

PRIVACY IMPACT ASSESSMENT

OpenNet Microsoft Exchange

1. Contact Information

A/GIS Deputy Assistant Secretary

Bureau of Administration

Global Information Services

2. System Information

(a) **Date of completion of this PIA:** February 2023

(b) **Name of system:** OpenNet Microsoft Exchange

(c) **System acronym:** OME

(d) **Bureau:** Information Resource Management (IRM)

(e) **iMatrix Asset ID Number:** 737

(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 OpenNet Microsoft Exchange (OME) is an administrative remnant email messaging support that facilitates or streamlines back-end legacy systems' administrative functionalities like delivery of record-email to archives, delivery of system-state alerts to

technical staff, dissemination of broadcast email to all Department recipients (like Department Notices), and delivery of other email notifications associated with system related business functions.

Previously, OpenNet Microsoft Exchange (formerly known as OpenNet Email SBU) was exclusively an on-premises system that hosted all electronic mailbox types (e.g., User, Shared, Health, Resource, Service Account). Today, all User (employee) electronic mailboxes reside in Exchange Online within Microsoft 365 (the cloud) and the Department's Office 365 boundary. Although interconnected with OME, Exchange Online (cloud email system) is a distinct and separate email system from OME.

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

OME references limited PII (i.e., name and email address) against that stored in Active Directory (AD) to validate or authenticate access to OME mailboxes and enable accurate email delivery and receipt. When a user is assigned access to an OME mailbox, their login credentials are validated in AD to resolve the appropriate access to the respective OME mailbox(es).

OME is not designed or intended to collect or be a repository for PII. However, PII may be received in a few OME mailbox use cases. The mailboxes in these instances are receive-only. When email is received in these mailboxes, in most cases it is offloaded to back-end systems and deleted from the email inbox after a few seconds or minutes. For example, mailboxes that facilitate archiving of personnel-related communications will contain PII for a short time. All email received in these mailboxes are pulled and transferred within minutes to the Global Talent Management (formerly HR) Career Development Archive Retrieval System (CDARS/HRCDA) archive. Afterward, emails in the associated OME mailboxes are deleted. In OME mailboxes that support the Bureau of Consular Affairs (CA) Immigration Visa Adjudication process, email can remain in the mailbox for up to 40 days depending on CA's backlog status. Once processed, the email is uploaded into the CA Electronic Document Processing System and removed from OME.

The following information are examples of what may be temporarily stored in OME mailboxes:

1. Social Security Numbers
2. Birth Certificates
3. Naturalization Certificates
4. Medical records
5. Driver's license information
6. Banking information
7. Passport numbers
8. Full name
9. Address
10. Birthdate

In other OME mailbox scenarios the mailboxes do not receive or collect PII at all. They facilitate the delivery of status alerts associated with system functionalities. For example, a mailbox may receive an email from IRM/SIO (System Integration Office) datacenter monitoring feeds to alert when there is a system dashboard failure or anomaly. Likewise, other mailboxes enable delivery of email system health events (trapped by System Center Operations Manager (SCOM)) to the email technical support staff. In another case that does not collect PII, the mailbox traps or quarantines email that meet specific security heuristics criteria and have been flagged malicious or suspicious.

While IRM operates and maintains the OME system, the information contained in each OME mailbox is owned by the individual bureau/office/post that has a business need for that mailbox and the data within it. In cases where PII may be received, the email is acted upon by processes that transfer the email to disparate (separate from OME) Bureau back-end systems or archives. The email messages are deleted and purged from the OME mailboxes after the email has been auto ingested to the back-end system.

Any PII collected and stored by back-end Bureau stakeholders is subject to the functional authority of the office collecting and offloading the information to their respective back-end systems or archive repositories.

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

22 U.S.C § 2651a (Organization of the Department of State)
5 U.S.C. § 301 (Management of the Department of State)
44 U.S.C. § 3101 (Records management by Agency heads)

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

☐ Yes, provide:

- SORN Name and Number:

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

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

OME is a tool that enables business communication by way of email, but it is not a "system of record" used to collection, maintain, use or disclose records containing PII as that term is defined in the Privacy Act of 1974.

(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.

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.)

OME is not a repository or archive system for email data and no backups of the mailboxes are performed. All email is journaled to eRecords, the official archive of email for the Department of State and a separate system from OME.

If yes provide (Consolidate as much as possible): [Click or tap here to enter text.](#)

Schedule number: N/A

- Disposition Authority Number: DAA-GRS-2014-0001-0001 (GRS 6.1, item 010) (Email of Capstone Officials)
- Length of time the information is retained in the system: Cut off in accordance with agency's business needs. Transfer to NARA 25 years after cutoff, or after declassification review (when applicable), whichever is later
- Type of information retained in the system: Email of Capstone Officials

Schedule number: N/A

Disposition Authority Number: DAA-GRS-2014-0001-0002 (GRS 6.1, item 011)
(Email of Non-Capstone officials)

Length of time the information is retained in the system: Temporary. Delete when 7 years old, but longer retention is authorized if required for business use.

- Type of information retained in the system: Email of Non-Capstone officials.

Schedule number: N/A

- Disposition Authority Number: DAA-GRS-2013-0005-0004 (GRS 3.1, item 020) (Information Technology Operations and Maintenance Records)
- Length of time the information is retained in the system: Destroy 3 years After agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.
- Type of information retained in the system: Records associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications

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?

OME is neither designed nor intended to serve as a PII repository or archive. It is an administrative messaging conduit that lends efficiencies to the execution of back-end bureau business requirements, such as delivery of record-email to archives, delivery of system-state alerts to technical staff, dissemination of broadcast email (like Department and Lapse of Appropriation Notices), and delivery of other email notifications associated with other system related business functions.

To authenticate mailbox users to the system, OME references limited PII (i.e., name and email address) and validates it against what is stored in Active Directory (AD). When a user is assigned access to a mailbox in OME, their login credentials are validated in AD to resolve the appropriate access to their office's respective OME mailbox(es).

While IRM operates and maintains the OME system, the information contained in each OME mailbox is owned by the individual bureau/office/post that has a business need for that mailbox and the data contained therein. In cases where PII may be received, the emails in the respective OME mailboxes are acted upon by automated processes that offshore the email to disparate (separate from OME) bureau back-end systems or archives. The email messages are deleted and purged from the OME mailboxes after the email has been auto ingested to the back-end system.

Any PII collected and stored by back-end bureau stakeholders is subject to the functional authority of the office collecting and offloading the information to their encrypted back-end systems or archive repositories.

(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?

To authenticate mailbox users to the system OME determines PII accuracy by querying Active Directory (AD), which validates usernames and user email addresses. None of those (usernames and email addresses) are stored in OME and no mailboxes associated with individual users or employees (User mailboxes) reside in the OME system.

Accuracy of the information maintained in an OME mailbox is the responsibility of each bureau/office/post that collects and owns the information.

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

To authenticate mailbox users to the system, OME queries information against what is stored in AD. This ensures that name and email address remain current.

Maintaining and ensuring accurate information within OME is the responsibility of each bureau/office/post.

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

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

The use of information collected in OME by the legacy applications vary by the mission of the office/bureau/post.

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

OME does not collect PII. However, the querying of usernames and emails are the minimum necessary to deliver emails to recipients, if needed, and to configure access to OME mailboxes.

Rules of Behavior exist for employees to ensure their adherence to the laws and regulations governing the use and maintenance of OME. Privacy concerns are to be taken into consideration by the individual offices/bureaus/posts when determining what information to collect and store.

5. Use of information

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

OME references PII in AD to authenticate mailbox users to the system.

Uses of PII received in OME mailboxes is dependent upon the business needs of the bureau/office/post gathering the data. An example of Department of State business processes that may maintain data in OME is the issuance of Visas.

(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. OME references PII that exist in Active directory for the purpose of administrating OME mailboxes.

The relevance of PII collected in OME by the legacy applications vary by the mission of the office/bureau/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:

No PII is shared internally.

External:

No PII is shared externally.

(b) What information will be shared?

Internal:

No PII is shared internally.

External:

No PII is shared externally.

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

Internal:

No PII is shared internally.

External:

No PII is shared externally.

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

Internal:

No PII is shared internally.

External:

No PII is shared externally.

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

Internal:

No PII is shared internally.

External:

No PII is shared externally.

7. Redress and Notification

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

No; notice is not required under the Privacy Act. OME does not collect PII, but only administers mailboxes and facilitates delivery of email.

Notice methods for content within OME may vary by bureau/office/post and may include the appropriate covering SORN.

(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 Privacy Act does not apply. Employees receive email addresses outside of the OME system, and their associated email addresses and names are stored in Active Directory. Consent is received to collect the information by AD when the applicant fills out the application for access. Employee mailboxes reside in Exchange Online (the cloud) and not OME.

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

The Privacy Act does not apply to the information handled in OME. User account information does not exist in OME.

Individuals wishing to access and amend Privacy Act covered information collected by the relevant sources and services should follow procedures defined in 22 CFR Subpart D 171.33 at <http://2001-2009.state.gov/documents/organization/108115.pdf> or via the Government Publishing Office (GPO) at <https://www.gpo.gov/fdsys/pkg/CFR-2012-title22-vol1/xml/CFR-2012-title22-vol1-part171.xml>. In addition, full instructions for accessing and amending PII held by the Department are available at the U.S. Department of State Freedom of Information Act (FOIA) website at <https://foia.state.gov/>. The site also provides complete information on FOIA, the Privacy Act, and related statutes and policies.

In addition to the procedures mentioned above, any additional access procedures for sites/instances will vary by the bureau/office/post.

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

☐ Yes ☒ No

If yes, explain the procedures.

If no, explain why not.

The Privacy Act does not apply to the information collected by OME. OME does not contain user account information.

Amendment procedures will vary by the mission of the bureau/office/post.

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

The Privacy Act does not apply to the information used by OME for the purposes of administering mailboxes.

Changes to information concerning an individual's PII are not made within the OME system. Subjects would need to contact the individual bureau/office/post collecting their PII to work through the process prescribed by that office in accordance with associated governance and regulations.

8. Security Controls

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

Information and access to system resources are secured through multiple layers of security to include personal identification verification (PIV) card access to server operation centers, multi-factor authentication, encryption applied to data at rest in the SIO's Enterprise Server Operations Centers (ESOCs). All data is secured by Transport Layer Security (TLS) when in transit. In addition, perimeter security; as well as active and monitored role-based access controls implemented through AD group membership to control individual access based on authorized roles and responsibilities are implemented.

(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).

Access Roles	Level of Access	PII Access
System Administrators	A limited number of System Administrators have access to OME to perform routine maintenance (e.g., software updates, hardware upgrades) and troubleshooting.	All PII listed in 3d according to their role and business need in specific scenarios.
Developers	A limited number of developers have access to OME to program new functionalities in the system. Developers' access focuses on system code.	No production PII is needed only that which is generated in development to validate functionality of a specific use case
End Users	End-users, according to their respective support roles in each bureau/office/post use case, have limited scope access based on that which is needed to perform their functions (which are specific to their bureau/post mission.)	A subset of PII data listed in 3d according to the their limited scope roles and business function(s)/office mission.

(c) Describe the procedures established to limit system and data access to only those individuals who have an “official” need to access the information in their work capacity.

Access is enforced by profiles according to the principle of least privilege, requirements of need, need-to-know and role and are executed as outlined in section b above.

Access Roles	Level of Access	PII Access
System Administrators	Front-end application and database	Read only for maintaining application operations and troubleshooting
Developers	Front-end application and code	Read only for validating and testing functionality changes.
End Users	Front-end application	Read, Update and Delete

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

System Administrators: must petition for access via the IRM Enterprise Services Portal. Privileged accounts (e.g., System Administrators, etc.) must complete a request for Tier 1 Admin and Service Accounts for OpenNet, ClassNet, and DMZ Enclaves. The request(s) must be approved by the Supervisor, ISSO, Branch or Division Chief, and the Contracting Officer’s Representative (if a Contractor) before being approved and enabled by IRM’s Enterprise Network Management (ENM).

Developers: must petition for access via the IRM Enterprise Services Portal, however, since no additional features, functions, or capabilities are being added in OME, this role is being phased out. There is no need for additional developers.

End Users: must submit a form titled “Request to Create Network-Domestic SMART” Account via the Enterprise Services portal. Then they must petition for OME access through their respective office management. Once proper approvals are received, the Mailbox Owner enables end-user access to the respective OME mailbox.

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

OME integrates with Microsoft System Center Operations Manager (SCOM) to detect and alert anomalous system behavior and configurations. OME integrates with Splunk security information and event management (SIEM) tool to monitor/audit system

activities and provide data analytics. Splunk also captures and retains system security specific events logs. OME integrates with iPost to audit noncompliant security settings and report risks scores. Each of these tools is used to evaluate the safety of OME and each tool has a dedicated staff of administrators to monitor and address discoveries and events around the clock.

(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.

All users are required to take the biennial privacy course, PA318 Protecting Personally Identifiable Information, and the annual cyber security course, PS800, Cyber Security Awareness, delivered by the Foreign Service Institute.