PRIVACY IMPACT ASSESSMENT

Integrated Personnel Management System (IPMS)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: February 2022
(b) Name of system: Integrated Personnel Management System
(c) System acronym: IPMS
(d) Bureau: Global Talent Management (GTM)
(e) iMatrix Asset ID Number: 951
(f) Child systems (if applicable) and iMatrix Asset ID Number:

- Global Employment Management System (GEMS) iMatrix # 135
- Overseas Personnel System (OPS), iMatrix # 7305
- HROnline (HROnline), iMatrix # 728
- Knowledge Center (KC), iMatrix # 729
- Executive Agency Personnel Support (EAPS), iMatrix # 2738

(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): N/A

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:

IPMS is a multi-year, mixed-lifecycle system that incorporates the underlying technical architecture for all OpenNet applications managed by the GTM Executive Office (GTM/EX). IPMS is used to manage personnel information for Department of State (State) 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 U.S. citizens employed by U.S. missions abroad.

IPMS includes over 60 subsystems. This PIA only covers the five IPMS "pillar" child systems listed in 2f above.

- The Global Employment Management System (GEMS) is State's corporate human resources management information system, which provides comprehensive employment data for all direct-hire State employees. It serves as State's primary transactional system of record for human resources/personnel data.
- The Overseas Personnel System (OPS) is an automated human resources system for managing overseas position and staffing information of Locally Employed Staff (LE Staff) as well as for record keeping and tracking of American employees while assigned abroad for both State and other United States Government (USG) agencies, including the United States Agency for International Development (USAID), under Chief of Mission (COM) authority.
- HROnline is the primary intranet portal for State users to access self-service and non-self-service IPMS subsystems which allows employees and contractors to view and edit employee profiles, perform foreign service position bidding functions, submit and review travel claims, submit and review employee grievance cases, view and maintain an employee's Electronic Official Personnel File (eOPF), view, submit, and manage student loan repayments, and perform emergency evacuation functions.
- The Knowledge Center (KC) Portal is a data warehouse of human resource (HR) data used for personnel and position reporting. KC ingests data from IPMS child systems GEMS and OPS. It also ingests data from GTM Next and FSI eternal to GTM, and from the Department of Labor (DoL) external to State to allow for powerful customized queries and reports.
- The Executive Agency Personnel Support (EAPS) is used to review, validate, audit, and continuously manage individual agencies overseas personnel, assignment, and position data of American and Locally Employed Staff (LE Staff) under Chief of Mission authority. The validated data is used for record keeping and tracking of American employees while assigned abroad and LE Staff for both State and other United States Government (USG) agencies.

Together, all IPMS subsystems 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 through seamless online workflow processes.

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

- Social Security Number (SSN), Full
- Employee System ID (EmpID)
- State Global Unique Identifier (SGID)
- First Name
- Last Name
- Birth Date
- Birth Country
- Birthplace
- Age
- Legal Residence (Address)/Physical Address
- Spouse/Cohabitant Name
- Spouse/Cohabitant SSN
- Gender
- Race and National Origin
- Known Traveler Number
- Handicap
- Med Clearance Code
- Employee Benefits – Benefit Selections
- Employee Review/Performance/Grievance Data
- Financial Information
- Legal Information
- Disability Status
- Education Information (schools, education level, degree information, student loan details, etc.)
- Email Address (Gov't and Personal)
- Security Clearance Level
- Beneficiary Data and Dependent Information
- Death Certificate
- Name and Location of Position's Organization
- Retirement Plan, Citizenship
- Evacuee Contact Information
- Passport Number
- Telephone number(s) (Gov’t and Personal)
- Alien Registration Number/USCIS Number
- Foreign Passport Number and Country of Issuance
- Visa Number (when applicable)
- Driver’s License Information

(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)
- 26 CFR 301.6109, Taxpayer identification
- 20 CFR 10.100, Federal Workers' Compensation

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

☒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 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)): N/A

- Disposition Authority Number: DAA-0059-2020-0021-0001; DAA-0059-2020-0021-0006; DAA-0059-2020-0021-0018

- Length of time the information is retained in the system:
  Permanent. Cut-off at end of calendar year of case closure. Transfer to the National Archives 25 years after cutoff.

- Type of information retained in the system:
  Records documenting the policies, procedures, plans, and guidelines in executing the Global Talent Management program for the Department of State. Records include program activities and policy and procedural matters relating to recruitment and employment, the examination process, classification and position designation memorandums and reports, performance evaluation, Presidential Appointments, and Title and Rank records. Records also include precepts, promotion lists, and reports related to the Foreign Service Selection Board, Global Employment Management System monthly and annual reports, Foreign Service disputes panel appeals case files, policy coordination historical and project reports files, suitability correspondence and memorandums of Foreign Service personnel, and all related substantive documentation and meeting minutes, related to global talent management records.

  Records include Foreign Service Officer yearly written examinations, agendas and minutes of the Board of Examiners of the Foreign Service, reader reports, correspondence and memoranda related to the preparation and grading of Written Examinations, procedures for oral examinations, lists of candidates designated for appointment, and other related substantive material on examinations.

  High profile casualty assistance case files related to Civil Service and Foreign Service personnel, including eligible family members, involved in serious injury, hospitalization, or death due to acts of terrorism, hostage affairs, or other distinctive activities that attract media, Congressional, or public interest. Records include, but not limited to notes, email communications, memorandums, explanation of benefits, and condolence letters.

- Schedule number (e.g., (XX-587-XX-XXX)): N/A

- Disposition Authority Number: DAA-0059-2020-0021-0007; DAA-0059-2020-0021-0009; DAA-0059-2020-0021-0010; DAA-0059-2020-0021-0011; DAA-0059-2020-0021-0012; DAA-0059-2020-0021-0016

- Length of time the information is retained in the system:
  Temporary. Cutoff at the end of calendar year of case closure or of appointment examination. Destroy when survivor or retirement claims are adjudicated or when records are 60 years old. Destroy 10-15 years after cutoff. Destroy 20 years after date death, attainment of age 62, or case closure. Destroy 10-20 years after date of separation from Foreign Service. Cutoff at the end of the calendar year.

- Type of information retained in the system:
  Records of grievance, discipline, and adverse action case files for Foreign Service Officers. Records include statements of grievance, supporting documentation, witness statements, interviews, hearings, and referral documentation to the Foreign Service Grievance Board. Discipline case files include documentation connected with any allegation of employee misconduct submitted for review for disciplinary action for any employee on Foreign Service appoint. Records include but not limited to reports of investigation, administrative inquiries, communications relevant to the allegations of misconduct, disciplinary, or administration action. Case files include proposed actions by deciding officials and resolution or action taken.
  Long Term personnel records of separated Locally Employed Staff (LES) and Personal Service Contract (PSC) employees consists of record copies of documents covering the entire service as prescribed in the Federal Personnel Manual and related Departmental guidelines.

  Records include documentation, correspondence, and dossiers of Foreign Service reappointment and unsuccessful candidates, qualification reports, summaries, rating sheets, and reports of oral examination. Records also include applications for designation to take written examinations, examination results, and answer sheets.
  Records consists of application for retirement, staff studies on voluntary or disability retirement, correspondence and documentation related to contributions to the Foreign Service Retirement System, prior service credit, Civil Service Retirement deductions, appointment data, applicable annuitant and non-annuitant information, precedent and Board of the Foreign Service separation case files, and health benefit files.

  Records consists of correspondence related to the submission of performance ratings and supplemental data for inclusion in the Foreign Service employee's performance folder. Records include comments concerning ratings, performance evaluation matters, rebuttal information, commendations, training reports, summary reports, and letters of reprimand. Also included is automated score card information such as biographic data, tenure dates, promotion history, rankings, skill codes, and related senior threshold board files.
  Records of the Global Community Liaison Office consisting of subject and historical documents including reports and memorandums. Records also include evacuation,

naturalization, employment program files, and Community Liaison Office country/posts and coordinator files.

- Schedule number (e.g., (XX-587-XX-XXX)):
- Disposition Authority Number:
  DAA-GRS-2014-0002-0011 (GRS 2.1, item 060)
- Length of time the information is retained in the system:
  Temporary. Destroy 1 year after date of submission.
- Type of information retained in the system:
  Application packages for competitive positions. These packages include the application, resume, supplemental forms, and other attachments including correspondence with the applicant.

- Schedule number (e.g., (XX-587-XX-XXX)): N/A
- Disposition Authority Number: DAA-GRS-2014-0004-0003 (GRS 2.5, item 020)
- Length of time the information is retained in the system:
  Temporary. Destroy 1 year after date of separation or transfer.
- Type of information retained in the system:
  Records not included in separating employee's Official Personnel Folder (eOPF), documenting individual employees' transfer to another Federal agency or office or voluntary, involuntary, disability, early retirement, retirement, or death separation from career, temporary, and political appointment service, and legal and financial obligations of government to employee and employee to government.

- Schedule number (e.g., (XX-587-XX-XXX)): N/A
- Disposition Authority Number: DAA-GRS-2016-0015-0011 (GRS 2.4, Item 090)
- Length of time the information is retained in the system:
  Temporary. Destroy 3 years after date of approval, completion of service agreement, or termination of incentive or differential payment, whichever is later.
- Type of information retained in the system:
  Records of recruitment, relocation, and retention incentives; federal student loan repayment; and supervisory differentials offered under the Federal Employees Pay Comparability Act.

- Schedule number (e.g., (XX-587-XX-XXX)): N/A

- Disposition Authority Number: DAA-GRS-2017-0011-0001 (GRS 2.1, item 050)

- Length of time the information is retained in the system:
  Temporary. Destroy 2 years after selection certificate is closed or final settlement of any associated litigation; whichever is later.

- Type of information retained in the system:
  Case files created when posting and filling competitive job vacancies to include case examining, competitive examination, merit promotion applicant case files, Senior Executive Service staff files, priority consideration files, and requests for personnel actions.

- Schedule number (e.g., (XX-587-XX-XXX)): N/A

- Disposition Authority Number: DAA-GRS-2017-0007-0004 (GRS 2.2, item 040); DAA-GRS-2017-0007-0005 (GRS 2.2, item 041); DAA-GRS-2017-0007-0008 (GRS 2.2, item 070)

- Length of time the information is retained in the system:
  Temporary. Destroy when survivor or retirement claims are adjudicated or when records are 129 years old, whichever is sooner, but longer retention is authorized if required for business use. Destroy when superseded or obsolete, or upon separation or transfer of employee, whichever is earlier. Destroy no sooner than 4 years after date of appraisal.

- Type of information retained in the system:
  Records of separated employees saved to the "permanent" folder in the eOPF include, but not limited to, career development case files on Foreign Service (FS) Officers and staff employees such as correspondence relating to assignment preferences, career development, training, and transfers. Also includes applications for FS retirement case files, annuitant and non-annuitant service record case files, FS former spouse health benefit files, Civil Service retirement case files, and Board of the Foreign Service separation case files.

  Records of separated employees saved to the "temporary" folder in the eOPF include, but not limited to, short-term files concerning travel of Foreign Service (FS) officers, FS residence and dependency reports, certificate of incapacity files, and travel orders and related assignment correspondence.

  Records include performance ratings, commendations, inspector reports, official reprimands, end-use summary reports, correspondence with Foreign Service (FS) and Civil Service employees regarding submission of performance ratings and supplemental data, and selection board administrative files.

- Schedule number (e.g., (XX-587-XX-XXX)): N/A

- Disposition Authority Number: DAA-GRS-2018-0002-0006 (GRS 2.3, item 060)

- Length of time the information is retained in the system:
  Temporary. Destroy no sooner than 4 years but no later than 7 years after case is closed or final settlement on appeal, as appropriate.

- Type of information retained in the system:
  Records of grievances filed by covered entities (for instance, employees who are not members of a bargaining unit). Records of disciplinary and performance-based actions against employees. Records of adverse actions (suspension, removal, reduction in grade, reduction in pay, or furlough) against employees.

  Note 1: Letter of reprimand filed in an employee's Official Personnel File is scheduled by GRS 2.2, item 041.

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, as amended, Federal employment
  - Executive Order 13478 (Amendments to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers)
  - 20 CFR 10.100, Federal Workers' Compensation

(d) How is the PII collected?

Internal to the Department of State, employees, managers, and HR specialists use the child systems with web interfaces to comprise the data stored in IPMS.

Additionally, IPMS child systems collect PII from the following internal Department of State Bureaus/Offices:

- Foreign Service Institute (FSI) - PII is collected from the Student Training Management System (STMS) via electronic data interchange (secure web services and database link) and manual file exchange via file share server with role-based access controls.
- Comptroller and Global Financial Services (CGFS) - PII is collected from the Global Foreign Affairs Compensation System American (GFACS AME) and Locally Employed Pay (GFACS LE) applications via electronic data interchange (Secure File Transfer Protocol - SFTP) and manual file exchange via file share server with role-based access controls.
- Medical Services (MED) - PII is collected from eMED via electronic data interchange (secure web services and database link).
- Diplomatic Security (DS) - PII is collected from Department of State Clearance System (DOCS), DS Employee Tracker (DS-ET), and the Identity Data Management System (IDMS) via electronic data interchange (secure web services).
- Information Resources Management (IRM) - PII is collected from GTM Next, which is hosted within the Cloud Program Management Office (CPMO)'s ServiceNow platform via secure web services. PII is also collected from Active Directory when users initially register on HROnline. PII is also collected by GTM Talent Acquisitions (TAC) staff members via IRM's Foreign Affairs Network (FAN), which is hosted in Google's FedRAMP approved Cloud (manual file upload to GEMS or to HROnline's child system eOPF).
- European and Eurasian Affairs (EUR) - PII for non-U.S. Citizens is collected from the Global Application Development Group (ADG) via electronic data interchange (secure web services) from the GoMBC (Merit Based Compensation) system.

External to the Department of State, IPMS collects PII from the following organizations:

<u>Department of Labor (DoL)</u>

- State receives data extracts on a weekly, monthly, or quarterly basis from DoL Office of the Chief Information Officer (OCIO) via SFTP protocol on a secure isolated landing zone (i.e., secure trusted zone). The data extracts may include case management, medical payment, compensation payment, and/or chargeback related information. When received by GTM, the Office of Workers' Compensation Programs (OWCP) stores the PII in State's Workers Compensation Database, a component application of IPMS which is limited to Authorized State

Personnel. Aggregated OWCP data is also stored in the Knowledge Center (KC) for reporting purposes.

Pearson VUE

- Pearson VUE is a commercial contractor that maintains the Foreign Service Officer Test (FSOT) application that is used to administer the online Foreign Service Written exam. The information is used by the Human Resources Talent Acquisitions Division (GTM/TAC). GTM/TAC logs into the Pearson VUE server through encrypted secure file transfer protocol (SFTP) to pull candidates' PII and upload into Recruitment Examination Evaluation Tracking Application (REETA), which is a child of HROnline, for processing (through Qualifications Evaluation Panel application).

Monster Government Solutions (MGS)

- GTM/TAC logs into Monster Gateway to State (GTS) server through encrypted secure file transfer protocol (SFTP) to pull applicants' PII and upload into IPMS for processing in the Monster Government Solutions Data Processor (MDP), which is a component of IPMS. GTM/EX/SOD application administrators also have access to GTS to manage application data ingested into IPMS.

Kiteworks (GTM SecureShare)

- Kiteworks is a FedRAMP approved Software as a Service (SaaS) solution that provides a secure file exchange and document storage solution. GTM uses Kiteworks to exchange Office of Personnel Management (OPM) forms necessary for benefit claims, annuitant updates, on-boarding/off-loading processes, and other human resource functions. Kiteworks also enables GTM to securely obtain required forms from other federal agencies including the Office of Personnel Management (OPM), Government Accountability Office (GAO), the White House, the DOL, and the DOD. The forms are then uploaded to eOPF and/or GEMS.

Other Government Agencies (OGAs)

- Other Government Agencies, including employees and contractors from the United States Agency for International Development (USAID), the Department of Agriculture (DoA), and the DoD serving under Chief of Mission (COM) Authority at Department of State posts have all personal data needed for identification, authentication, reporting, and payroll input into the Overseas Personnel System (OPS). Personal data for this category of employee is input directly into OPS by users or human resource specialists.

(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?

Employee data integrity and completeness within IPMS are checked using internal management reports and quality reviews. Wherever applicable, data integrity rules validate data received by IPMS child systems from State and external data sharing partners. If the data pertain to an employment application, the applicant is responsible for the accuracy of the information. The applicant is responsible for verifying his/her personal and demographic information in the application process and making changes to his/her profile as needed. For eligible family members, as defined by 5 FAM 784-785, the employee is responsible for ensuring the accuracy of information.

GEMS: Employees are responsible for ensuring the accuracy of their information in GEMS. Data from DS, MED, GTM Next, Foreign Service Officer Test (FSOT) hosted by Pearson Vue, and Monster/GTS are validated against business rules prior to ingestion into GEMS. GEMS position and employee data are consumed by all IPMS child systems to ensure accuracy in those systems.

OPS: Some employee information in OPS is extracted from GEMS while some is entered by the employee. Supervisors, Security Administrators and Government Project Managers review forms completed by employees in OPS for accuracy. Data from EUR (ADG) is validated against business rules prior to ingestion into OPS.

HROnline: HROnline serves employee self-service and non-self-service functions to allow users to submit human resource actions such as grievance and travel claims for themselves or others. Human Resource Officers compare PII submitted by users against PII contained in GEMS or OPS to ensure accuracy.

KC: Data from DoL, FSOT, and Monster/GTS are decrypted and then validated against business rules prior to ingestion into KC.

EAPS: Locally Employed Staff and/or Other Government Agency employees under Chief of Mission Authority at posts' 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 are updated at post, the program will submit the data to the EAPS database. This completes the data transaction cycle. Data from EUR (ADG) are validated against business rules prior to ingestion into EAPS.

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

Yes, the information collected, maintained, and processed by IPMS and its child systems is current. Procedures to ensure information remains current include allowing the user to make modifications with self-service functions within each child system. If the user recognizes out-of-date information, they may submit changes to the information in their records to the HR Help Desk or via another system maintained within GTM.

(h) 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.

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

IPMS collects the absolute minimum amount of PII required to satisfy its statutory purposes and the mission of the Bureau of Global Talent Management. Functional changes to IPMS are reviewed to ensure that the use and collection of PII is necessary prior to implementation of additional PII collection and storage.

5. Use of information

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

The information is used specifically for the following business purposes:

- Facilitate domestic and overseas workforce onboarding, management, planning, employee services, employee conduct, suitability, and grievance resolution, and employee and family support (GEMS, OPS, HROnline, KC).
- Retain and maintain mandatory Electronic Official Personnel File (eOPF) documents and forms (GEMS, HROnline).
- Review, validation, auditing, and continuous management for Washington, D.C.-based Executive Branch Agencies (EAs) for the individual EA presence overseas in a near real-time environment (EAPS, OPS).
- Provide support for the overseas review and correction of employee and position records that exist at EAs in Washington and individual embassies and consulates (EAPS).
- Allow users to create travel authorization documents for persons evacuated during a crisis (EAPS).
- Provide automation of the DS-1552 - Leave Data-Departure for Post and the DS-1707 - Leave, Travel, and Consultation Status (HROnline).
- Provide reporting and metrics on recruitment, diversity, and other human resource related statistics (KC).
- Verify contractors registering for HROnline access.
- Track all personnel, including other government agency (OGA) personnel, under Chief of Mission (COM) Authority at each overseas installation, regardless of employment category, and serve as the system of record for Locally Employed (LE) Staff under COM (OPS).

(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. IPMS and its child systems allow for GTM to provide for workforce management, workforce planning, employee services, employee, and family support, verifying contractors, and to serve as State's system of record for human resources.

(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?

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 Locally Employed Staff (LE Staff) salary analysis.

(2) Does the analysis result in new information?

Yes, the analysis may result in new information. Information that may be produced includes 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 LE Staff 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 State.

(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.

IPMS maintains a test or staging environment that utilizes production data, including real PII, for production support troubleshooting, Assembly Testing, and User Acceptance Testing. This test or staging environment is included in the IPMS Authority to Operate (ATO) boundary and all servers, accounts, and databases within the test/staging environment are configured, controlled, and secured at the same level as production. All users with access to IPMS applications in production will also have the same access/roles in test/staging. In addition, GTM/EX Business Analysts, Independent Verification & Validation staff, Functional Owner representatives, and Production Support staff who are all cleared U.S. citizens may obtain limited access to the test/staging environment based upon business need, and direct-hire supervisor and GTM ISSO approval. User access and activities in the test/staging environment are audited and movement of data restricted.

6. Sharing of PII

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

Internal: IPMS shares information with the following internal bureaus and offices:

- Bureau of Global Talent Management (GTM) – GEMS, HROnline
- Bureau of Information Resource Management (IRM) – GEMS, KC, HROnline
- Foreign Service Institute (FSI) – GEMS, OPS
- Office of Medical Services (MED) – GEMS, OPS, EAPS
- Bureau of the Comptroller and Global Financial Services (CGFS) – GEMS, OPS
- Bureau of Diplomatic Security (DS) – GEMS, OPS, EAPS
- Bureau of Administration (A) – GEMS, OPS
- Overseas Building Operations (OBO) – GEMS, OPS
- Bureau of European and Eurasian Affairs (EUR) – OPS, EAPS
- Office of Management, Strategy, and Solutions (M/SS) Center for Analytics (CfA) – KC, GEMS, OPS, HROnline
- All Bureaus and Posts – GEMS, OPS, KC, HROnline, EAPS

External: IPMS shares information with the following external organizations:

- Office of Personnel Management (OPM) – GEMS, KC, HROnline
- Transportation Security Administration (TSA) - GEMS
- Department of Homeland Security (DHS) – GEMS
- Pearson Vue (Foreign Service Office Test and OnVUE) – GEMS, HROnline
- National Resident Matching Program (iMatch) - GEMS
- Dr. Campion (Campion Consulting) - HROnline
- Department of Defense (DOD) and Other Government Agencies (OGAs) - GEMS, OPS, EAPS

(b) What information will be shared?

Internal: The following information is shared internally:

- GTM: PII related to a person, including beneficiary and family member information, position, training, SGID/ Employee ID, and transaction data from GEMS and OPS.

- IRM: PII related to a person, including beneficiary and family member information, position, training, SGID/Employee ID, pay plan, grade, tenure, skill code, and transaction data from.
- FSI: Employee information including position, salary, location, and organization data.
- MED: Employee and dependent medical information.
- CGFS: Employee's salary and benefits information.
- DS: Employee and applicant person data, employee position, disciplinary action data, and contractor's data.
- A: Employee information necessary for case management, logistics, and official travel; and human resource records for record retention/disposition.
- OBO: Overseas position information.
- EUR: Person and position data for Locally Employed Staff.
- M/SS CfA: Applicant and employee position data.
- All Bureaus/Posts: employee and applicant data, and employee position and disciplinary action data. Bureau and Post users must submit ad-hoc report requests to the GTM/EX Help Desk providing their report needs, need to know, and direct-hire supervisor approval for reports that contain PII.

External: The following information is shared externally:

- OPM: Information relating to civilian employees, including positions and employees in the competitive, excepted, and Senior Executive services. Data is shared from GEMS, KC, and OPS.
- TSA: Known Traveler Number (KTN), full name (First, Middle, and Last), gender, race, national origin, and date of birth
- DHS: 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 an email), Citizenship Status, First Date of Employment, and Visa Number (when applicable) is entered DHS' E-Verify. If Driver's License is used, state is also entered. For some cases a copy of the employee's photo documentation is required.
- Pearson VUE: Applicant information including applicant ID and name is shared with Pearson VUE's Foreign Service Office Test (FSOT) system
- National Resident Matching Program (iMatch): Direct-hire name and email address.
- Dr. Campion (Campion Consulting): Applicant written exam records are stripped of all identifying PII. PII fields are stripped but applicants have several long-character fields in which to input narratives – some narratives may contain PII. Data from HROnline are also transmitted to Dr. Campion.
- Department of Defense (DOD) and Other Government Agencies (OGAs):
  - Forms and documents required as part of eOPF are shared with gaining agencies and/or the DOD when employees depart State.
  - Personnel reports for OGAs, including USAID, are provided upon request from OPS/EAPS to designated human resource specialist employees of the OGAs.

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

Internal: The intended purposes for sharing are to support the following:

- GTM: Information is shared with HRNet, GTS, and Personnel Reporting and Statistics (PRAS) to support hiring, retention, diversity, and position analysis for State.
- IRM: Department-wide reporting from the Career Development Archive Retrieval System (CDARS); Single-identity provisioning and continuous Diagnostic and Mitigation reporting for State Enterprise Identity Credential, and Access Management (SE-ICAM); human resource case management, telework and performance management, and on-boarding processes.
- FSI: State's training process by sharing person, agency, position, and location data needed for FSI to validate eligibility for training and mandatory training modules required.
- MED: The Foreign Service medical clearance process.
- CGFS: The payroll process.
- DS: State's State Global Unique Identifier (SGID) and authentication processes, and personal data to necessary to initiate and verify clearances.
- A: Travel, logistics, and parking processes.
- OBO: Annual Capital Security Cost Sharing (CSCS) and Space Requirements Planning processes for Rightsizing Position Management Functionality.
- EUR: Merit-based compensation and awards for Locally Employed Staff.
- M/SS CfA: Department-wide reporting and data sharing.
- All Bureaus/Posts: Reporting and trend analysis of hiring, staffing patterns, and other human resource related topics of interest to Bureaus, Offices, and Posts.

External: The intended purposes for sharing are to support the following:

- OPM: Requests for information from Congress and/or the Executive Office of the President.
- TSA: The secure flight program.
- DHS: Verify employment suitability.
- Pearson VUE: Pearson VUE scheduling of oral and written FSOT exams.
- National Resident Matching Program (iMatch): Algorithmic ranking of position bids.
- Dr. Campion (Campion Consulting): Analysis of the written portion of the FSOT and applicant/test taker metrics.
- Department of Defense (DOD), USAID, and Other Government Agencies (OGAs): Ensure that forms/documents required as part of Electronic Official Personnel Folder (eOPF) are shared as required with gaining agencies and/or the

DOD when employees depart State; provide tracking of all non-State employees/contractors under Chief of Mission (COM) Authority at US Posts and allow for necessary reporting and financial accounting.

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

Internal: There are four different methods of data sharing:

- Interface – This applies to systems that are connected electronically and owned by the same system owner. (GTM)
- Connection – This applies to systems that are connected electronically, internal to State, that fall under the purview of State's Designated Approval Authority. (IRM, FSI, MED, CGFS, DS, A, OBO, EUR)
- Interconnection - This exists when an application under the State's Designated Approval Authority shares information through a direct electronic connection, with another agency or entity outside of State.
- 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. (GTM, CGFS, M/SS CfA, and all Bureaus and Posts)

Most of IPMS internal data sharing is transmitted via the Department of State's intranet, OpenNet. OpenNet is the principal data network supporting all Department of State's Sensitive But Unclassified (SBU) Information Technology (IT) services. OpenNet is also a dedicated agency network for the secure transmission of SBU information among State component offices, domestically and overseas.

Most connections are automated between servers with other State bureaus within IRM managed OpenNet. Methods of data sharing include Oracle database sockets, database links, flat text file transfer, SQL table transfer, XML file transfer, encrypted email, secure ftp (SFTP), and secure web services. Data sharing is secured by firewall rules, the State's Public Key Infrastructure (PKI) technology, and/or service accounts/passwords which are changed at least every 60 days per State policy.

Data from IPMS is also shared internally via DS managed Microsoft O365 SharePoint site. IPMS users upload disciplinary files for DS investigators to review. The files are automatically deleted within a standard set time period.

For sharing with GTM's PRAS system, select IPMS data is copied to a State approved, encrypted hard drive and uploaded to the PRAS network for use in providing aggregated data on State staffing patterns. PRAS transmission methods are covered in that system's PIA.

External:

- OPM: IPMS data is shared electronically with OPM via secure connection in accordance with the Enterprise Human Resource Integration (EHRI) reporting requirements. The Memorandums of Understanding (MOU) between OPM and the Department of State requires the incorporation of all electronic safeguards required by both agencies, for submittal of Central Personnel Data File (CPDF) and EHRI reportable data elements.
- TSA: TSA Files are placed into Secure Flight dropzone within DHS. Access to Secure Flight is limited to authorized State and DHS TSA personnel. Once the authorized user is authenticated, files will be placed into the Secure FTP flight dropzone using an approved secure file transfer protocol tool. 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.
- DHS: (E-Verify) information is shared utilizing the DHS secure portal in accordance with the MOU established between DHS and the Department of State.
- Pearson VUE: FSOT information is shared utilizing State encrypted emails or password protected files sent via State unencrypted email with password provided separately.
- National Resident Matching Program (iMatch): Information is shared by GTM/Career Development and Assignments (CDA) staff uploading select lists of State direct-hire names and email addresses directly into the iMatch system.
- Dr. Campion (Campion Consulting): FSOT written test data is shared by GTM/TAC/BEX and GTM/EX/OTS/SDD staff via email.
- DoD and Other Government Agencies (OGAs): Information is shared utilizing encrypted emails, DOD SAFE, and/or the GTM Contractor Owned, Contractor Operated, FedRAMP approved secure file share Kiteworks Cloud solution.

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

Internal: IPMS implements Data at Rest Encryption to protect data at rest and Transport Layer Security (TLS 1.2) to protect data in transit. Most 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. In addition, GTM maintains signed data sharing agreements between GTM and other Bureaus/Offices in MOUs to ensure that the data elements, methods of sharing, security responsibilities including personnel clearance requirements, and incident response procedures are documented, reviewed, and agreed to by all stakeholders.

External: For external data sharing, Memorandums of Understanding (MOU), Memorandums of Agreement (MOA), and/or Interconnection Service Agreements (ISA) are in place to enforce the required management and technical security controls. IPMS implements Data at Rest Encryption to protect data at rest and Transport Layer Security (TLS 1.2) to protect data in transit and ensures that external data sharing partners implement similar encryption controls to safeguard shared PII data. In addition, GTM documents requirements for appropriate access control and user supervision in data sharing agreements with external entities. For system-to-system data sharing agreements with external entities, GTM documents a requirement for the external system to have or to be in the process of obtaining an Authority to Operate issued by a Federal Agency or the Federal Risk and Authorization Management Program (FedRAMP) Program Management Office (PMO).

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

For Department of State employees, a PAS is posted on the login screen for HROnline, which acts as the gateway for access to GEMS and OPS.

EAPS and KC are mainly reporting applications and do not collect PII directly from users/applicants, so notice is not provided.

(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?

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

IPMS is not the initial point of collection, so individuals do not have the opportunity to decline to provide their information in most instances. Consent is provided by individual State employees and employees of other government agencies when they provide their information at the initial point of collection for the source systems.

As a child system of IPMS, an individual may input their information into HROnline. The individual may decline to provide information, but the refusal to do so would restrict their ability to complete employee/manager system processes.

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

Individuals, who wish to gain access to or amend records pertaining to them, may do so through Information Programs and Services (A/GIS/IPS). The procedures are detailed in the following System of Record Notices (SORNs): STATE-31, STATE-24, STATE-05, and STATE-36. Individuals may also access their information directly in GEMS, OPS, EAPS, HROnline, or KC.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals who are State employees may update their information as needed by directly accessing the child systems. For HROnline, an employee must have an active HROnline account to access any of several applications including GEMS and OPS. Employees have self-service accounts in GEMS.

Individuals who are not State employees may follow the notification and redress procedures stated in System of Record Notices STATE-31, STATE-24, STATE-05, and STATE-36.

Individuals may update personal record information in EAPS through the Phone Book application within the system. Phone Book is used to review, validate, audit, and continuously manage individual contact information for overseas personnel.

If no, explain why not.

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

The procedures to correct employee information are provided to employees by their HR officer. Individuals who are not employees are notified of the procedures to correct their information via the SORNs listed above.

8. Security Controls

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

The information in IPMS is secured through implementation of the minimum baseline of security controls for a moderate impact system for confidentiality, integrity, and availability. Security controls used 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 implementing and conducting assessments of security and privacy controls employed within federal information systems and organizations. Access to IPMS from an end user or a user with elevated privileges is approved by a direct-hire supervisor and the GTM ISSO or the Functional Owner of the application and provisioned by the application administrators. Application identifiers and authenticators are provisioned based on the NIST SP 800-53 Rev 4 and State requirements. The IPMS server operating system, web servers, applications, and databases are configured according to the Diplomatic Security (DS) secure configuration standards, or according to vendor or DoD secure/hardening guides where DS guides are not available. Account privileges to all IPMS applications are based on roles with the concept of least-privilege and need-to-know. All authentication to IPMS applications and system assets requires at least 1 level of Multi-Factor Authentication (MFA).

(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).

- **System Administrators:** Responsible for creating administrative and service accounts, 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. System administrators have access to PII stored on file shares for data transfers, which may include all PII elements included within IPMS child systems.
- **Database Administrators:** The Database Administrators (DBAs) are responsible for the administration and maintenance for both the Oracle and Microsoft SQL Server database applications. DBAs are also responsible for the integrity of the data. Additional responsibilities include the use of DBA views (important Oracle metadata with details about tables, indexes, physical storage, etc.), edits, and deletes. Database administrators have access to PII stored in database tables, which may include all PII elements collected and stored by the IPMS child systems.
- **SECREF Administrators:** The HROnline SECREF System Administrator role is responsible for managing all user accounts that have access to applications under the HROnline umbrella. The HROnline SECREF Administrator roles below generally do not provide direct access to PII but can be used to grant access permissions to any other user or the administrator themselves.
- **HROnline Privileged Roles:** There are numerous elevated roles in HROnline with access to other user's data. Access to PII is limited based on the role. The following are some of the roles used to administer the HROnline application: personnel technician, bureau, career development officer (CDO).
- **Production Support Engineers:** Senior software engineers and senior business analysts responsible for providing subject matter expertise (SME) to troubleshoot and resolve critical production stoppage issues and/or develop time-sensitive ad-hoc data reports requested by upper management. Production Support Engineers have access to other user's PII which may include all PII stored within the IPMS Pillars.
- **Help Desk Agents:** Responsible for supporting IPMS users which requires them to have access to limited PII including name, email address, DOB, clearance level, and position. Helpdesk agents have the following functional responsibilities:

  - Verify access requests and assign user roles and rights to include unlocking HROnline accounts.
  - Account Request Management - Review all request forms, create tickets for all accounts/installs, scan and control all customer documents required for account creation, update permissions
- **Human Resources (HR) Specialists:** Responsible for providing a variety of human resource management services including consultation and advice to State managers. HR Specialists have access to extensive PII elements which may include name, DOB, SSN, beneficiary information, date of death, and financial information depending on the service request.
- **Human Resources System Access Request (HR SAR) Functional Owners/Approvers:** Responsible for reviewing and approving/denying access requests to IPMS subsystems. These users do not have access to PII by virtue of being a Functional Owner/Approver, but they can grant access requests for all subsystems/applications that they are approvers for.
- **Users:** Roles and responsibilities vary for each IPMS child system:
  - GEMS - Except for system administrators and human resource specialists, all users authorized to access GEMS do so to utilize State's corporate human resources self-service application that includes employee and manager self-service, benefits management, competency management, and performance management functionality.
  - OPS - Department of State U.S. Direct Hires (e.g., members of the Foreign Service and Civil Service), Department of State Locally Employed Staff members, USAID U.S. Direct Hires, and USAID Locally Employed Staff members are eligible to request access to OPS. In addition, users must be employed in a role and/or at a post that requires access to OPS and must be approved by a direct-hire supervisor.
  - HROnline - Users have the ability for the user to view, edit and delete their own PII information. The Grievance User provides access to other users PII including name, email address, and grievance case information.
  - KC - Serves as a reporting and data warehouse tool allowing users are to create, retrieve, modify, and distribute reports and documents which may contain all PII to other KC and non-KC users to meet business requirements.
  - EAPS - Users from Washington DC-based Executive Branch agencies (EAs) and other agencies with an overseas post presence access EAPS, 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.

(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.

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. For access to GEMS, OPS, and

KC, each prospective authorized user must also sign a user access agreement, take specified training modules, have their clearance status be confirmed by DS, and receive supervisor and application security team approval before being granted 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). Use access is restricted depending on their role and need-to-know.

For HROnline and EAPS, users request access via the HR SAR and complete the access request form specific to the application. The HR Helpdesk team reviews the request form and completes any other necessary checks such as clearance verification. The application Functional Owner/Approver must then approve the completed request prior to access being granted.

GEMS, OPS, and HROnline provides “self-service” functionality (meaning that users only have access to their own PII). For self-service functions the user’s OpenNet access is considered enough to implicitly grant access to the application.

In emergencies, users may request access to specific HROnline applications and roles directly to the GTM ISSO. The GTM ISSO or alternate ISSO may approve and the GTM ISSO, Alt ISSO, or a member of the GTM Security, Assurance, and Compliance (SAC) Branch may grant access to specific HROnline applications/roles for a limited duration if the user’s direct hire cleared supervisor approves the request and the Functional Owner/Approver is notified.

IPMS System and Database Administrators must obtain elevated access accounts and State Personal Identity Verification (PIV) cards associated with the elevated accounts to administer IPMS networks, servers, workstations, accounts, mid-tier application technology, and databases. These account request forms must be signed by the administrator after reading and acknowledging the elevated access rules of behavior and then also signed by the administrator’s direct-hire supervisor and the GTM ISSO or alternate ISSO.

In GEMS, personnel actions that change a user’s employee status, position, or department will automatically result in the user losing all non-self-service roles in GEMS and any applications that depends on GEMS for role provisioning. HROnline applications also automatically revoke access/roles when a user’s Organizational Unit (OU) changes in Active Directory (for example when a user is reassigned from Post to Domestic Bureau).

For SECREF administrator roles, the GTM SAC Branch review the bimonthly reassignments reports to ensure that SECRF administrator roles are de-provisioned when users reassign. For all other applications, supervisors and application Functional Owners/Approvers are responsible for periodic checks to ensure that users who no longer have a need to know have their access/roles de-provisioned.

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

- **System Administrators**: System administrators are responsible for granting and removing access to the system of all relevant Users. System administrators must request access via an approval form, which must be signed by the supervisor and GTM ISSO. As such, system administrators will maintain full administrative access to the system until their duties change.
- **Database Administrators**: DBAs require full access to the backend of the system in order to deal with any technical difficulties that may arise. Database administrators must request access via an approval form, which must be signed by a direct-hire supervisor and GTM ISSO. Once database administrators rotate out of GTM/EX/OTS their access to the system will be terminated.
- **SECREF Administrators**: The HROnline SECREF Administrators grant access permissions to any other user or the administrators themselves. They are also responsible for managing all user accounts that have access to applications under the HROnline umbrella. Because of this they have full access to the system. SECREF Administrators must request access via email or via an internal ticketing system; access requests must be approved by a direct-hire supervisor and the GTM ISSO. Once a SECREF System Administrator rotates out of the GTM ISSO team or the GTM/EX/OTS Branch Chief team, their access will be revoked.
- **HROnline Privileged Roles**: There are numerous elevated roles in HROnline with access to other user’s data which gives them limited access to data within the system. Privileged roles are requested via the internal GTM System Access Request or via an internal ticketing system and must be approved by a direct-hire supervisor and functional owner or GTM ISSO. Once a direct-hire's position changes, and once a contractor changes Post/Bureau, their access is revoked.
- **Production Support Engineers**: Production Support Engineers troubleshoot and resolve critical production stoppage issues and/or develop time-sensitive ad-hoc data reports requested by upper management which gives them limited access to limited data within the system. Production Support Engineers must request access via an internal ticketing system; access requests must be approved by a direct-hire supervisor and the GTM ISSO. Access is reviewed annually and once a direct-hire's position changes or once a contractor's Post/Bureau changes, their access is revoked.
- **Help Desk Agents**: Help Desk Agents are responsible for supporting users of IPMS subsystems and work flowing system access requests which gives them limited access to limited data within the system. Help Desk Agents must request access via email or via an internal ticketing system; access requests must be approved by a direct-hire supervisor and the GTM ISSO. Once a direct-hire's position changes, and once a contractor changes Post/Bureau, their access is revoked.
- **Human Resources (HR) Specialists**: Human Resources (HR) Specialists provide a variety of human resource management services including consultation and advice to State managers. They have limited access to limited data within the system. Access is requested via an access request form and is granted based on the user’s position code in GEMS, and supervisor and security team approvals. Once a direct-hire's position changes, and once a contractor changes Post/Bureau, their access is revoked.

- **Human Resources System Access Request (HR SAR) Functional Owners/Approvers:** Review and approve/deny access requests to IPMS subsystems. Department of State users are assigned as Functional Owners/Approvers in the HR SAR for each IPMS subsystem and have limited access to IPMS subsystems. Access is requested via email or via an internal ticketing system; access requests must be approved by a direct-hire supervisor and the GTM ISSO. Once a direct-hire's position changes, and once a contractor changes Post/Bureau, their access is revoked.
- **Users**: User's access varies for each IPMS child system:
  - GEMS - All users authorized to access GEMS do so to utilize State's human resources management information systems which gives them limited access to their data within the system. All direct hires maintain user level access to GEMS until they depart State.
  - OPS – Since OPS users have access to PII of all users under Chief of Mission (COM) Authority they maintain full access within OPS to all their data. Once a direct-hire's position changes, and once a contractor changes Post/Bureau, their access is revoked. For other Government Agency (OGA) users, each Agency is responsible for performing an annual review and notifying GTM to remove departed users' accounts.
  - HROnline – HROnline provides the ability for the user to access self-service applications to view, edit and delete their own PII. Since they can only manipulate their own information, they only have access to their information within the system. Once a direct-hire's position changes, and once a contractor changes Post/Bureau, their access is revoked. Access is automatically granted based on the user's employment status code in GEMS and their location in Active Directory.
  - KC - Users of the Knowledge Center (KC) perform reporting and data analysis and as such have access to extensive data including PII, financial data, and diversity data. They have limited access to limited data within the system. Once a direct-hire's position changes, and once a contractor changes Post/Bureau, their access is revoked. Access is granted based on a user's position code in GEMS, or via a request form which must be approved by a direct-hire supervisor and the security team.
  - EAPS - Users access EAPS 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 as such they have limited access to limited data within the system. Once a direct-hire's position changes, and once a contractor changes Post/Bureau, their access is revoked. For other Government Agency (OGA) users, each Agency is responsible for performing an annual review and notifying GTM to remove departed users' accounts. Access is granted based on position and location codes in GEMS and Active Directory.

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

Access is restricted by system and roles within each child system. Audit logs are maintained to record system and user activity including invalid logon attempts and access. The GTM Information System Security Officer (ISSO) team conducts monthly audits of IPMS to monitor the audit logs for unusual activity. System managers and user personnel work cooperatively to implement access controls. Access is reviewed regularly to ensure that all users still have a need to know for the roles/applications they are granted.

(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; however, State users who regularly access PII other than their own are required to take biennial PII course, PA318, and an annual cyber security course, PS800. Access to State’s intranet is disabled if users do not take and pass PS800 course annually. In addition, the GTM ISSO team provides all elevated users with access to the GTM development and test environments with a standard operating procedure (SOP) and/or Rules of Behavior (ROB) form for the minimization of PII in non-production environments.