eRecords PIA

1. Contact Information

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

2. System Information

(a) Name of system: eRecords

(b) Bureau: IRM/OPS/MSO/MD

(c) System acronym: eRecords

(d) iMatrix Asset ID Number: OpenNet 240260/ ClassNet 254697

(e) Reason for performing PIA: Click here to enter text.

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

(f) Explanation of modification (if applicable): N/A

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
A full A&A by a 3rd Party Assessor is expected to be completed by January 2017.

(c) Describe the purpose of the system:
The purpose of the eRecords system is to capture all e-mails and attachments that interact with a Department of State e-mail account and store them in a secure repository which allows for search, retrieval, and view when necessary.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
The system stores any and all emails, attachments, and documents that are sent/received over OpenNet and ClassNet. The information included in the emails can include but is not limited to full name, date of birth, SSN, address, and other personnel data. The system was not designed to do anything with the PII that is sent/received through email, and it does not use or disseminate any of the PII that will be stored in it.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
5 U.S.C. 301; 44 U.S.C. 3544.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide: A new SORN for the eRecords System has been drafted and submitted to the Privacy Office for their review.

- 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.
Click here to enter text.

(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 Division 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:

- Schedule number (e.g., (XX-587-XX-XXX)):
  - GRS 6.1, Item 10: DAA-GRS- 2014-0001- 0001 –For Capstone officials.
  - GRS 6.1, Item 11: DAA-GRS- 2014-0001- 0002 – For Non-Capstone officials.
  - N1-GRS-04-5, item 1 – For transitory messages.
- Length of time the information is retained in the system:
  - 25 years after end of tenure for Capstone officials.
  - 7 years from date of email for Non-Capstone officials.
  - 180 days from date of email for transitory.
- Type of information retained in the system:
  Emails sent/received over the Department of State Network

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.
☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?
There is no intentional collection of SSN's. The system is storing emails, attachments and whatever may be included in the body of the emails. The system does not do anything with the information that is sent/received in the emails. Any collection of SSN is the responsibility of the collecting office which is required to have the appropriate authority to collect.

(c) How is the information collected?
The information is collected through emails that are sent/received over OpenNet and ClassNet. Whenever an email is sent or received, the system will store the email along with its attachments. Nothing is done with the contents of the emails or attachments.

(d) 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.
The OpenNet information will be stored in the Amazon Web Services GovCloud as well.

(e) What process is used to determine if the information is accurate?
There is no process in place to determine if the information in the system is accurate. The purpose of the system is not built around accuracy. The purpose of the system is to simply store any and all emails, attachments, and documents that are sent/received over OpenNet and ClassNet.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
The emails that will be stored will be current. There is no way to determine if the PII sent/received within that email is current. The system is not dependent upon whether the information within the email is current or not. The system was designed for the purpose of storing the email, attachments, and documents that are sent/received over OpenNet and ClassNet.

(g) Does the system use information from commercial sources? Is the information publicly available?
No, the system does not use information from commercial sources. The system only stores emails, attachments, and documents that are sent/received over OpenNet and ClassNet. Once the email is sent/received, nothing is done with the information. The emails are simply stored.

(h) Is notice provided to the individual prior to the collection of his or her information?
The opportunity does not exist to provide notice prior to an individual sending an email to the Department. However, the warning banner that appears upon logging into OpenNet and ClassNet will notify individuals of the collection when sending outbound emails. This system can't be accessed without first being logged into OpenNet or

ClassNet. As such, leveraging the banner will be the most effective way of providing notice.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

In accordance with Presidential Memorandum -- Managing Government Records November 28, 2011, any and all emails sent or received over OpenNet will be stored.

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

The primary concern was the security of the information that will be placed in the cloud. The system only collects emails, attachments, and documents that are sent/received over OpenNet. The information within those emails is not used or disseminated. The emails will be stored in the Azure Gov Cloud which has been FedRamp approved for High Impact Systems. This provides superior security than other cloud providers who have not been FedRamp approved for High Impact Systems, therefor providing a more secure housing for the stored emails.

5. Use of information

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

The purpose of the eRecords system is to capture all e-mails and attachments that interact with a Department of State e-mail account and store them in a secure repository which allows for search, retrieval, and view when necessary.

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

Yes, the system is designed to store all of the Department of State emails, attachments, and documents that are sent/received over OpenNet. The system is designed to store these emails for easy access if they are needed in the future.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?
N/A

(2) Does the analysis result in new information?
N/A

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

(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 N/A

6. Sharing of Information

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

The information in eRecords will be available to all offices. Individuals will have the ability to access their own emails but not anyone else's. The Office of the Legal Advisor (L) along with the Bureau of Diplomatic Security (DS) will have the right to flag or view emails they deem necessary in the course of their legislative or investigative duties, respectfully.

(b) What information will be shared?

Email messages including the body and any attachments will be shared.

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

The purpose of sharing information is so that individuals have access to the emails that they have sent or received as well as to aid in various investigations. The sharing of information is strictly limited to those who have been approved for that role. This will allow the appropriate people to access the necessary emails.

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

Individuals will have access to their own sent or received emails through a search function. They will not have the ability to edit or delete these emails. L and DS will have specific access privileges that will allow them to access the system directly and flag or save emails that they feel are necessary. They will not have to make any requests.

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

eRecords is password-protected and under the supervision of the information owner. Access privileges reflect separation of duties and least privilege, and are only extended to those Department personnel who have a need for the records in the performance of their duties.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

The privacy concerns that were identified are as follows:

- Ensuring that eRecords users can only access their own sent and received emails, not those of other users.
- Ensuring that appropriate representatives in L and DS are accessing only the required emails within eRecords.
- The system identifies who is executing various queries. The access controls in place will limit what users have the ability to obtain.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
Individuals will not be allowed to gain access to their information that has been stored within eRecords.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☐Yes ☒No

If yes, explain the procedures.
N/A
If no, explain why not.
Individuals will not be allowed to access eRecords in order to edit anything that they may have sent/received over OpenNet and ClassNet.

(c) By what means are individuals notified of the procedures to correct their information?
There are no means of correcting information that was sent/received over OpenNet.

8. Security Controls

(a) How is 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 a myriad of security controls put into place for the protection of this system that will be enforced on the state side as well as by our cloud provider (Azure).

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.
All Department of State employees will have access to their own sent and received emails within eRecords. Special access privileges will be assigned to those in Legal and DS which will allow them to access all sent and received emails. This will give them the ability to flag emails that they deem necessary. The system owner must approve the individuals to have those special access privileges. From there a system administrator will provide them the appropriate access privileges.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?
Daily system monitoring and auditing takes place by the system administrators to ensure that there is no misuse of the system taking place and verifying that only the appropriate people are accessing the system.

(d) Explain the privacy training provided to authorized users of the system.
All users of the system must take the security awareness training that the Department of State requires upon hire. They are also required to take the training on an annual basis. This training thoroughly addresses privacy procedures that will be followed by the users of the eRecords system. Users are also required to take the course PA459, Protecting Personally Identifiable Information, offered by FSI.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.
To ensure the security of the information within the system, we will do Transport Layer Security encryption. We will also be using Transparent Data Encryption for data at rest.

(f) How were the security measures above influenced by the type of information collected?
Due to the nature of the information in the system, this system has been labeled as a HIGH impact system. Therefore, the appropriate security controls have been put into place at the Department of State as well as Microsoft Azure (cloud provider) to ensure that the information is protected at all times.

9. Data Access

(a) Who has access to data in the system?
All Department of State employees will have access to their own sent and received emails within eRecords. They will not have the ability to view any other users' emails. Select employees within DS and Legal will have the ability to view, flag and save all emails sent or received over the Department of State exchange server.

(b) How is access to data in the system determined?
Access privileges reflect separation of duties and least privilege, and are only extended to those Department personnel who have a need for the records in the performance of their duties. Individuals who are authorized to examine detailed information about the network and system usage of specific users are assigned privileged system accounts for that purpose. When it is determined that an individual no longer requires access his or her account is disabled.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
All users will have access to their own emails within the eRecords system. They will not have the ability to view any other users' emails. Special permissions will be assigned to select users who require special access to the system. Those privileges will be approved by the system owner.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?
Users will only be able to access their own emails within the eRecords system. If a user requires special access to the system they will be required to submit a request to the system owner with a justification as to why they need further access to the system. From there the system owner will review the request and determine if the user in fact needs

further access to the system. Upon approval, the system owner will forward the request to a system admin who will move forward with adjusting that user's access privileges. User access privileges will be audited on a semi-annual basis. This will be done to ensure that all user access privileges are correct and that users who no longer need access to the system have been removed.

Additionally, the use of audit logs is a deterrent to those seeking to misuse data.