04-003-09b(1); A-04-003-09b(2); A-04-003-09c(1); A-04-003-09c(2); A-04-003-10; A-04-003-11; A-04-003-12; A-04-003-13; A-04-003-14a; A-04-003-14b; A-04-003-15a(1); A-04-003-15a(2); A-04-003-15b(1); A-04-003-15b(2); A-04-003-18; A-04-003-19a; A-04-003-19b; A-04-003-20.

Description Foreign Service Files

Disposition: TEMPORARY: Delete within 180 days after recordkeeping copy has been produced; retire to RSC within 2 years of appointment for transfer to WNRC and destroy when 7 years old; destroy 2 years from date of most recent documentation; retire to RSC 2 years after the year of the oral examination for transfer to WNRC and destroy when 7 years old; destroy after 6 months; destroy 6 months – 5 years after date of examination; retire to RSC 2 years after the year of the Written Examination for transfer to WNRC and destroy when 7 years old; retire to RSC 2 years after the year of appointment for transfer to WNRC and destroy when 7 years old; destroy all folders of candidates who are 55 years or older; destroy all non-policy material when 2 years old; retire to RSC after 2 years and destroy 8 years thereafter; destroy after candidates have been notified of grades and grades have been recorded on permanent record card; destroy when 3 years old;

retire to RSC when 5 years old and transfer to National Archives when 20 years old.

PERMANENT: Retire to RSC every 5 years for transfer to the WNRC and transfer to the National Archives when 25 years old; retire to RSC when 5 years old and transfer to National Archives when 20 years old; retire policy documents to RSC when 5 years old for permanent retention; retire to RSC when 10 years old for transfer to WRNC and transfer to the National Archives when 25 years old.

DispAuthNos: N1-059-00-07, item 9; N1-059-00-07 item 10a; N1-059-00-07, item 10b; N1-059-00-07, item 11a; N1-059-00-07, item 11b; NC1-059-80-20, item 4a; NN-171-171, item 2; NC1-059-83-06, item 1b; II-NNA-400, items 9a and 9b; II-NNA-400, item 9c; N1-059-00-07, item 14a; N1-059-00-07, item 14b; N1-059-00-07, item 15a(1); N1-059-00-07, item 15a(2); N1-059-00-07, item 15b(1); N1-059-00-07, item 15b(2); N1-059-00-07, item 15c(1); N1-059-00-07, item 15c(2); II-NNA-400, item 12; II-NN-3412, item 2; NN-171-171, item 4; NN-173-062, item 3; N1-059-00-07, item 16a; N1-059-00-07, item 16b; N1-059-00-07, item 17a(1); N1-059-00-07, item 17a(2); N1-059-00-07, item 17b(1); N1-059-00-07, item 17b(2); N1-059-00-07, item 13; N1-059-00-07, item 19a; N1-059-00-07, item 19b; NC1-059-00-07, item 1.

Schedules: A-04-004-18

Description Integrated Personnel Management System (IPMS) Foreign Service Assignment Management Application (IFSAMA)

IFSAMA is a computer system that replaced the Automated Personnel Transactions System (APTS) in November 1997 and controls all phases of the Foreign Service personnel assignment and travel process. It tracks and reports on employee assignment, employee travel history, and the Foreign Service bidding process. It also collects training data, eligible family member information, employee and eligible family member medical information, tour of duty data and pending assignment data.

Disposition: TEMPORARY: Cut off annually. Delete when obsolete or no longer needed. (N1-059-88-15).

DispAuthNos N1-059-00-08, item 7.

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?

•26 CFR 301.6109, Taxpayer identification;
•Executive Order 9397, as amended, Federal employment;
•Executive Order 13478 (Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers) and
•20 CFR 10.100, Federal Workers' Compensation.

(c) How is the information collected?

Internal to the Department of State, PII is collected by IPMS from employee and manager self-service applications and through manual data entry by HR specialists. Employees, managers and HR specialists use applications with web interfaces to enter information into IPMS. Additionally, IPMS collects information from the following internal Department of State Bureaus:

- FSI - PII is collected from STMS via electronic data interchange.
- CGFS - PII is collected from CAPPS and FSNPay via electronic data interchange
- MED - PII is collected from eMED via electronic data interchange
- DS - PII is collected from Department of State Clearance System, DS Employee Tracker, and the Identity Data Management System (IDMS) via electronic data interchange.

External to the Department of State, PII is collected by IPMS from the following organizations:

Department of Labor (DOL)

- DoS receives data extracts on a weekly, monthly, or quarterly basis. DOL Office of the Chief Information Officer (OCIO) provides the data extract via SFTP protocol on a secure isolated landing zone (i.e., secure trusted zone) within the ECN/DCN network. This solution is FIPS 140-2 compliant and provides DoS personnel secure authentication access to DOL workers compensation files. All files utilize data encryption. The source information system is the Office of Workers' Compensation Programs' (OWCP) Integrated Federal Employees' Compensation System, which is hosted on the ECN/DCN and maintained by the Office of the Assistant Secretary for Administration and Management (OASAM). The data extracts may include case management, medical payment, compensation payment, and/or chargeback related information. When received by HR, the OWCP PII is stored in DoS's Workers Compensation Database, a component application of IPMS and is limited to Authorized DoS Personnel.

Pearson VUE

- Pearson VUE is a commercial contractor that maintains the Foreign Service Officer Test Application that is used to administer the online Foreign Service Written exam. Information is collected through an interactive user session through the contractor hosted web site. The candidate user creates an account in a web form process providing name, date of birth, SSN, residential address, telephone number, and e-mail address. The information is maintained and used by the Human Resources Recruitment, Examination, and Employment office (HR/REE). HR/REE logs into Pearson VUE server through encrypted secure file transfer protocol (SFTP) to pull candidates PII and upload into IPMS for processing (through Qualifications Evaluation Panel application).

Monster Government Solutions (MGS)

- MGS is a commercial contractor that maintains the Hiring Management System (a.k.a., Gateway to State (GTS)). The Hiring Management System is a web-based job candidate assessment tool that is accessible via the internet from the USAJobs website, and is used to automate the staff acquisition process for Civil Service and

most Foreign Service jobs. HR/REE logs into Monster GTS server through encrypted secure file transfer protocol (SFTP) to pull applicants PII and upload into IPMS for processing through Monster Government Solutions Data Processor (MDP) application.

(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.

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

Employee data integrity and completeness within IPMS are checked through the use of internal management reports and quality reviews. If the data pertains to an employment application or an application for the Foreign Service Officer exam, the applicant is responsible for the accuracy of the information. The applicant has the opportunity and responsibility to verify his/her personal and demographic information in the application 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. For EAPS data, Department American employee information is verified daily with GEMS for data integrity and completeness.

A data extract program is run each morning to download the GEMS position and employee data into the EAPS database. Based on the GEMS extract data, an analysis program is executed to validate the accuracy of GEMS position and employee data with EAPS position and employee data. Once the data is updated at Post, the program will submit the data to the EAPS database. This completes the data transaction cycle. GEMS position and employee data is consumed by HRKC, HRCASE, HROnline and OPS and employees are responsible for ensuring the accuracy of their information in GEMS. Some employee information in OPS is extracted from GEMS while some is entered by the employee. Employees can review their information for accuracy in OPS or GEMS and make corrections thorough their HR specialist. Supervisors, Security Administrators and Government Project Managers review forms completed by employees in OPS for accuracy.

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

Yes. Information is collected, maintained and processed by the IPMS child application components of HR Online, EAPS, GEMS, and KC including their child applications to enable the Bureau of Human Resources to fulfill its mission of providing worldwide HR management. Procedures to ensure information remains current include allowing the employee user to make modifications with self-service functions of each application. If the user recognizes out-of-date PII, they may also submit changes to the PII in their records from the HR Help Desk or other application maintained within HR.

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

IPMS does not use commercial information nor is IPMS information publicly available.

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

A Privacy Act statement is posted on the login screen of Entrance On Duty (within IPMS) for Candidates that have been offered employment by the HR Bureau.

For Department of State employees, when logging into HR Online or accessing GEMS through HROnline, a Privacy Act statement is posted on the login screen that complies under the Privacy Act of 1974, 5 U.S.C. § 552a (as amended). The functionality to present this statement to the user was implemented on July 10, 2015.

(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?

Consent is provided by individual DoS employees when he/she provides his/her information after reading the Privacy Act statement on the login page of the HROnline. Dependents do not have access to IPMS or child applications and therefore cannot provide consent. Dependents' information is entered by the Department of State employee providing such information. The employee has parental/custodial rights to provide consent for dependents whose PII is being provided. Before being released to a third party, the dependent PII would be excised.

Department of State employees may decline to provide information, but the refusal to do so would restrict their ability to complete employee/manager system processes.

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

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

In light of the privacy concerns surrounding the system, IPMS collects the absolute minimum amount of PII required to satisfy its statutory purposes and the mission of the Bureau of Human Resources. Procedural and technical security controls, including permission and access controls, are in place to protect IPMS data in transit and at rest. Only authorized users have access commensurate with their clearance level and need-to-know.

5. Use of information

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

The information is used specifically for the following business purposes:

- Provide overseas workforce management, workforce planning, employee services, and employee and family support.
- Provide financial information including earnings and leave as an HR service for all LES.
- Review, validation, auditing, and continuous management for Washington-based Executive Branch Agencies (EAs) for the individual EA presence overseas in a near real-time environment.
- Provide support for the overseas review and correction of employee and position records that exist at EAs in Washington and individual embassies and consulates.
- Allow users to create travel authorization documents for persons evacuated during a crisis. Information collected by EAPS is used by posts and the Family Liaison Office (FLO) during an evacuation to track and manage the departure of evacuees. This service also includes the location of persons while at Post and alternate contacts (if available) where a person may be reached during and after the evacuation. Locations include the addresses to which State employees have relocated following evacuation and also those of their family members.
- Provide automation of the following DoS forms related to overseas activities: the DS 1552, Leave Data-Departure for Post; and the DS-1707, Leave, Travel, and Consultation Status.

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

Yes. IPMS applications allow for HR to provide for workforce management, workforce planning, employee services, and employee and family support.

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

If yes:

(1) What types of methods are used to analyze the information?
IPMS is a worldwide human resources system that supports the recruitment and management of personnel; the methods of data analysis vary. Methods used to analyze data include: Performing complex analytical tasks predicated on matching, relational analysis, scoring, reporting, or pattern analysis. Additional methods used to analyze data include compensation plan calculations of total compensation and sensitivity analysis of pay increase mathematical models used for LES salary analysis. LES pay information is used to calculate the total count of positions/employees by country, total cost of compensation by country, and the compensation increase by country.

(2) Does the analysis result in new information?
Information that may be produced includes the following types of aggregated data: reports pertaining to workforce planning, hiring summary data, Foreign Service residence, dependency data, performance management reports, post and regional compensation plan recommendations, hiring summary data, and LES salary increases. Reports are generated on a need-to-know basis for statistical purposes. These statistics include: skills inventories, data quality reviews, internal management controls, and official reporting, internal and external to the Department. For EAPS only, following an evacuation, summary reports may be produced containing evacuee PII. No new information is derived.

(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.

IPMS shares information with the following internal organizations

- Bureau of Information Resource Management (IRM)
- Foreign Service Institute (FSI)
- Office of Medical Services (MED)
- Bureau of the Comptroller and Global Financial Services (CGFS)
- Bureau of Diplomatic Security (DS)
- A Bureau (A)
- Overseas Building Operations (OBO)

IPMS shares information with the following external organizations:

- Office of Personnel Management (OPM)
  - IPMS data is shared electronically with OPM via secure connection in accordance with the Central Personnel Data File (CPDF) and Enterprise Human Resource Integration (EHRI) reporting requirements. The MOU between OPM and the Department of State requires the incorporation of all electronic safeguards required by both agencies, for submittal of CPDF and EHRI reportable data elements.
- Transportation Security Administration (TSA)
  - TSA maintains the Secure Flight program. GEMS assigns the Known Traveler Number (KTN) to Department personnel who opt-in to the Secure Flight Program.
- Department of Homeland Security (DHS)
  - Limited data is shared electronically with DHS via secure connection and in accordance with the MOU established between DHS and the Department of State.

(b) What information will be shared?

- IRM: IPMS shares person, position, and transaction data.
- FSI: IPMS shares employee, position, salary, location, and organization data.
- MED: IPMS shares employee and dependent medical information.
- CGFS: IPMS shares employee salary and benefits information.
- A Bureau: IPMS shares employee information.
- OBO: The EAPS application of IPMS shares overseas position information.
- OPM: IPMS shares information with OPM in accordance with the CPDF and EHRI reporting requirements. Executive agencies are required by the Director of OPM to report information relating to civilian employees, including positions and employees in the competitive, excepted, and Senior Executive services.

- TSA: GEMS shares KTN, full name (First, Middle, and Last), gender, race, national origin and date of birth with TSA.
- DHS: Information shared by DoS with DHS's E-Verify includes: Last Name, First Name, MI (if applicable), Other Last Name Used (if applicable), Date of Birth, Social Security Number, Employee's Email Address (if employee provided and email), Citizenship Status, if Driver's License is used: State is entered in E-Verify, First Date of Employment, and Visa Number (when applicable). For some cases we are required to upload a copy of the employee's photo documentation

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

The intended purposes for sharing are to support the following:

- IRM: Department-wide reporting and analysis from the Enterprise Data Warehouse (EDW).
- FSI: The training process.
- MED: Foreign Service medical clearance process.
- Bureau of Comptroller and Global Financial Services: Payroll process.
- A Bureau: Travel, logistics, and parking processes.
- OBO: Annual Capital Security Cost Sharing (CSCS) and Space Requirements Planning processes for Rightsizing Position Management Functionality.
- OPM: Workforce data gathered by OPM to respond to requests for information from Congress and/or the Executive Office of the President.
- TSA: Secure Flight Program.
- DHS via E-Verify: to verify employment suitability.

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

There are four different methods of data sharing:

- Interface – This applies to systems that are connected electronically, and owned by the same system owner.
- Connection – This applies to systems that are connected electronically, internal to DoS, that fall under the purview of the Department's Designated Approval Authority.
- Interconnection - This exists when an application under the Department's Designated Approval Authority shares information through a direct electronic connection, with another agency or entity outside of the Department.
- Information Sharing – this applies to those situations where direct electronic interfaces between systems do not exist and where information is passed using manual processes such as downloading a file from a secure website or receiving it from email, or secure FTP. This applies to all sources of data whether internal or external to the Department.

All IPMS internal data sharing is transmitted via the Department of State's intranet, OpenNet. OpenNet is the principle data network supporting all Department of State's sensitive but unclassified IT services. OpenNet is also a dedicated agency network for the secure transmission of Sensitive But Unclassified information among Department of State component offices, domestically and overseas.

Most connections are automated between servers with other Department bureaus within IRM managed OpenNet. Methods of data sharing include Oracle database sockets, flat text file transfer, SQL table transfer, XML file transfer, and secure ftp.

External sharing is as follows:

- TSA Files are placed into Secure Flight dropzone within DHS. Access to Secure Flight is limited to authorized DoS and DHS TSA personnel. Once the authorized user is authenticated, files will be placed into the Secure FTP flight dropzone. Upon completion (or attempt) to open the file, Secure Flight personnel will send an email notification to the list provider (Department of State) indicating the disposition of the attempt. Files are generated and delivered on a weekly basis.

- IPMS data is shared electronically with OPM via secure connection in accordance with the Central Personnel Data File (CPDF) and Enterprise Human Resource Integration (EHRI) reporting requirements. The MOU between OPM and the Department of State requires the incorporation of all electronic safeguards required by both agencies, for submittal of CPDF and EHRI reportable data elements.

- DHS (E-Verify) information is shared utilizing the DHS secure portal in accordance with the MOU established between DHS and the Department of State. Access to E-Verify information is strictly limited to authorized DoS personnel on a valid need-to-know basis for conducting official U.S. Government business between DHS and DoS.

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

IPMS implements Data at Rest Encryption to protect data at rest and Transport Layer Security (TLS 1.2) to protect data in motion. All IPMS internal data sharing transmits information via OpenNet. Security controls for sharing include access control, identification and authentication, audit and accountability, system communications, and system information integrity. For each sharing arrangement,

procedural and technical security controls are in place to protect the data in transit and at rest. Use of data encryption, audit log reviews, data masking and separation of duties are some of the controls in place to mitigate the risk of data and information exposure. Full security controls are included in the IPMS System Security Plan (SSP) and align with the National Institute of Standards and Technology's (NIST) SP 800-53 R4 minimum security control baseline for a Federal Information Processing Standard (FIPS) Publication 199 moderate system categorization.

For external data sharing Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), and/or Interconnection Service Agreement (ISA) are in place to enforce the required management and technical security controls.

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

Unauthorized access to IPMS, data leakage and information exposure are concerns identified by HR. These risks are mitigated through adherence to and implementation of security controls in the IPMS system design and operation. Procedural and technical security controls, including permission and access controls, are in place to protect data in transit and at rest. Use of data encryption, audit log review, data masking and separation of duties are some of the controls in place to mitigate the risk of data exposure. Access to data is granted to systems administrators, helpdesk agents, HR specialists and hiring managers at a level commensurate with their need-to-know and database management responsibilities. The sharing of data is limited to carry out mission critical activities.

7. Redress and Notification

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

System of Record Notices STATE-31, STATE-24, STATE-05, and STATE-36 provide guidance for record access and amendment procedures. Individuals, who wish to gain access to or amend records pertaining to them, may do so through Information Programs and Services (A/GIS/IPS) as directed in the aforementioned SORNs.

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

☒Yes ☐ No

If yes, explain the procedures.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses. Individuals who are Department employees may update their accounts as needed. Individuals who are not Department employees may follow the notification and redress procedures stated in the System of Record Notice, STATE-31, STATE-24, STATE-05, and STATE-36.

Individuals may update personal record information to EAPS through the Phone Book application. Phone Book is used to review, validate, audit, and continuously manage individual contact information for overseas personnel. The application is used by employees responsible for updating contact information such as phone numbers and address information while under Chief of Mission authority. The data, once updated, is used to update the contact information available in EAPS.

For HROnline, an employee must have an active HROnline account to access any of several applications including GEMS. Employees have self-service accounts in GEMS.

(c) By what means are individuals notified of the procedures to correct their information?

STATE-31, Human Resource Records, along with the other SORNs provide guidance for record amendment procedures. Individuals who wish to amend records pertaining to them may do so through Information Programs and Services (A/GIS/IPS) as directed in the aforementioned SORNs. The procedures to correct employee information are provided by their HR officer.

8. Security Controls

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

The information in IPMS is secured through implementation of the minimum baseline of controls for a Moderate impact system for confidentiality, integrity, and availability. Security controls used in HROnline meet the requirements found in the NIST Special Publication 800-53 Rev 4 (NIST SP 800-53 Rev 4) which provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations. Access to the application from an end user or a user with elevated privileges is controlled by the application administrators. Application identifiers and authenticators are provisioned based on the NIST SP 800-53 Rev 4 and DoS requirements. The IPMS server

operating system, web servers, applications, and databases are configured according to the Diplomatic Security (DS) secure configuration standards. Account privileges to all IPMS applications are based on roles with the concept of least-privilege and need-to-know.

(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.

IPMS applications utilize Single Sign-On functionality provided by the IRM managed Active Directory. Applications in IPMS do not require an additional manual authentication step. Assignment of individual application access permissions are approved by the application or data owner and provisioned by HR/EX. User access is restricted based on least privilege and need-to-know. For the HROnline and EAPS child systems of IPMS, an applicant may request the access to each individual application with a corresponding role through the HR System Access Request (SAR) module available on the HROnline and HR Portal web pages. To access records, the individual must first be an authorized user of the Department of State's unclassified computer network. Each prospective authorized user must also sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and lists prohibited activities (e.g. curiosity browsing). A user name and password is created and user's access is restricted depending on their role and need-to-know.

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

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 audits logs monthly for unusual activity. System managers, key security and user personnel cooperate and work closely to implement access controls.

(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 IPMS. The Department of State requires all new employees and contractors to complete a Cyber Security Awareness Course (PS 800), that contains a Privacy component, provided by DS/SI, before or immediately after the employment start date and prior to being granted access to the system. All Department of State personnel must complete the Cyber Security Awareness Course yearly. In addition, the OpenNet account request form

signed by all employees and contractors who will have access to IPMS contains a "Computer Security Awareness Form" that includes privacy orientation. All Department employees are also required to take PA459-Protecting Personally Identifiable 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.

Yes IPMS and its child applications include access controls, encryption of data at rest, and in transit, and strong authentication. Privacy risks are mitigated through implementation of and adherence to security controls in the IPMS system design and operation. HR has adopted the Department-wide "Rules of Behavior for Protecting PII" that lists the privacy rules of behavior applicable to Department of State records, regardless of format, that include PII. Procedural and technical security controls, including permission and access controls, are in place to protect data in transit and at rest. Use of data encryption, audit log review, data masking and separation of duties are some of the controls in place to mitigate the risk of data exposure. Access to data is granted to systems administrators, helpdesk agents, HR specialists and hiring managers at a level commensurate with their need-to-know and database management responsibilities.

Lastly, access to PII is on a need-to-know basis and requires HR/EX approval. Requests to receive reports containing personnel sensitive information are reviewed for approval by HR/EX on a case-by-case basis. Technical detail for security controls in IPMS is found in the IPMS SSP, Appendix J: Minimum Security Controls.

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

The security measures above were influenced by the sensitivity of information being collected, processed and/or stored. As such, baseline requirements for a system with moderate impact rating for confidentiality, integrity, and availability were implemented. IPMS 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 Rev 1, 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 KC. NIST SP 800-53 Rev 4 security controls for a moderate system and privacy overlay controls were included in the design and operation of IPMS.

9. Data Access

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

IPMS applications utilize Single Sign-On functionality provided by the IRM managed Active Directory. Applications in IPMS do not require an additional manual authentication step. Assignment of individual application access permissions are approved by the application or data owner and provisioned by HR/EX. User access is restricted based on least privilege and need-to-know. To gain internal access to OpenNet, all IPMS users must maintain at least a SECRET security clearance level. For the HROnline and EAPS child systems of IPMS, an applicant may request the access to each individual application with a corresponding role through the HR System Access Request (SAR) module available on the HROnline and HR Portal web pages.

System Users	Roles and Responsibilities
System Administrators	Responsible for installing hardware, and operating system software onto Web servers and Database servers. Additional responsibilities include troubleshooting, support and maintenance. System administrators also plan for and respond to service outages and other problems.
Database Administrators	The Database Administrators (DBAs) are responsible for the administration and maintenance for both the Oracle 11g Release 2, and Microsoft SQL Server 2008 and SQL Server 2014 database applications. DBA's are also responsible for the integrity of the data and the efficiency and performance of IPMS as a system. Additional responsibilities include the use of DBA views (important Oracle metadata with details about tables, indexes, physical storage, etc.) edits and deletes.
SECREF Administrator Roles	System Administrator – This role is responsible for managing all user accounts that have access to applications under the HROnline umbrella. Developer – This role allows users to proxy in non-production environments. This also allows users to review the debug and error logs

	IPMS Support - This role allows users to enable/disable circuits and assign/remove roles for user accounts.
HROnline Privileged Roles	The following roles are used to administer the HROnline application: • Assignment Officer • Personnel Technician • Bureau • Consultative POC • Career Development Office
Developers	Develop and maintain IPMS software used for development.
Help Desk Agents	Help desk agents staff the HR/EX Help Desk and are responsible for supporting users of HR applications. In addition to regular users, HR Division Chiefs have power user roles allowing them administer rights to view, edit or delete user accounts. Helpdesk agents have the following functional responsibilities: • Determine and assign user roles and rights to include unlocking HROnline accounts • Account Request Management - QA all request forms, create tickets for all accounts/installs, scan and control all customer documents required for account creation, update permission
Human Resources (HR) Specialists	Human Resources (HR) Specialists provide a variety of human resource management services including consultation and advice to Department managers.
Civil Service (CS) and Foreign Service (FS) direct hire employees, contractors, dependents, FS Consular Agents, students, other USG Agency employees under COM authority, and resident US citizens	Authorized IPMS users access the system through one of the six subsystems (i.e., GEMS, HROnline, EAPS, WebPS, KC, and HRCC). User roles and responsibilities for each IPMS subsystem are addressed below accordingly. **GEMS** With the exception of system administrators, all users authorized to access the GEMS subsystem do so to utilize the Department's corporate human resources management information systems self-service application that includes employee and manager self-service, benefits management, competency management, and performance management functionality. **HROnline** HROnline is HR's primary intranet portal for employees to access self-service applications to view, edit and delete their information.

	WebPS (PSCDB) Users that access the Web Post Personnel System (WebPS), are responsible for all aspects of overseas position management to include the viewing, editing, deleting and the administration of overseas position and staffing information of Locally Employed Staff (LES) as well as for record keeping and tracking of American employees while assigned abroad for both State and other United States Government (USG) agencies under Chief of Mission authority. WebPS users are generally from other agencies and are likely to be physically located abroad at Post. The Post Personnel Common Database (PSCDB) is the instance of WebPS that is considered within the IPMS authorization boundary. WebPS is a child of the Web Post Administrative Software Suite Explorer (WebPASS) and are included under the WebPASS authorization boundary. **EAPS** Users that are from Washington-based Executive Branch agencies (EAs) and other agencies with an overseas post presence access the EAPS subsystem, to review, validate, audit, and continuously manage positions in a near real-time environment. EAs are responsible for the review and validation of their reported post presence. **KC** Users of the Knowledge Center (KC) include: systems administrators, database administrators, helpdesk agents, HR specialists, and hiring managers. To access the KC, users must first be authenticated and granted access to the SAP BusinessObjects XI 3.1 SP6 environment. Within the BusinessObjects environment, user are responsible for creating, retrieving, and modifying existing corporate reports and documents, and to distribute such reports to other KC and non-KC users to meet business requirements. In addition, through the InfoView website, users are able to create their own ad-hoc reports based on the consolidated data in the Knowledge Center data warehouse. **HRCC** Users of the Human Resources Customer Connection (HRCC) system include: system administrators, helpdesk agents, HR specialists, and users. Access to the HRCC system is handled

	through single sign-on with OpenNets Active Directory. Role authorization is handled by the GEMS system. That is, user roles are controlled within the GEMS architecture and passed through HRCC.

(b) How is access to data in the system determined?

Access to data in the system is determined by the individual's role and authorized responsibility.

To access records, the individual must first be an authorized user of the Department of State's unclassified computer network. Each prospective authorized user must also sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and lists prohibited activities (e.g. curiosity browsing). A user name and password is created and user's access is restricted depending on their role and need-to-know

(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.

No. User access is restricted to only those roles for which their position is authorized. Individual record information is available only to the user with appropriate privileges and their supervisor when applicable.

(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. Each prospective IPMS authorized user must sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the individual to perform his or her official duties and is also a formal acceptance of responsibility to notify HR/EX by phone or email when access to the system is no longer approved or valid for the respective user. Audit Logs are maintained to record system and user activity including invalid logon attempts and access. The HR Information System Security Officer (ISSO) conducts monthly audits

of IPMS to monitor the audit logs for unusual activity. System managers and user personnel work cooperatively to implement access controls.