PRIVACY IMPACT ASSESSMENT

EMC Avamar – Data Offshoring

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: January 11, 2022
(b) Name of system: EMC Avamar Data Offshoring (DOFF)
(c) System acronym: DOFF
(d) Bureau: IRM
(e) iMatrix Asset ID Number:7603
(f) Child systems (if applicable): N/A
(g) Reason for performing PIA:

☐ New System
☐ Significant modifications 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 purpose of the EMC Avamar Data Off-shoring (DOFF) Deployment Project is to deploy a solution that will enable the Department of State (DoS) to back up post data to a secure remote location, while also providing local backup capabilities. The data offshoring service will allow posts that are evacuated or have a need to restore their data in Washington, D.C. to quickly access their restored data, ensuring continuity of operations.

DOFF is the acronym given to Avamar that is used during the Authority to Operate (ATO) process and is listed as such in the Xacta system. However, for the sake of this document the system will be addressed as Avamar.

Avamar is a system that allows DoS to backup and replicate data from posts in Washington, D.C. The data within the Avamar system are a backup of other systems, each with its own PIA documenting information collection and maintenance processes.

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

The Avamar system contains a backup of the email storage and file level data normally stored in other systems at post. As the system is a backup and recovery system, all post data types are covered. Examples of PII elements that may be collected during the backup of a system include names of individuals, birthdates, email addresses, personal addresses, SSN's, business addresses, and phone numbers. Note that the data collected by Avamar are encrypted and stored in a proprietary format and are un-viewable unless the data are restored (in the event of an emergency or evacuation). Once the data are restored, PII safeguards used at posts (e.g., permissions) will remain in place. Avamar does not store a user's name or state email for authentication purposes.

This applies to both standard users and Avamar administrators. The types of PII listed in the previous paragraph are examples of PII data types that may be replicated in the event Avamar runs a backup at post. Avamar does not collect data or replicate differently from regular users or system administrators. Regardless of the user's access to Avamar, or their affiliation with the system, the data that are backed up remain the same and are determined post to post. Authorized users are administrators at post and System administrators. To run a manual backup, an administrator would need to log on authenticating with the appropriate credentials. The PKI authentication feature was just released in August 2021 to the field. This capability is still being introduced to each post. For this reason, Avamar administrative users at posts that do not have the PKI feature on their instance of Avamar, will need to use username and password to run a manual backup.

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

- 5 U.S.C. 301 (Management of the Department of State)
- 22 U.S.C 2651a (Organization of the Department of State)
- NARA and OMB Managing Government Records Directive (M-12-18)
- Federal Information Security Modernization Act (FISMA) of 2014
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources
- Homeland Security Presidential Directive (HSPD) 7 Critical Infrastructure Identification, Prioritization, and Protection

(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.

The Avamar backup cannot be searched by personal identifiers. Avamar data are indexed by metadata in the backed-up files. There is no way for a user to search or view the information contained within a file. To view a backup, the user must know the file location to access it. Authorized users must open an individual file and can only retrieve data using free text search rather than search by data type or field. Data are restored with rights and permissions in place. Avamar as a system does not qualify as a system of records, therefore, a SORN citation is not required.

(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.)

Description: The primary purpose of Avamar is IT business continuity and disaster recovery – not archival or records retention. The system was never designed for long-term records management. Avamar does have a local and off-site retention policy, which has been set by DOS management and documented in the system's Concept of Operations. Avamar retains onsite backups for sixty days and off-site backups for up to one year. Backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data. If yes provide (Consolidate as much as possible): Below is Avamar's Retention Schedule Provided by Records and Archives

- Schedule number (e.g., (XX-587-XX-XXX)):
  A-07-006-04

- Disposition Authority Number:
  DAA-GRS-2013-0006-0005 (GRS 3.2, item 040)

- Length of time the information is retained in the system:
  Destroyed when superseded by a full backup, or when no longer needed for system restoration, whichever is later

- Type of information retained in the system: Backup files

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?

Avamar cannot recognize or exclude PII at a file-level. Furthermore, Avamar merely backs-up this information, which was already collected by an application that deemed the collection necessary.

(d) How is the PII collected?

Information is collected via an agent that backs up all files on a server or other computing device. Information remains in an unreadable state on the Avamar system. Any PII is collected by the system for which the data is backed up.

(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?

Overall data integrity will be verified via checksums in the Avamar system to ensure backups complete without corruption. If the system identifies corrupted backups, the Avamar system will revert to the last known "good" backup of data. Specific data will not be looked at unless they are part of a restore operation.

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

Information is captured in Avamar as the backup system so that it can be restored either at post or in Washington, D.C. (in the event of a post evacuation). Backups occur on a nightly basis, capturing any changes to the information updated from that day.
Overall data integrity will be verified via checksums in the Avamar system to ensure backups complete without corruption. If the system identifies corrupted backups, the Avamar system will revert to the last known "good" backup of data. Specific data will not be looked at unless it is part of a restore operation.

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

No commercial information, publicly available information, or information from other Federal agency databases is used.

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

Avamar does not analyze data or minimize PII, it simply backs up files. Any data minimization would be completed by the end user at post.

5. Use of information

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

The intended use of the data is for IT disaster recovery purposes. If post were to evacuate or experience any type of data-loss, it could restore its production-level data to a secure location by leveraging local or off-site backups stored via Avamar.

(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 purpose of the system is to back up post data to a secure remote location, while also providing local backup capabilities. The information stored in this system is in line with the stated purpose. There are no collateral uses of this information outside the stated purpose above.

(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.

Avamar does not create test data files. Any test data would have to be introduced by post. If post were to use test data, Avamar cannot differentiate/determine if PII is present in that data.

6. Sharing of PII

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

Internal: PII is not shared internally at the Department.

External: N/A

(b) What information will be shared?

Internal: N/A

External: N/A

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

Internal: N/A

External: N/A

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

Internal: N/A

External: N/A

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

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?

No, information is not collected directly from record subjects and any back up restoration performed by Avamar is a result of an action initiated by post.

(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?

Not applicable. Avamar files are only backups. The opportunity to provide consent was provided at the time of collection by post or the subject.

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

Avamar is intended to back up post data to a secure remote location, while also providing local backup capabilities. As such, individuals cannot petition the system directly for access. Data subjects will contact the original collecting office/bureau/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.

Data collected by the system will be used to reconstitute a post’s data in the event of an evacuation of personnel. Users will have access to their data and can access/update/modify it when systems are back online. Data subjects will contact the original collecting office/bureau/post regarding correcting inaccurate or erroneous information.

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

Individuals are notified by the collecting office/bureau/post that originally collected the information.

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

Information in Avamar is secured through access controls and advanced encryption standards (AES) in accordance with Federal Information Processing Standards (FIPS).

(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).

The following list constitutes the administrative user groups that would be able to restore a backed-up file and access the backend grids of the system. The first two administrative user groups have various levels of admin access to a backup. The last two user groups have access to Avamar's backend grids, also known as the system's "backend". Administrative rights are only provided to the groups below, and that decision is determined by a cleared US direct hire at Post and is contingent on the threat level of that post or region.

None of these categories of Admin users can view the data contained in a backed-up file. When the standard Post user's data are restored to them, they are restored with permissions intact. Lastly, when the replicated data are in the Avamar system, they are in an encrypted and unviewable state to all users below.

Post Avamar Operators-GG: This group will have the right to add new machines, restore backed-up files, run backup jobs, and run restore tasks.

Post Avamar Administrators-GG: This group will have the right to perform out of place restores and restore backed-up files (i.e., restore to a new virtual machine or folder) on OpenNet only.

Access is limited to the original creators and users of the information. Only the storage location is changed. The data are encrypted during the replication in Washington, D.C. There should be no additional risk since the information will not be shared with additional parties. To access Avamar, authorized users/operators first log into OpenNet and then log into Avamar.

Avamar Data Offshoring and Backup Ops Team (EML): Only these domestic Avamar administrative groups have access to Avamar's backend grids and can restore backed-up files.

O365 Team: This team will have temporary access to Avamar grids during the migration of Post data to the cloud. The O365 team cannot run a backup job or restore backed-up files.

(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.

The Avamar system will follow standard system administration procedures that exist at DoS to limit access to the system to those who have a need-to-know. Avamar administrators are also required to use a separate logon and password to access the system to ensure backups run properly and to restore data as needed. Information in the Avamar system remains in an unreadable, unusable state at all times. Information that is restored retains the access levels and permissions of the source system that created the information (e.g., Word, Excel, database, etc.). There will be no change in who has access to the data when implementing the Avamar backup solution.

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

Security Management at Post determines the staff to administer Avamar. Access is only provided to authorized system administrators (i.e., via privileged system administrator accounts) at post who are responsible for monitoring backups. Avamar employs least privilege access through role-based access controls using Active Directory (AD) groups. This applies to every Avamar administrative user group. Again, standard users are not considered because they are more "customers" of Avamar rather than a system stakeholder that can access backup data. All administrative users listed in section 8 (b) have access determined by role-based access controls using Active Directory. The degree of administrative access increases as we move from the "Post Avamar Operators" and move up the chain to the domestic data offshoring and backup ops teams. Administrative access regarding viewing an Avamar backup is granular in this regard.

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

The Avamar system can track updates, changes, deletions, additions, etc. by username as part of the system audits and can be configured to send alerts when changes are made. The Avamar system tracks updates, changes, deletions, and makes additions by username, using the monitoring and safeguarding feature "Auditid," as part of the system's Level-1 hardening capability. Once accounts are created within Avamar, the system will automatically log account creations, system logins and lockouts. The "Auditid" feature meets STIG requirements.

(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. Before being granted access to OpenNet, all users must complete PS800: Cybersecurity Awareness, which contains privacy training and take it annually to retain access. All users are required to complete the mandatory biennial FSI course PA318, Protecting Personally Identifiable Information.