PRIVACY IMPACT ASSESSMENT

eRecords Management System

1. Contact Information

<table>
<thead>
<tr>
<th>A/GIS Deputy Assistant Secretary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bureau of Administration</td>
</tr>
<tr>
<td>Global Information Services</td>
</tr>
</tbody>
</table>

2. System Information

   (a) Date of completion of this PIA: September 2023
   (b) Name of system: eRecords Management System
   (c) System acronym: eRecords
   (d) Bureau: Information Resource Management
   (e) iMatrix Asset ID Number: 240260
   (f) Child systems and iMatrix Asset ID Number (if applicable): N/A
   (g) Reason for performing PIA:

   ☒ To update existing PIA for a triennial security reauthorization

   (h) Explanation of modification (if applicable):

3. Purpose

   (a) Describe the purpose of the system.

   eRecords serves multiple, interrelated content management needs. First, eRecords captures all OpenNet emails (and attachments) involving a Department of State email account on the state.gov domain. All OpenNet emails are retained in a secure repository per NARA retention rules. Second, eRecords includes a self-service portal for Department users to retire office records per records management guidelines. Third, eRecords includes a self-service portal for Department users to submit content responsive to Freedom of Information Access (FOIA) and other transparency requests. Authorized users may search, retrieve, and export content from eRecords as part of their employment duties.

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

   The system stores all emails, attachments, and documents that are sent/received over OpenNet on the state.gov domain collected under the specific authorities of the originating office such as: personnel management, payroll, and other authorized administrative functions. The information included in the emails may include but is not limited to full name, date of birth, social security number (SSN), home/work address,
and other personnel information (such as Employee ID). As a byproduct of full text indexing, the system will collect the content of all emails.

The stored PII can be accessed by authorized users responding to FOIA requests, Congressional queries, litigation, and criminal investigations.

NOTE: Even though IRM houses the information, individuals sending an unclassified email containing PII are responsible for the PII collected.

(c) How is the PII above collected?

The information is collected through emails that are sent/received over OpenNet on the state.gov domain. Whenever an email is sent or received, the system indexes and stores the email along with its attachments until it is deleted pursuant to the appropriate NARA-approved disposition schedule.

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

eRecords is used to capture all e-mails and attachments that interact with a state.gov e-mail account and store them in a secure repository that allows for search, retrieval, and disposition by authorized users. This collection and storage meets Federal Records Act requirements as well as OMB Directive M-12-18 Managing Government Records Directive. Authorized Department users will be able to access the eRecords archive to comply with FOIA requirements, Federal Records Act requirements, Congressional queries, litigation, criminal investigation, and other administrative purposes authorized by law or regulation.

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

☒ Yes  ☐ No

If no, please explain:

4. Authorities and Records
(a) What are the specific legal authorities and/or agreements that allow the information to be collected?

44 U.S.C. 3544 – Coordination of Federal Information Policy

(b) If the system contains Social Security numbers (SSNs), list the specific legal authorities that permit the collection of Social Security numbers.

The system stores the full text of email documents and attachments, some of which may include SSNs collected under the specific authorities of the originating office such as:
personnel management, payroll, and other authorized administrative functions. As a byproduct of full text indexing the system will collect the content of all emails.

(c) In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)?

☐ Yes, please indicate relevant System of Records Notice (SORN) below.

- SORN Name and Number:

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

eRecords is not a “system of records” as defined by § 552a(a)(5) because it (1) does not index files by personal identifier and (2) is not used to retrieve data by using a personal identifier.

(d) 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.

(e) List the Disposition Authority Number(s) of the records retention schedule(s) submitted to or approved by the National Archives and Records Administration (NARA) for this system?

DAA-GRS-2014-0001-0001 (GRS 6.1, item 010)
DAA-GRS-2014-0001-0002 (GRS 6.1, item 011)
DAA-0059-2019-0001
DAA-0084-2015-0001-0005
DAA-0084-2015-0001-0007
DAA-0084-2015-0001-0009
DAA-0084-2015-0001-0001

5. Data Sources, Quality, and Integrity

(a) What categories of individuals below originally provide the PII in the system?

Please check all that apply.

☒ Members of the public (U.S. persons which includes U.S. citizens or LPRs)
☒ U.S. government employees/contractor employees
☐ Other (people who are not U.S. citizens or LPRs)

(b) Do the individuals listed in 5(a) provide PII on individuals other than themselves?

Please check all that apply.
Members of the public
☒ U.S. government employees/contractor employees
☐ Other
☐ N/A

(c) What process is used to determine if the PII is accurate?

There is no way for eRecords to determine if the PII is accurate. Accuracy of the content depends on the sender(s) of the email. The system is designed to index and store the content of the emails as received without modification.

(d) What steps or procedures are taken to ensure the PII remains current?

Emails are stored within hours of receipt and maintained for up to 25 years. They are current at the time of receipt. Emails cannot be accessed or changed by the sender once sent.

(e) Was the minimization of PII in the system considered?

☐ Yes ☒ No

If no, please explain.

The purpose of the system is to collect all email documents, attachments files, and cables that are sent or received over OpenNet. Inherently this will include retention of PII that is shared. Minimization of PII is not possible for this system.

(f) Does the system use information, including PII, from commercial sources?

☐ Yes ☒ No

If yes, please list the commercial sources.

(g) Is the information, including PII, collected from publicly available sources?

☐ Yes ☒ No

If yes, please list the publicly available sources.

(h) 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?

(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?

(i) If the system will use test data, will it include real PII?

☐ Yes  ☒ No  ☐ N/A - this system does not use test data

If yes, please provide additional details.

6. Redress and Notification
(a) Explain whether a notice is provided to the record subject at the point of collection of their information.

No, notice is not provided to record subjects by eRecords. The originating office/bureau has the responsible for providing notice to record subject, if applicable.

(b) Are opportunities available for record subjects to decline to provide the PII?

☐ Yes  ☒ No

If no, please explain why not.

Record subjects who use OpenNet will automatically have their emails and attachments retained by eRecords.

(c) Are opportunities available for record subjects to consent to particular uses (other than authorized uses) of PII?

☐ Yes  ☐ No

If yes, please explain.

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

Record subjects cannot gain access to their information in eRecords.
(e) Are procedures in place to allow a record subject to correct or amend their information?

☐ Yes  ☒ No

If yes, explain procedures and how record subjects are notified.

If no, explain why record subjects are not able to correct their information.

To ensure the integrity of email sent and received, individuals are not allowed to modify emails in the eRecords archive.

7. Sharing of PII
   (a) To what entities (outside of the owning office) will the PII be transmitted? Please identify the recipients of the information.

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Office of Legal Adviser (L)</td>
<td></td>
</tr>
<tr>
<td>Bureau of Diplomatic Security (DS)</td>
<td></td>
</tr>
<tr>
<td>Bureau of Administration (A)</td>
<td></td>
</tr>
<tr>
<td>The Office of the Historian (FSI/HO)</td>
<td></td>
</tr>
</tbody>
</table>

(b) For each of the entities in 7(a), list the PII from 3(b) that will be transmitted.

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Messages (body and attachments) that are relevant to a specific information access request will be shared.</td>
<td></td>
</tr>
</tbody>
</table>

(c) For each of the entities in 7(a), what is the purpose for transmitting the information?

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The purpose of sharing with the bureaus identified above is to allow the processing in order to comply with FOIA requirements, Federal Records Act requirements, Congressional queries, litigation, criminal investigation, and other administrative purposes authorized by law or regulation.</td>
<td></td>
</tr>
</tbody>
</table>

(d) For each of the entities in 7(a), list the methods by which the information will be transmitted.
<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized users within IRM will give access to eRecords for review with the bureaus and offices by granting limited one-time access to the system to see relevant information identified in a search in order to fulfill FOIA requirements, Federal Records Act requirements, Congressional queries, litigation, criminal investigation, and other administrative purposes authorized by law or regulation. Once given access, the designated office/bureau will select the pertinent emails so that IRM personnel can export and send to them via file transfer.</td>
<td></td>
</tr>
</tbody>
</table>

(e) For each of the entities in 7(a), what safeguards are in place for each method of internal or external transmission?

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>eRecords follows the Role Based Access Controls (RBAC) methodology. Authorized users within IRM are granted limited or full access (depending upon their need to know) for searching or sharing specified categories of information in the eRecords archive by a central systems office that is responsible for ensuring searchers are adequately trained. The system is designed to deny access except as need-to-know rights are granted. Furthermore, an audit trail of all access is generated to monitor behavior of searchers.</td>
<td></td>
</tr>
</tbody>
</table>

8. Security Controls
(a) How is all of the information in the system secured?

To ensure the security of the information within the system, the system has Transport Layer Security encryption as well as Transparent Data Encryption for data at rest. Along with that, there are myriad of security controls that will be enforced on the Department side as well as by our cloud provider (Azure).

(b) 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.

eRecords is housed in Microsoft Azure Cloud.

(c) In the table below, list the general roles that access the system (e.g., users, managers, developers, administrators, contractors, other). Include what PII is accessed, the procedure for each role to access the data in the system, and how access to the data in the system is determined for each role.

<table>
<thead>
<tr>
<th>Role</th>
<th>What does this role do?</th>
<th>What PII does this role have access to?</th>
<th>What rights to the PII does this user have (read-only, edits, etc.)</th>
<th>How does the role initially obtain access?</th>
<th>Who approves the role’s access?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Administrator</td>
<td>- Grant and remove users to/from Bureau Administrators groups - Set restrictions on roles the Bureau Administrator can create. - Manage the process of assigning users to the Auditor and Investigator roles. The Global Administrator does not have rights to use the eRecords archive in any other capacity.</td>
<td>This role has full access to PII.</td>
<td>The global administrator has full rights to PII.</td>
<td>System Administrator assigns them access.</td>
<td>System Owner</td>
</tr>
<tr>
<td>Bureau Administrator</td>
<td>- Provide and remove search access for users within their assigned Bureau only</td>
<td>This role has limited access to PII.</td>
<td>This role has limited rights to PII. This role will only be able to access the PII that was given by the Global Admin.</td>
<td>Access is given by the Global Admin</td>
<td>Global Admin</td>
</tr>
<tr>
<td>Role</td>
<td>Responsibilities</td>
<td>Access Level</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>- Search the archive to discover and view messages within the constraints established by the Bureau Administrator (and therefore limited by the Global Administrator) - Associate discovered messages to cases, for the purpose of establishing relevancy to a specific search reason - Share cases and discovered messages with other users who are granted at least same permission level</td>
<td>This role has limited access to PII.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investigator</td>
<td>Has full access to all messages within the archive regardless of security descriptors.</td>
<td>Full access to PII</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditor</td>
<td>Has unrestricted access to the specific information to which the user is assigned.</td>
<td>This role has limited access to PII</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Create various user roles depending on permissions set by the Global Administrator.  

They are only able to see what is within the constraints established by the Bureau Admin.  

Bureau Administrator  

Full rights  

Global Administrator  

Auditor  

Full rights  

Global Administrator  

Investigator  

Full access to PII  

Global Administrator  

Global Administrator  

Investigator  

Full access to PII  

Global Administrator  

Global Administrator  

Auditor  

Full access to PII  

Global Administrator  

Global Administrator
(d) After receiving initial access, describe the steps that are taken for the roles defined above to maintain access.

After initial access is given to the user, they will then be able to function within eRecords based upon the constraints set forth by the roles in which they were given. All actions taken by these various roles are logged within eRecords.

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

☒ Yes  ☐ No

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒ Yes  ☐ No

(g) Privacy Related Training Certification
   - Do all OpenNet users of this system take the course PA318 Protecting Personally Identifiable Information biennially?

☒ Yes  ☐ No
- Do all OpenNet users of this system take the course PS800 Cybersecurity Awareness Training annually?

☒ Yes  ☐ No

- Are there any additional privacy related trainings taken by any of the roles identified in 8(c) that has access to PII other than their own for this system?

☐ Yes  ☒ No

If yes, please list the related trainings here: