PRIVACY IMPACT ASSESSMENT

OBO Electronic Model Lease (OBO EML)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: August 2022
(b) Name of system: OBO Electronic Model Lease
(c) System acronym: OBO EML
(d) Bureau: Overseas Buildings Operations
(e) iMatrix Asset ID Number: 322153
(f) Child systems (if applicable) and iMatrix Asset ID Number:

(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 Bureau of Overseas Building Operations (OBO) and posts use the Electronic Model Lease (EML) application to do Post's leasing actions for residential, offices, structures, lands, and functional properties, including assigning occupants to residential properties and communicating with landlords. The OBO EML application provides post with the

ability to manage all aspects of its real property leases in an automated environment. This includes but is not limited to leasing and housing. EML is key to supporting other OBO systems including the Real Property Application (RPA) for maintaining real property assets and the electronic Lease Waiver (eLWR) application for providing waivers for occupants to reside in available leased properties.

EML information provides OBO with an automated system to track the leasing, renewal, and termination of buildings, lands, and structures by the Department.

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

Names of Subject Occupant
Family Information (names, number and age of occupants)
Personal Address of Post-assigned Residence
Property Owner Name (US persons/non-US persons)
Property Owner Personal Email Address
Property Owner Personal Address
Property Owner Personal Phone Number
Financial Information (Amount of Lease)

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

22 U.S.C. § 300 - Dispositions of property; damage payments; acceptance of gifts or services
5 U.S.C. 5912 - Quarters in Government owned or rented.

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

☒Yes, provide:

- SORN Name and Number:
  Contractors Records, STATE-45
  Human Resource Records, STATE-31

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  September 27, 1977
  July 19, 2013

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☒Yes ☐No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Schedule number: N/A

- Disposition Authority Number:
DAA-0059-2020-0019-0011
DAA-0059-2020-0019-0005

- Length of time the information is retained in the system:
Destroy 7 years after the property is no longer owned/leased by the Department.
Destroy when 20 years old

- Type of information retained in the system:
EML will contain data regarding costs, leases, and other contracts associated with real estate and facilities; project management tracking; planning and budget data; maintenance, operations, and planning management data; and other related data. EML also contains name, personal address, and contact information of leasing occupants and property owners.

  Backup of Files: Electronic copy, considered by the agency to be a Federal record, of the master copy of electronic record or file retained in case the master file or database is damaged or inadvertently erased. Incremental backups are done daily; full backups are done weekly and monthly to storage area network on disks.

4. Characterization of the Information

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

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

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

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

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

☐Yes ☐No ☒N/A

- If yes, under what authorization?

(d) How is the PII collected?

OBO EML users enter the PII of occupants by associating them to the appropriate lease or they may search a list of occupants provided by the Real Property Application (RPA) associating the occupants to the appropriate lease. PII may be provided by Human Resources at Post using the State Department's Human Resources system. PII of landlords is provided by landlords and/or agents representing the landlords to the USG Employee and/or USG Contractor by phone, email, or in person conversation.

(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?

OBO EML quality assurance actions to verify PII include reviewing data for missing information and correcting technical errors that prevent submission.

Additionally, the coordination and collection of property lease documentation and reviews of that documentation are done for completeness prior to approval and execution of leases in OBO EML. Post management, including the General Services Office (GSO), the Financial Management Office (FMO), and OBO, together validate lease entries and ensure completeness and accuracy of the data and attachments during the approval process.

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

Posts are required to update the information in EML prior to completing all lease transactions, as a business process. This ensures the information in EML remains current.

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

The system does not use information from commercial sources. The information is not publicly available.

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

The information collected is the minimum PII required for reporting and verifying occupant information in order to complete business processes.

5. Use of information

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

The data are used to assign occupants to residential properties. Landlord information is used for notices and other communication from posts or headquarters including terminations, amendments, and renewals of leases.

(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, OBO EML was designed for the management of leases. The PII is necessary in order to ensure that the occupant is being placed in appropriate housing based on criteria including their rank within the State Department and their family size, i.e., number of persons on their orders who will be living at Post.

(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.

Internal: Information is shared internally with the Real Property Application (RPA).

External: There is no external sharing.

(b) What information will be shared?

Internal:
Names of Subject Occupant
Family Information
Property Address of Post-assigned Residence
Property Owner Email Address
Property Owner Address
Property Owner Phone Number

External: N/A

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

Internal: PII is sent to the Real Property Application for the purpose of lease and property management.

External: N/A

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

Internal: Information will be encrypted within the Department's SBU OpenNet system. EML provides a representational state transfer application programming interface (REST API) that allows for the bi-directional transfer of information between RPA and EML. The API allows EML to send data to RPA and RPA to send leasing data to EML on an as-needed basis.

External: N/A

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

Internal: Information will be encrypted with the Department's SBU OpenNet system and transferred via REST API to RPA. Additionally, the WebAPI uses Hypertext Transfer Protocol Secure endpoint on the Department's secure network to ensure that the data is encrypted during transit using TTLS/SSL.

External: N/A

7. Redress and Notification

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

Notice is not provided to the record subject prior to the collection of information. Most record subjects' information is received from HR or RPA so there is not an opportunity to provide them with notification as EML does not collect the information from record subjects directly.

Most landlords are not U.S.-persons but for those who are, it is the responsibility of each post to provide notice at the point of collection.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐Yes ☒No

If yes, how do record subjects grant consent?

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

The majority of records subjects' information is obtained from HR so they do not have the opportunity to decline to provide information or grant consent. For the few landlords who are U.S.-persons, consent is granted by providing their information as noted in 4(d).

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

Subject occupants are not able to gain access to their information in OBO EML. Individual employees/contractors who want to gain access to their information must file under the Privacy Act as outlined in the SORNs cited at 3f. Property owners do not have access to their information in OBO EML.

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

☒Yes ☐No

If yes, explain the procedures.

Subject occupants are able to correct their information in OBO EML by emailing their Post Management General Services Office. Individuals receive initial instructions on correcting their information in OBO EML from the General Services Officer at Post. Further instructions to correct inaccurate or erroneous information may be found in the applicable SORNs cited in 3f.

If no, explain why not.

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

Individuals receive initial instructions on correcting their information in OBO EML from the General Services Officer at Post. Post or OBO personnel manage the information internally using reports. In the event data is incorrect, individuals can request changes with the responsible management authority at post or at OBO Headquarters. Record subjects may also view procedures to correct their information in the applicable SORNs cited in 3f.

8. Security Controls

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

The information in the system is secured by Active Directory (AD)/Single Sign on (SSO) and the user is granted access to the OBO's Electronic Model Lease application using the users PIV card. Information in the system is also secured by the system's user role-based security including authentication and authorization of access.

(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).

Post Users
Post Users can see all PII in 3(d) and include:

- Facilities Staff, Financial Staff, Housing Staff, and Management Officers
- Create, edit, and submit new electronic leases, terminations, amendments, and renewals.
- Create and edit existing electronic leases, terminations, amendments, and renewals.
- Execute electronic leases, terminations, amendments, and renewals.

Post Management Users
Post Management Users can see all PII in 3(d) and include:

- General Services Officer(s) and Financial Management Officer(s)
- Create, edit, and submit new electronic leases, terminations, amendments, and renewals.
- Create and edit existing electronic leases, terminations, amendments, and renewals.
- Approve Post user electronic leases, terminations, amendments, and renewals.
- Recommend approval of certain electronic leases to HQ users.

Headquarters (HQ) Users
Post Users can see all PII in 3(d) and include:

- Legal, Real Property Portfolio Management (RPL), Knowledge Management (KM), Area Management (AM)
- Have all of the permissions of the post management user and can also assign electronic leases to other HQ users.

System Admin Users

Post Users can see all PII in 3(d) and include:

- Development Staff and Real Property Portfolio Management (RPL)
- Have all of the permissions of the headquarters users and also approve/reject user access accounts.

(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.

As Electronic Model Lease (EML) is available on the Department of State OpenNet system, a potential user must have access to OpenNet using a Personal Identification Verification (PIV) card and Multi-Factor Authentication (MFA) using Microsoft Authenticator. Once access to OpenNet has been authenticated, potential users can request access to the EML application.

If a potential user who does not have access to the Electronic Model Lease (EML) application clicks on or enters the link into their web-browser, the Electronic Model Lease (EML) 'No Access' page is displayed.

To gain access to the Electronic Model Lease (EML) application, a potential user is required to request access using the Electronic Model Lease (EML) application User Access Request form by pressing the 'Request Access' button.

Once pressed, the Electronic Model Lease (EML) User Access Request form is displayed and requires the potential user to provide their name, select post(s) to which they are requesting access to and to select their potential user role from the provided list shown in sections 8(b) and 8(d). The potential user saves and submits their Electronic Model Lease (EML) User Access Request.

The potential user's access request is reviewed by either post management or Washington, D.C. headquarters as detailed in sections 8(b) and 8(d). Management approval is required and approval is based on position as well as a need-to-know.

Upon approval or denial of the potential Electronic Model Lease (EML) Users Access Request, a follow-up email is sent to the potential user providing additional details about their Electronic Model Lease (EML) User Access Request.

Annually, all Electronic Model Lease (EML) user access is reviewed and confirmed as needed or not needed based on their user role as detailed in sections 8(b) and 8(d).

Accounts are deactivated after 90 days of no activity. Emails are sent to users at 15, 7, 5, and 1 day(s) prior to deactivation. Once deactivated, user accounts are deleted the following day.

Users are able to request a change to their user role by submitting a User Access request that must be reviewed and approved or denied by the appropriate personnel.

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

Potential users must request access via the Electronic Model Lease (EML) application. The Electronic Model Lease (EML) User Access Request is reviewed by the appropriate staff based on the user role selected and is either approved or denied based on the employees need to know. A follow-up email is sent to potential users with additional details on their User Access Request. Access is reviewed on an annual basis and rescinded if there is no longer a need-to-know. Following is a listing of the User Roles available for selection:

- **Post Users –** Post management users review initial access request and conduct annual access review.
- **Post Management Users –** HQ users review initial access request and conduct annual access review.
- **Headquarters (HQ) Users** – System admin users review initial access request and conduct annual access review.
- **System Admin Users**
  - Access requests reviewed by HQ users.
  - Access is reviewed annually by HQ users.

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

NIST 800-53 Rev 4, App. J controls are in effect and enforced, and auditable events are captured by Splunk. The information can only be accessed by PIV card and is Single Sign-on enabled which prevents impersonation by any users. Changes or additions to existing data are captured in application audit logs. The audit logs document unintended modification and unauthorized access, and dynamically audit retrieval access to data that are designated as critical.

(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 are no role-based privacy trainings but all OpenNet users with access to EML are required to take the mandatory PS800 - Cybersecurity Awareness Training, which has a privacy component, annually and the PA318 “Protecting Personally Identifiable Information” training on a biennial basis.