PRIVACY IMPACT ASSESSMENT

Integrated Logistics Management System (ILMS) PIA

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: April 2022
(b) Name of system: Integrated Logistics Management System
(c) System acronym: ILMS
(d) Bureau: Bureau of Administration (A)
(e) iMatrix Asset ID Number: 830 (ILMS)
(f) Child systems (if applicable) iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable):

3. General Information

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

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

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

(c) Describe the purpose of the system:

The Integrated Logistics Management System (ILMS) is maintained by the Office of Logistics Management's Office of Program Management and Policy (A/LM/PMP) in the administration of its mission to provide worldwide logistics services and integrated support. The information collected and maintained in this system is necessary to ensure fiscal accountability in transporting the effects of Department of State (Department) bureau and embassy employees, and provides end to end supply chain management to Department users including:

- ***Procurement:*** ILMS is used by embassy and bureau personnel to support procurements. The purpose of the procurement module is to allow procurement agents and approvers to request items, contracts, and other services. In addition, the ILMS procurement module tracks receipt, invoice approval for payment, and documentation for procurement awards. ILMS also includes invoice approval for payment functionality for non-procurement invoices, such as leases and employee reimbursements.
- ***Federal Assistance:*** A Bureau system myGrants works alongside Integrated Logistics Management System (ILMS) to automate and centralize the federal assistance process at the Department. Specifically, ILMS integrates with myGrants for award file storage and award issuance. The purpose is to support the Department's mission to provide a centralized and integrated solution for Federal Assistance issued by overseas posts and domestic bureaus. The Federal Assistance module supports the end-to-end federal assistance planning, pre-award, award, post-award, and closeout processes for the Department. The system is used by the Department to issue and monitor federal assistance to the recipients of the award.
- ***Warehouse Management:*** The Warehouse Management module provides end-to-end visibility of all warehouse inventory, processes, and reporting, for all accountable, non-accountable, and expendable items before shipment to post.
- ***Diplomatic Pouch and Mail:*** The Diplomatic Pouch and Mail (DPM) module provides domestic mail, Diplomatic Post Office (DPO) mail, and unclassified and classified pouch service to the Department and other government and foreign agencies.
- ***Expendables:*** The ILMS Medical Expendables (MEDx) module is used by domestic Travel Clinic and overseas Health Unit personnel to dispense, replenish, and receive pharmaceuticals and medical supplies. The module also allows domestic travel clinic and overseas Health Unit users to track item consumption and recipients, including controlled substances, adjust and track inventory levels, and manage item storage locations within the Health Unit. Vaccination records of Department of State personnel and eligible family members are managed within the module.
- ***Transportation Management:*** The Transportation Management module's main purpose is to manage and track the movement of shipments from their origination to their final destination. This includes recording receipt, booking, and status information for supplies and personal effects shipments that are processes through the Department's supply chain. It also tracks billing information for transportation services, which integrates with the Department's financial systems for payment processing.
- ***Fleet Management:*** The role of the Fleet Management module is to track the asset record of the vehicle and have a system of record containing all information about the armored and non-armored motor vehicles operating in the embassies around the world. It is designed to allow insight into the daily usage, maintenance, fueling and upkeep of all Department-owned vehicles.

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

PII is collected from the following groups of individuals (specific information on each user role can be found in 8b):

- **Department end-users and non-Department end-users**: Department end-users are Department employees, eligible family members, and locally employed staff. Non-Department end-users are contractors, customers/travelers, vendors, recipients of federal financial assistance, and government agency employees. The Department end-users and non-Department end-users will also consist of privileged users, such as approvers, fulfillers, and personnel that can collect PII (domestic travel clinic and overseas Health units, General Services Officer (GSO) staff at Post, Travel and Transportation Management staff in DC, mailroom staff). These users just have privileged access as explained in section 8b.
- **Support users**: Support desk personnel that approve requests submitted by end-users. While they have the ability to access certain PII as explained in section 8b, only information required for authentication purposes (i.e. – name and business email address) may be collected.

- ***Procurement Module:***
  - **First and Last Name, Business/Home/Remittance Address, Phone Number, Email Address, Individual/Vendor's Fax Number:** Collected from Department and non-Department end-users. These PII elements are maintained for purposes of identification, communication, pickup, delivery, drop-off, and payment functions.
  - **Purchase Card Information, including cardholder's first and last name, account number, business email address, office address, business phone, and business fax number.:** ILMS captures Department and non-Department end-users' purchase card information to apply or update existing purchase cards within the external bank system, facilitate procurement of goods and services using purchase cards, and to support approvals for payment for purchase card transactions.
  - **Vendor/Employer/Applicant Tax ID:** ILMS captures **Tax ID (TIN) from non-Department end users** for purposes of identification for procurement awards. Vendor information is collected from non-Department end users (foreign national companies/entities/small businesses), some of which have a TIN. ILMS also maintains vendor information from domestic non-Department end users via Sam.gov, a system used by vendors to register to do business with the U.S. government.
  - **Vendor Banking Information, including bank name, address, routing number, and/or account number:** Department end-users may upload invoices or supporting procurement documentation that includes vendor banking information for the purpose of making procurement awards. Vendor banking information is collected from non-Department end users about vendor banks and may include
  - **Medical Information:** Department end-users may upload invoices or supporting documentation associated with their hospitalization, physical exams, or other medical expenses for employee reimbursement. This information is required to support approvals for payment to relevant parties. The information stays internal to the Department and is not sent from ILMS to vendors.

  - **Education Information, including name and educational services provided:** Department end-users may upload invoices or supporting documentation associated with their education expenses, including special needs education expenses. This information is required to support approvals for payment to relevant parties. None of this information is passed from ILMS to the vendors.
  - **Signatures:** Signatures are captured from Department and non- Department end-users to acknowledge completion of tasks or receipt of shipment.
- ***Federal Assistance:***
  - **Vendor/Employer/Applicant Tax ID, First and Last Name, Email Address, Business Address, Phone Number:** ILMS captures the above information for purposes of identification for Federal Assistance Awards from non-Department end-users and Department end-users.
- ***Warehouse Management:***
  - **First and Last Name and Email Address:** Collected from Department end-users who are issued/loaned inventory items for the purpose of inventory tracking.
- ***Diplomatic Pouch & Mail:***
  - **First and Last Name, Business/Home/Remittance Address:** Collected from Department and non-Department end-users. Home address is only collected from Department end-users. These PII elements are maintained for purposes of identification, communication, pickup, delivery, drop-off, and payment functions.
  - **Signature of Mail Recipients:** Collected from non-Department end-users. These customers at post sign for their packages on an electronic signature pad to confirm that the addressee received their mail. The signature completes the chain of custody for each piece of mail and is saved as an image in ILMS.
- ***Expendables:*** This information is necessary to process pharmaceuticals and medical supplies consumption and track recipients.
  - **First and Last Name:** This application collects names of Department end-users, names of pharmaceutical and supply recipients, and names of prescribers.
  - **Date of Birth:** This application collects date of birth of Department end-users.
  - **Last 5 Digits of SSN:** ILMS does not directly collect SSN from end-users. For Department end-users, the SSN is obtained via the integration between the Bureau of Global Talent Management (GTM) Global Employment Management system (GEMS) and ILMS.
- ***Transportation Management:*** This information is necessary to process personal effects shipments when employees move from post to post.
  - **First and Last Name, Addresses, Email Address, Phone Numbers:** Collected from Department and non-Department end-users at post upon packout travel request from that post.
  - **Last 5 digits of SSN:** ILMS does not directly collect SSN from end-users. For Department end-users, the SSN is obtained via integration between GEMS and ILMS. For non-Department end-users, SSN is entered manually by logistics staff dealing with personal effects shipments.
- ***Fleet Management:*** This information is necessary to track all armored and non-armored motor vehicles operating in the embassies around the world.

- **First and Last Name, Email Address, and Phone Number:** To account for driver-car assignments from Department end-users (embassy employees) and non-Department end-users (customers).
- **Vehicle Registration, License Plate Number, VIN Numbers, Driver's License Number:** The information is pertaining to all vehicles at Post, most of which are Department-owned, but can also be other government agencies or personally owned vehicles. Driver license number is collected from all drivers driving the Department-owned motor vehicle to ensure any employee that may operate a vehicle is licensed to do so.

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

- 22 U.S.C. 4081, Travel and Related Expenses
- 22 U.S.C. 5724a, Relocation Expenses of Employees Transferred or Reemployed
- 5 U.S.C. 301, 302, Management of the Department of State
- 22 U.S.C. 2651a, Organization of the Department of State
- 22 U.S.C. 2677, Availability of Funds for the Department of State
- 22 U.S.C. 3921, Management of the Foreign Service
- 22 U.S.C. 3927, Responsibility of Chief of Mission
- 31 U.S.C. 901—903 (Agency Chief Financial Officers)
- Federal Financial Management Improvement Act of 1996
- 22 U.S.C. 5724, Travel and Transportation Expenses of Employees Transferred
- Executive Order 9830 (as amended) (Amending the Civil Service Rules and Providing for Federal Personnel Administration)
- Executive Order 12107 (as amended) (Relating to the Civil Service Commission and Labor-Management in the Federal Service)

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

☒Yes, provide:

- SORN Name and Number: State-70, Integrated Logistics Management System
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): January 25, 2022

☐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):

- Disposition Authority Number:
  Procurement: DAA-GRS-2013-0003-0001 (GRS1.1, item 010)
  Federal Assistance: DAA-GRS-2013-0008-0007 (GRS1.2, item 010)
  Contracts Management: DAA-GRS-2013-0003-0001 (GRS 1.1, item 010)
  Warehouse Management: DAA-GRS-2016-0011-0001 (GRS 5.4, item 010)
  Diplomatic Pouch and Mail: DAA-GRS-2016-0012-0002 (GRS 5.5, item 020)
  Expendables: DAA-GRS-2016-0011-0001 (GRS 5.4, item 010)
  Transportation Management: DAA-GRS-2016-0011-0001 (GRS 5.4, item 010)
  Fleet Management: DAA-GRS-2016-0011-0001 (GRS 5.4, item 010)

- Length of time the information is retained in the system: DAA-GRS-2013-0003-001 (GRS 1.1 item 010) – delete after 6 years; DAA-GRS-2013-0008-0007 (GRS 1.2, item 010) – delete after 3 years; DAA-GRS-2016-0011-001 (GRS 5.4, item 010) – delete after 3 years; GRS-2016-0012-0002 (GRS 5.5, item 020) – Temporary, delete after 1 year

- Type of information retained in the system:
  Procurement, Shipping, Inventory, Transportation, Medical records supporting worldwide logistics and supply chain functions for the Department.

4. Characterization of the Information

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

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

(b) On what other entities above is PII maintained in the system?

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

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

The system does not collect full SSNs directly from individuals, last 5 digits of the SSN are imported into the system from the integration between ILMS and HR GEMS.

- If yes, under what authorization?

- 31 U.S.C. 7701, Taxpayer Identifying Number
- 26 U.S.C. 6109, Identifying Numbers
- 22 U.S.C. 4081, Travel and Related Expenses
- 22 U.S.C. 5724a, Relocation Expenses of Employees Transferred or Reemployed
- 5 U.S.C. 301, 302, Management of the Department of State

(d) How is the PII collected?

The PII required for access to Procurement, Federal Assistance, Diplomatic Pouch and Mail, and Fleet Management modules is collected from the individual through the online ILMS Access Request Form (ARF). The access request process is the same for Department employees, contractors, and non-employees. The form will vary depending on the role selected and will determine what PII is required. Once the ARF is reviewed and approved by the supervisor, the end-user's profile is created within PeopleSoft, ServiceNow, and Ariba (applications within ILMS) by the support users. The ARF collects PII specifically for the profile page within each of the four modules listed above.

- ***Procurement:***
  - Vendor information is input into supplier entry (SE) forms by procurement agents and each SE form has a unique SE number associated to it (i.e., SE-xxxxxx). First and last name, phone number, and email address is input as part of the ILMS Support user creation process as mentioned above. Vendor information is collected on domestic non-Department end users via a feed from the Federal government's procurement system, Sam.gov.
  - Social Security Number, vendor banking information, medical information, and education information may be included on documents or images uploaded to the system by Department and non-Department end-users.
  - Purchase card information is obtained via integration with the Department's external bank system, Citibank. An automatic, daily batch job runs in ILMS to load new purchase card data into the system from Citibank.
  - Signatures are collected for use in producing a printed signature on electronic documents that require a valid signature for Department end-users and non-Department end-users, typically through a Word form that allows users to "draw" their signature as part of the end-user profile creation mentioned above and managed by the support users.
- ***Federal Assistance:***
  - First and last name, email, phone number, and vendor/employer/applicant tax ID are entered into the ILMS Access Request Form for creation of the profile within PeopleSoft, ServiceNow, and Ariba for Department end-users. For non-Department users, the information is entered directly into the myGrants Federal Assistance module for ServiceNow since they do not have access to OpenNet systems, PeopleSoft, or Ariba.

  - Social Security Number, signatures, date of birth, vendor/employer/applicant tax ID, and vendor banking information may be included on documents or images uploaded to the system by Department and non-Department end-users.
- ***Warehouse Management:***
  - First and last name and email address are collected via the State Department standard DS-584 form: Property Transaction that is generated and completed by the individual requestor and entered into the module by Warehouse logistics staff upon initial issuance/loan to the individual requester.
- ***Diplomatic Pouch and Mail:***
  - First and last name, business/home/remittance address, phone number, email address, and fax number are collected via manual input in data entry fields either by privileged users or directly by the end-user.
  - Signature of mail recipients is collected via an electronic signature pad. The signature immediately displays in the system and the page is saved. Once the signature is saved, it is associated with the item(s) and can be looked up at any time.
- ***Expendables:***
  - First and last name and date of birth are entered by Medical Expendables privileged users into the desktop module.
  - Last 5 of SSN is integrated from GEMS for Department end-users through nightly batch transfers.
- ***Transportation Management:***
  - First and last name, last 5 digits of SSN, address, email address, and phone number are integrated from GEMS for Department end-users through nightly batch transfers. For non-Department end-users, PII is entered manually by A/LM/OPS/TM staff.
- ***Fleet Management:***
  - First and last name, vehicle registration, license plate number, VIN number, Driver's License Number, email address, and telephone number are manually input in data entry fields by privileged users or end-users during account creation.

(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?

- ***Procurement:*** Accuracy of the information is the responsibility of the individual end-user who provides their own information. The information can be updated if the individual identifies the information to be inaccurate. Transmission of encrypted export files between ILMS and Citibank occur daily and ensure purchase card information is accurate. This file is placed in Citibank's sFTP server and ILMS is updated after decrypting and retrieving the file. Additionally, a separate file is retrieved from Citibank's sFTP server for users to complete their reconciliation process in ILMS and confirm the information accuracy.

- ***Federal Assistance:*** Accuracy of the information is the responsibility of the end-user who provides their own information. In addition, ILMS Federal Assistance system administrators perform annual user reconciliation and account reviews to ensure accuracy of PII in the system.
- ***Warehouse Management:*** Accuracy of the information entered on the DS-584 form is the responsibility of the end-user.
- ***Diplomatic Pouch and Mail:*** Accuracy of the information is the responsibility of the individual end-user who provides their own information. The information can be updated if the individual identifies the information to be inaccurate.
- ***Expendables:*** Recipients are asked by privileged users (Health Unit personnel) to confirm the information in their recipient profile (first and last name, date of birth and last 5 digits of their SSN) upon the dispense of a pharmaceutical, including vaccines and controlled substances. If the information is inaccurate, or unavailable, Health Unit personnel can update the information (first and last name and/or date of birth) or create a new recipient profile. In the case that the last 5 digits of SSN is incorrect, GEMS (HR) is the source system from which ILMS obtains information and the accuracy of the information is the responsibility of GEMS.
- ***Transportation Management:*** GEMS (HR) is the source system from which ILMS obtains information, the accuracy of the information is the responsibility of GEMS. The PII required of non-Department end-users is collected directly from the individual and they are responsible for accuracy. On rare occasions, the PII of non-Department end users is validated by A/LM/OPS/TM staff by referencing the travel orders/travel authorization documentation provided by the individual or the individual’s sponsoring agency.
- ***Fleet Management:*** End-users are responsible for entering accurate information into the system, however, privileged users (motor pool supervisors and/or GSOs) confirm accuracy of the information entered by users at their respective post. Cross-referencing information entered with a valid driver’s license is done to verify data.

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

- ***Procurement:***
  - End-users are prompted to review their profile and confirm accuracy annually. If changes need to be made, the user must submit an ILMS Support Desk ticket specifying the information that needs to be updated. It is the individual’s responsibility to submit a data correction.
  - Purchase Card information remains current through daily integrations with Citibank.
- ***Federal Assistance:*** The PII is current and remains current as it is validated by ILMS Federal Assistance system administrators who perform annual user reconciliation and account reviews to ensure accuracy of PII in the system.

- ***Warehouse Management:*** The information is current as of the most recent issue/loan. If the requester departs from their position, they are expected to return all loaned equipment. Warehouse logistics staff will either suspend or remove them from the Requester list. Name changes are also made, when necessary, upon issuance/loan.
- ***Diplomatic Pouch and Mail:*** End-users are prompted to review their profile and confirm accuracy annually. If changes need to be made the user must submit an ILMS Support Desk ticket specifying the information that needs to be updated. It is the individual's responsibility to submit a data correction.
- ***Expendables:*** End-users are prompted to review their profile and confirm accuracy and currency annually. If changes need to be made, the user must submit an ILMS Support Desk ticket specifying the information that needs to be updated. Prescriber names are entered upon the dispense of all pharmaceuticals. End-users or privileged users may update the prescriber profile or create a new prescriber profile in the module.
  End-users are asked by privileged users (Health Unit personnel) to confirm the information in their recipient profile (their name and date of birth) and last 5 digits of their SSN) upon the dispense of a pharmaceutical, including vaccines and controlled substances. If the information is inaccurate, or unavailable, Health Unit personnel can update the information (first and last name and date of birth) or create a new recipient profile. The last 5 digits of SSN is current and remains current for Department end-users via nightly batch transfers from GEMS, which reflects updates to PII as they occur.
- ***Transportation Management:*** The PII is current and remains current for Department end-users via nightly batch transfers from GEMS, which reflects updates to PII as they occur. Information for non-Department end-users is reviewed each time new shipments are created for travelers of other agencies and updated as needed. End-users are prompted to review their profile and confirm accuracy and currency. If changes need to be made the end-user must submit an ILMS Support Desk ticket specifying the information that needs to be updated. It is the individual's responsibility to submit a data correction.
- ***Fleet Management:*** End-users are prompted to review their profile and confirm accuracy and currency. If changes need to be made the user must submit an ILMS Support Desk ticket specifying the information that needs to be updated. It is the individual's responsibility to submit a data correction.

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

No, ILMS does not use information from commercial sources nor is the information publicly available.

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

Privacy concerns are at the forefront of the system design and enhancements. ILMS only collects the minimum amount of PII necessary to support the purpose of the system as described in section 3(c).

5. Use of information

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

Information on the intended uses of the PII within each ILMS module is included below.

- ***Procurement:*** The PII is used to maintain procurement records and support the processing and management of procurement requests and payment approvals.
- ***Federal Assistance:*** The PII is used to support issuance of federal assistance awards.
- ***Warehouse Management:*** The PII is used for tracking issued/loan inventory items.
- ***Diplomatic Pouch & Mail:*** The system uses PII for purposes of identification, communication, pickup, delivery, drop-off, and payment functions.
- ***Expendables:*** The PII is used to dispense, replenish, and receive pharmaceuticals and medical supplies including vaccines.
- ***Transportation Management:*** The PII is used to identify employees' shipments to ensure they get to the right place and to communicate with employees about their shipments.
- ***Fleet Management:*** The PII in Fleet Management is used to track changes and the financial information is used to capture details about the vehicle that was purchased.

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

Yes, the PII is relevant to the purpose of ensuring fiscal accountability in transporting the effects of Department and other embassy employees and providing end to end supply chain management to Department users. No collateral uses exist for the information collected by the system.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No
If yes:

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

(2) Does the analysis result in new information?

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

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

(d) If the system will use test data, will it include real PII? ☐Yes ☐No ☒N/A
If yes, please provide additional details.

6. Sharing of PII

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

- ***Procurement:***
  Internal: The PII is shared internally with the Department's financial management systems for accounting. The Department's financial management systems owned by the Bureau of the Comptroller and Global Financial Services (CGFS) are as follows: Momentum, Regional Financial Management Systems (RFMS), and Global Financial Management systems (GFMS). These systems will be referenced collectively as "the Department's financial management systems" throughout the remainder of the document.

  External: Purchase card information is shared with the external banking system, Citibank, to establish and update end-user purchase card accounts. PII is also shared with Ariba Supplier Network (ASN) to provide a point of contact for the procurement order and provide a payment method to a vendor.

- ***Federal Assistance:***
  Internal: Vendor information is shared internally with the Department's financial management systems for accounting. Federal assistance recipient information is shared internally with the program and grants offices issuing the federal assistance.

  External: N/A

- ***Warehouse Management, Diplomatic Pouch and Mail Management, Expendables, Transportation Management, Fleet Management:***
  Internal: N/A

  External: N/A

(b) What information will be shared?

- ***Procurement:***
  Internal: Internal sharing with the Department's financial systems includes:
    - Name, Phone Number, Email Address

  External: External sharing with Citibank and ASN include:
    - Name, Phone Number, Email Address, and Purchase Card Information

- ***Federal Assistance:***
  Internal: Sharing with the Department's financial systems includes:
    - Names, Phone Number, Email Address for vendors

  Sharing with State Department Federal Assistance staff in program and grant offices includes:
    - Names, Business Address, Phone Number, Email Address, Fax Number, and Vendor/Employer/Applicant Tax ID

External: N/A

- ***Warehouse Management, Diplomatic Pouch and Mail Management, Expendables, Transportation Management, Fleet Management:***
  Internal: N/A

  External: N/A

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

- ***Procurement:***
  Internal: Information is shared with the Department's financial systems to facilitate financial commitments, obligations, and payment.

  External: Information is shared with Citibank to establish purchase card accounts and track usage. Information is shared with Ariba Supplier Network in order to provide a point of contact for the order and establish communication with a vendor. The integration with ASN helps Department of State directly submit orders to vendors, typically for office supplies requested by domestic offices.

- ***Federal Assistance:***

  Internal: Information is shared with the Department's financial systems to facilitate issuance of Federal Assistance Awards.

  External: N/A

- ***Warehouse Management, Diplomatic Pouch and Mail Management, Expendables, Transportation Management, Fleet Management:***
  Internal: N/A

  External: N/A

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

- ***Procurement:***
  Internal: Internal sharing is transmitted via encrypted connections on the Department's OpenNet network.

  External: The information is shared via encrypted integrations with Citibank and ASN. Encrypted export files of account creation and account maintenance requests are transmitted from ILMS to Citibank. The requests are processed in Citibank system (CitiManager) and a file is generated on their end with the new account information. This file is placed in Citibank's sFTP server.

ASN is hosted on Ariba’s cloud marketplace, facilitating interactions between buyers and sellers. ASN orders account for a small percentage of overall Ariba transactions. The majority of orders generated within Ariba are created into a pdf document which is then emailed or printed and provided to the vendor. There is no ‘file’ placed for these transactions.

- ***Federal Assistance:***
  Internal: Internal sharing is transmitted via encrypted connections on the Department’s OpenNet network.

  External: N/A

- ***Warehouse Management, Diplomatic Pouch and Mail Management, Expendables, Transportation Management, Fleet Management:***
  Internal: N/A

  External: N/A

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

- ***Procurement***
  Internal: The system owner and ISSO have approved the sharing arrangement via a Memorandum of Understanding (MOU). The connections with the Department’s financial management systems comply with the applicable Risk Management Framework (RMF) and Department security requirements.

  External: External sharing with Citibank is safeguarded by an Interconnection System Agreement (ISA) and a Memorandum of Understanding (MOU) which specify the sharing requirements. External sharing with ASN is safeguarded by the role-based access control implementation. The vendors from ASN have read-only access to the system to safeguard the PII. The vendors are required to authenticate to ASN with a user-id and password to be granted the read-only view.

- ***Federal Assistance:***
  Internal: Internal sharing with the Department’s financial management systems for accounting is safeguarded by FIPS 140-2 encryption. Access to information is controlled by role and location-based security within the system.

  External: N/A

- ***Warehouse Management, Diplomatic Pouch and Mail Management, Expendables, Transportation Management, Fleet Management:***
  Internal: N/A

  External: N/A

7. Redress and Notification

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

Before accessing [Procurement, Federal Assistance, Diplomatic Pouch and Mail Management, and Fleet Management], all ILMS end-users are presented with a link to the ILMS Privacy Act statement (which covers the PII collected in the end-users' profile) located on the bottom margin, prior to logging in to the system. The ILMS system owner is working to move the PAS to the ILMS profile page and to applicable forms where end-users are actually entering their PII. All information including first and last name, business/home/remittance address, phone number, email address and fax number for the Diplomatic Pouch and Mail Management modules is collected in the end-users' profile. The only exception is the signature, which is saved as an image.

Procurement (Purchase Card and Uploaded Documents), Expendables (for 5 last digits of SSN), Federal Assistance (Uploaded Documents) and Transportation modules (PII originated from GEMS through nightly batch transfers): The originally collecting system is responsible for providing notice to the individual, prior to collecting their PII, as ILMS and its applications are unable to do so.

Warehouse Management collects PII via DS-584. However, the information collected does not constitute a Privacy Act system of record so a Privacy Act statement is not needed.

Expendables: If a MEDx end-user is creating a new Recipient Profile for a recipient of a vaccine or pharmaceutical at the time of the dispense, the record subject is asked to provide the PII needed (their name and date of birth) to complete the transaction. It is the responsibility of the privileged user (health unit personnel) collecting the information from the record subject to provide notice prior to the collection of the individual's information.

(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?

End-users accessing the Procurement, Federal Assistance, Diplomatic Pouch and Mail, and Fleet Management consent to the use of their information when they submit the requisite portions of their profile through completion of the online ILMS Access Request Form (ARF). Failure to provide the required information will result in inability to access the modules to complete their duties.

Procurement (Purchase Card Information and Uploaded Document), Expendables (for last 5 digits of SSN), Federal Assistance (Uploaded Documents) and Transportation modules: It is the responsibility of the originally collecting system to obtain consent from the individual as ILMS and its applications are unable to do so.

Warehouse Management: The record subject provides consent by completing and submitting the DS-584 form.

Expendables: Department record subject gives their consent by providing the requested PII. Failure to do so will result in their inability to obtain the services they seek.

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

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

Procurement, Federal Assistance, Diplomatic Pouch and Mail, Expendables, Fleet Management, and Transportation ILMS end-users who are granted access to their individual module can access their PII.

Other non-ILMS users such as vendors are often foreign nationals and are not granted access to ILMS. They will not have access to view their information.

Additionally, U.S. record subjects have notification and redress rights under the Privacy Act, and the relevant procedures are described in 45 CFR 5b.5 rulemaking and the SORN. Individuals who want to gain access to records pertaining to them should follow the procedures laid out in the covering SORN, State-70.

Warehouse Management: Upon issue/loan the requester can see their contact information on the system generated DS-584 and must review/sign prior to completing the transaction. The requester does not have any system access to reference this form or the data after their review but can choose to retain a copy of the final DS-584 for their records. If they wanted to access this information or form at a later date, they would have to request that an end-user or privileged user provide it. This information remains available to the requester and privileged users indefinitely via the system data (i.e., the “loan” record) stored in ILMS and the DS-584 document that is generated and stored on the loan record.

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

☒Yes ☐No

If yes, explain the procedures.

- ***Procurement:*** End-users correct their PII by submitting a ticket to the ILMS support desk to correct PII. Other non-ILMS users such as vendors are often foreign nationals and do not have access to view this information or suggest a correction. They may enlist privileged Department end-users to update on their behalf.
- ***Federal Assistance:*** End users can correct inaccurate or erroneous PII by editing the appropriate data fields on their user profile on the specific federal assistance module and application forms.
- ***Warehouse Management:*** DS-584 is physically provided to the end-user (i.e., the individual being issued the loaned property) in a printed form when the loan of the property is physically completed. At this time, they can review the information for updates and sign the document for filing. If the information is not correct, the original loan transaction (and DS-584) would be cancelled and a new loan transaction (and DS-584) would be created with the corrected data for the end-user to review and sign.
- ***Diplomatic Pouch and Mail Management:*** End users can correct inaccurate or erroneous PII by editing the appropriate data fields on their user profile on the specific diplomatic pouch and mail management module.
- ***Expendables:*** End users should work with GTM to make the necessary PII updates and the updated information will integrate into ILMS accordingly. If an ILMS support desk ticket is opened for the Expendables module regarding invalid data (SSN, name, DOB), the end user will be redirected to contact GTM (GEMS) to resolve the data issue. If urgent, the support desk can escalate the request to a system administrator to provide the customer with the invalid information within the system or make the correction directly in ILMS to enable post to process transactions.
- ***Transportation Management:*** End users should work with GTM (GEMS) to make the necessary PII updates and the updated information will integrate into ILMS accordingly. Privileged users such as traffic managers and travel counselors can update the PII records in ILMS. Users would be aware of any necessary changes that need to be made with PII when submitting their ILMS packouts to move from one location to another. Overall, even if changes are made directly in ILMS any changes to PII should be made with GTM (GEMS) as that information will integrate into ILMS.
- ***Fleet Management:*** Users with admin privileges can make changes to a user profile without submitting a help desk ticket. However, vehicle information cannot be edited by users and drivers will need to submit a ILMS Support help desk ticket to make those changes in ILMS. Driver specific information (i.e., driver’s license number, email address, phone number, etc.) are editable by anyone with edit permission to the employees’ module (usually supervisors/dispatchers).

If no, explain why not.

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

All users using the ILMS system are notified on how to correct their information during webinar training, which includes training materials for the respective application modules on processes and procedures to correct wrong inputs/information. In addition, end-users can find information on the procedures to update their PII on the support section which is available within the system.

All end-users accessing the Procurement, Diplomatic Pouch and Mail, and Fleet Management modules are prompted to review the information in their profile annually and may correct any inaccuracies by submitting an ILMS Support Desk ticket.

- ***Federal Assistance:*** End users are prompted to review the information on their user profile and application forms annually and are advised to correct any inaccuracies by updating the appropriate PII fields on their user profile. These data fields are editable on their user profile and application forms.
- ***Warehouse Management:*** Corrections are done in real time before the transaction is completed.
- ***Expendables and Transportation Management:*** Users are made aware from their training at Foreign Service Institute (FSI) to contact GEMS to update their PII to avoid any discrepancies but can also reach out to A/LM/OPS/TM or Transportationquery@state.gov. Transportationquery@state.gov includes Traffic Manager, Travel Counselors and A/LM/OPS/TM and operates like a Customer Support Desk for these users. They will provide travelers the proper guidance on next steps including reaching out to GTM.

Additionally, the Department's Privacy Act practices allow for record subjects to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the System of Records Notice, "Security Records, STATE-70.

8. Security Controls

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

The information is secured via multifactor authentication to access the system as well as the implementation of data at rest encryption. Information is also secured by using the concept of 'least privilege' which necessitates granting access only needed for the user's approved role, as indicated on their account request form. The system complies with all Department security mandates as well as risk management framework (RMF) security controls.

(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).

- ***Procurement*:**

  End-Users: Procurement end-users are only able to see PII that pertains to their business unit. These users include section approvers, procurement agents, accountants, financial management officers, and contracting officers. Procurement agents and GSOs have full access to Ariba vendor records associated with their post or business unit, which does not contain banking details. This restricts PII to those with a need to know. Most modules allow ad-hoc assignments to end-users outside of the current business unit with a need to know – such as the eFiling assignment of a CO/COR, and ad-hoc approvers in Ariba. This provides access to a particular request or document, but not the entire business unit. Ariba users have access to all attachments on any request which is routed to them for approval. These attachments may contain PII information as well. Other non-ILMS users such as vendors are often foreign nationals and do not have access to view this information or suggest a correction.

Privileged Users and Administrators: ILMS support personnel to include, developers and system administrators have access to all the PII across business units. The support personnel have elevated privileges to implement system enhancements and patches as required by the business. These privileged users and administrators have full access to any information in ILMS.

Support Users: Help desk role or functional support permission that has access to the procurement module PII for system troubleshooting purposes. This role has access to all PII across business units.

- ***Federal Assistance*:**
  End-Users: ILMS Federal Assistance consists of grantors and grantees. Grantors are Department users that assist grantees with the federal assistance planning, pre-award, award, post-award, and closeout processes. Grantors' permissions are designated for Department end-users, and only permits access to the front-end and restricts visible records by requesting office/business unit. This role has access to view the following PII elements from grantees and grantors in the business units they are associated with, except for EIN/TIN which is only from grantees. Grantees are individuals applying to and/or recipients of federal assistance grants. These end-users are permitted access only to their own data profile.

  - User ID
  - First and Last Name
  - EIN/TIN

  Administrators: Administrators have access to PII as part of their system operations and maintenance responsibilities. This role has access to all end-user profile pages and the following PII listed above. Administrators are not privileged users.

  Support Users: Help desk role or functional support permission, designated for Tier 1 and 2 help desk users, as well as Tier 3 system technicians. This role permits access to view and update bureau configurations and user accounts. This role has access to the entire user profile data and application data, and only to the following PII elements:

  - User ID
  - First and Last Name
  - EIN/TIN

- ***Warehouse Management:***

End-Users: This is a group of Department of State U.S. Direct Hire employees that manage issuance of program property to employees of the program prior to their deployment to the field. This role has access to view the following PII elements:

- First and Last Name
- Email Address

Privileged Users: This is a group of Department of State U.S. Direct Hire employees that manage the overall program which owns and reports on property being issued to employees. This role has access to view the following PII elements:

- First and Last Name
- Email Address

- ***<u>Diplomatic Pouch and Mail Management:</u>***

  End-Users: Clerks are responsible for making sure that the mailroom operates smoothly and that the mail is tracked properly in ILMS. This includes the processing of inbound and outbound mail. This role has access to view the Customer Directory for Posts they have access to, and only to the following PII elements:

  - First and Last Name, Business/Home/Remittance Address
  - Signature of Mail Recipients

  Privileged Users: Supervisors such as GSO staff at Post, Travel and Transportation Management staff in DC and mailroom staff are responsible for overseeing mailroom operations and using ILMS to process mail and manage the configured settings of their Post in ILMS. This role has access to view the Customer Directory for Posts they have access to, and only to the following PII elements:

  - First and Last Name, Business/Home/Remittance Address
  - Signature of Mail Recipients

  Administrators: Developers and contractors that have access to additional configuration pages to perform system enhancements and patches as required by the business. This role has access to view the Customer Directory for Posts they have access to, and only to the following PII elements:

  - First and Last Name, Business/Home/Remittance Address
  - Signature of Mail Recipients

- ***<u>Expendables:</u>***

  End-Users: Health Unit personnel at post have Medical Expendable User access, which is a general user access. Users may view and update inventory information and complete processes and transactions. This access allows them to complete tasks contained with the Medical Expendables module functionality, such as receiving, dispense, submitting replenishment orders, managing post-specific health unit locations, and viewing reports. The access is limited only to the posts to which the user has access, so generally only one post. The exception is Regional Medical Officers (RMOs) and Managers (RMMs), which may have multi-post access as they are responsible for overseeing multiple post health units. This role has read access to the entire profile and PII associated with the Health Unit(s) for which they have access, based on Defined User Preferences.

Privileged Users: Titled Medical Expendables Master, these privileged users can make administrative updates in their Health Unit configuration. Only select Accenture Federal Services (AFS) personnel and MED/QM leadership in Washington, DC have access to the Medical Expendables Master role. This role grants access to the "MEDx Master Configuration" page where those users may take such actions as updating the global Master Item List, medical item categories and pharmaceutical expiration dates. This role has access the entire profile and PII associated with the Health Unit(s) for which they have access, based on defined user preferences.

Administrators: Titled .NET (software framework) - Medical Expendables these are individuals with development roles. This role has read access to the entire profile and PII accessible in the module, for all Health Units

- ***<u>Transportation Management</u>*:** All Transportation Management users have access to the following PII:
  - First and Last Name
  - Last 5 digits of SSN – Read Only for Audit purpose.
  - Addresses - Only for the handled origin and destination address details
  - Email Address
  - Phone Numbers
  - Date of Birth – This is the only additional PII that is available on the profile that the end-users could have access to.

End-Users: Travel counselors and bookers under the Central Transportation Management with a business need-to-know and overseas shipping staff. These end-users are responsible for managing transportation services for personal effects shipments. Travel counselors are responsible for coordinating transportation services for individual shipments while bookers provide similar services for shipments that require freight forwarding services, which involves coordinating several shipment legs to get the shipment to its final destination. Overseas, shipping staff are further restricted to only have access to PII for employees stationed at their post, for whom they must coordinate shipments. This role has access to the entire user profile page (traveler profile) and can view the PII listed above. In particular, end-users can see the last 4 digits of their own SSN, which comes from GEMS, on the traveler profile.

Privileged Users: Traffic managers and logistics managers who are ultimately responsible for all personal effects shipping have access to monitor all personal effects shipments for quality control and strategic planning (e.g., awarding contracts to transportation vendors). This role has access to the entire user profile page (traveler profile) and can also update the PII listed above. In particular, privileged users can see the last 5 digits of the SSN for every profile in the system.

Support Users: Support users for the ILMS Transportation module have access to PII for system troubleshooting purposes. This role has access to the entire user profile page (traveler profile) and the PII listed above. In particular, support users can see the last 5 digits of the SSN for every profile in the system.

Administrators: Administrators have access to PII as part of their system operations and maintenance responsibilities. This role has access to the entire user profile page (traveler profile) and the PII listed above. In particular, administrators can see the last 5 digits of the SSN for every profile in the system.

- ***Fleet Management*:** All Fleet Management users have access to the following PII:
  - First and Last Name
  - Vehicle Registration
  - License Plate Number
  - VIN Numbers
  - License Number
  - Email address
  - Telephone number

  Administrators: Developers who make system enhancements and are responsible for configuring and developing code to make system changes. The administrators also include the ILMS Accenture contractors that are part of the ILMS Fleet teams and help to troubleshoot the system when system users experience issues and work with the developers on enhancements. This role has access to view the entire profile on the Fleet Management module and modify technical system details. Based on their privileges, they can also edit and delete.

  Privileged Users: The Overseas Fleet Division Desk Officers manage a subsection of the total embassies that use the system. The embassies are broken up geographically and an Overseas Fleet Division Desk Officer is responsible for overseeing their respective division. They manage all motor pool operations from a Post level and from an administrative standpoint. This role has access to view and edit the entire profile page on the Fleet Management module and the PII elements above.

(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.

Potential users submit an account request form which is reviewed and approved by their supervisor, as well as the ILMS Information System Security Officer (ISSO) prior to granting the account. An annual review of accounts is conducted by supervisors and the ISSO to ensure access is granted at the correct level and only to the modules for which they have a need to access.

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

For the roles specified in 8(b), access to data in ILMS, and all its modules, is restricted based on the permissions granted by their approved access request form.

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

All users' (to include: end-users, privileged users, support users, and administrators) actions executed within ILMS are logged in a table and viewable/searchable by system administrators. System administrators are unable to edit these logs and can only view for the purposes of continuous monitoring. The system administrators monitor the logs and get email alerts for any attempts at gaining unauthorized access, unusual activity, and integration errors. There is an established baseline of normal system activities, and the system uses Splunk to monitor and notify on activities outside of that baseline. Login and logout activity are tracked in ILMS and its associated applications, as are the addition or removal of roles within the system. The ISSO also has access to monitor system administrators' actions executed in the system.

(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. All Department employees are required to take the annual mandatory Cyber Security Awareness course PS800, which contains a privacy module, and the biennial privacy course, PA318 Protecting Personally Identifiable Information, delivered by the Foreign Service Institute.