

# Integrated Personnel Management System

## 1. Contact Information

**A/GIS/IPS Director**

Bureau of Administration

Global Information Services

Office of Information Programs and Services

## 2. System Information

- (a) Name of system: Integrated Personnel Management System
- (b) Bureau: 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): The Current PIA for Integrated Personnel Management System was signed in October of 2015. However IPMS has made a significant change to the way it shares information with the Transportation Security Administration.

## 3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
  - Yes
- (b) What is the security Assessment and Authorization (A&A) status of the system?

IRM issued the HR IPMS ATO on October 2015 for 18 months; it expires April 30, 2017.
- (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), HR Knowledge

Center (KC), the Web Post Personnel System (WebPS)<sup>1</sup>, the Human Resources Online (HROnline) system and the Executive Agency Personnel Support (EAPS) system. 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 through online seamless workflow processes.

(d) (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 Information

The principle sources of information include all Department of State CS and FS direct hire employees, employee dependents, FS Consular Agents, applicants for CS and FS

---

<sup>1</sup> Web Post Personnel System falls under the Web Post Administrative Software Suite (WebPASS) system boundary that is administered by the PASS Program Management Office, which is part of the Bureau of Information Resource Management (IRM). Subsequently, the Web Post Personnel System PIA is the responsibility of IRM.

employment, students, U.S. Citizen direct hires, dependents, and resident U.S. citizens employed by U.S. missions abroad. GEMS is the source for most U.S. Citizen direct hire employee data used by applications under the IPMS. GEMS data includes initial employee information via resume, or other equivalent employment forms (e.g. OF-612, locator info, Check-In forms, assignment cables, etc.). Department-sponsored training data, including language training, is provided by the Foreign Service Institute's (FSI) Student Training Management System (STMS).

Payroll-related information is provided by the Bureau of Comptroller and Global Financial Services (CGFS), Consolidated American Payroll and Pension System (CAPPS) and Foreign Service National Payroll System (FSNPay). Medical data is provided by the Office of Medical Services (MED), Electronic Medical Records System (eMED) and security clearance information is provided by Diplomatic Security (DS).

Other sources of PII include the Department of Labor (DOL) which collects workman's compensation data; Gateway to State (GTS) which collects job applicant data; and the Foreign Service Officer Test (FSOT) application which collects prospective candidate information via online registration for the Foreign Service exam.

(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 11th 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, State-05

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN: May 2, 2008
- 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): May 9th 2013

- (g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?  Yes  No
- (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 yes provide:

- Schedule numbers: A-04-003-01a through A-04-003-20
- Length of time the information is retained in the system: When records have reached their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration
- Type of information retained in the system: FSOT data through entire lifecycle, employee personnel records, post assignments, and dependent records.  
url:<http://infoaccess.state.gov/recordsmgmt/recdispsched.asp?cat=records#search>. The Department also follows the National Archives and Records Administration (NARA) General Records Schedule 1 (GRS-1) for Civilian personnel records supplemented as necessary to meet the specialized records management needs of the Department

#### 4. Characterization of the Information

- (a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

- (b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

Yes  No

- If yes, under what authorization?

- 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 will receive data extracts on a weekly, monthly, or quarterly basis. DOL OCIO will provide 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 OWCP's (iFECS), which is hosted on the ECN/DCN and maintained by 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 new 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).

#### Department of Homeland Security (Known Travel Number)

- The Transportation Security Administration maintains the TSA's Secure Flight program. This program conducts watch list matching of airline passenger data to the federal government watch lists for International and Domestic flights. TSA Secure Flight also conducts matching of airline passenger data to specific eligible low-risk population lists. PII data that is produced from GEMS is extracted and, upon verification, is exchange between Department of State (HR/EX/SDD) and DHS/TSA via a secure encrypted file Data transfer.

#### 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. Applicant PII data is submitted to DOS via an encrypted connection to HR's dedicated server in the HRNet system hosted in the State Department's DMZ. When received by HR, the PII is manually uploaded into IPMS.

(d) Where is the information housed?

Department-owned equipment

FEDRAMP-certified cloud

Other Federal agency equipment or cloud

Other - Data collected through FSOT and GTS are stored at their respective contractor owned and operated hosting sites. These data are transferred to IPMS.

(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

(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 contact the HR Help Desk to submit for changes to the PII in their records from the Help Desk or other application maintainer 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. IPMS does use information from service providers (e.g. PearsonVUE, and Monster Government Solutions) and from the U.S. Department of Labor. For employees transferring to the Department from another agency, the individual's Official Personnel Folder (OPF) or Merged Records Personnel Folder (MRPF) is provided by the losing agency. These personnel records contain information related to the hiring process. Pending the official transfer of the employee's OPF the losing Federal agency provides

the SF-75 form containing the employee's information necessary to complete the hiring and transfer process. PII from the DOL is used for reporting, and trending purposes, as well as to help manage the performance of the Department of State's worker safety and health program

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

For Department of State employees, a secure single sign-on solution is used to access IPMS. The purpose, use and authority for collection of information submitted are provided in STATE-31.

A notice of record is provided by the Web.PS system; illustrated within the Web.PS Privacy Impact Assessment.

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?

Individuals that are not Department of State employees do not provide information to IPMS. 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

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

Privacy concerns were considered. IPMS collects the absolute minimum amount of PII required to satisfy the statutory purposes of this system 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 and documents collected and maintained in IPMS are in keeping with the Bureau of Human Resources' mission. Uses of IPMS include determining the size and configuration of the Department of State's workforce to meet its goals of defending national security and promoting national interests; documenting all processes associated with individual employment histories and career progression; ensuring that all employees and potential employees have equal opportunities; and to make personnel management determinations about employees throughout their Federal careers. For EAPS specifically, the information and documents collected and maintained are used to support HR's mission of managing the Department's authoritative source for overseas position data. 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 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 also 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 are varied. 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?

New information that may be produced includes reports pertaining to workforce planning, hiring summary data, individual employee information, 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. The newly created information is accessible to government employees who make determinations about the individual during and after an evacuation management emergency

- (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
- Office of Medical Services
- Bureau of the Comptroller and Global Financial Services
- Bureau of Diplomatic Security
- A Bureau
- 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.

- (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.
- Bureau of the Comptroller and Global Financial Services: 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.

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

The intended purposes for sharing are used 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

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

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. Data sharing is fully explained in the IPMS System Security Plan (SSP), Section 2.9.4, System Data Sharing. 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.

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.

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

All IPMS internal data sharing transmits information via OpenNet. Security controls for sharing internally 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.

**(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?

Human Resources Records, along with the other SORNs provides guidance for record amendment procedures. System of Record Notice, STATE-31, STATE-24, STATE-30, and STATE-36 provides 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).

(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.

For EAPS, the only application by which individuals may update personal record information to EAPS is Phone Book. 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.

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

STATE-31, Human Resource Records, along with the other SORNs provides 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).

## 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’s user policy and rules of behavior are the general terms under which federal employees and contractors use the system. The Department requires all new employees and contractors to attend Cyber Security Awareness training, and the completion of the Department’s Protecting Personally Identifiable Information course (PII-PA-459) before or immediately after the employment start date and prior to being granted access to the system. In addition, the OpenNet account request form signed by all employees and contractors includes a “Computer Security Awareness Form” that provides privacy orientation. To retain access, all Department personnel must complete annual refresher training. Access to data is limited to cleared U.S. Government employees/contractors administering the system who meet “official” need-to-know criteria.

- (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 adherence to and implementation of 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 baseline requirements for a system with moderate impact rating for confidentiality, integrity, and availability. 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 were included in the design and operation of IPMS. In particular, the PII data influenced the application of the controls from the following families: access control, audit and accountability, identification and authentication, system and communications protection, and system and information integrity control families.

## 9. Data Access

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

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.

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

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 IPMS application 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?

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.