PRIVACY IMPACT ASSESSMENT

Cross Domain Solution

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: March 2022
(b) Name of system: Cross Domain Solution
(c) System acronym: CDS
(d) Bureau: Information Resource Management (IRM)
(e) iMatrix Asset ID Number: 291512
(f) Child systems (if applicable) iMatrix Asset ID Number: N/A
(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):

N/A

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:

Cross Domain Solution (CDS) transfers files that are sent/received from OpenNet to ClassNet and from ClassNet to OpenNet. The CDS is an effort to modernize the Department's cross enclave guard with the ability to move data from the high side (ClassNet) to the low side (OpenNet) systems and vice versa outside of Outlook or any email system. The CDS implementation preserves existing security features and ensures

adequate protection of the otherwise isolated domains. The CDS satisfies system requirements including but not limited to robust content filtering, antivirus, reliable human review, segregated and role-based access to traffic by classified/unclassified systems, and comprehensive audit capability. The CDS also supports Department Messaging Systems Office custom applications with ability to scale to support additional systems with cross domain data transfer requirements in the future.

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

The system transfers all emails, attachments, and documents that are requested for transfer from OpenNet to ClassNet and from ClassNet to OpenNet. The transferred files may include personally identifiable information (PII), but neither the PII nor these files are searchable.

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

5 U.S.C. 301 Departmental regulations
44 U.S.C. 3544 Federal agency responsibilities

(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 information is not searchable in CDS. Administrators or Reliable Human Review (RHR) Operators can only access flagged or rejected files by a globally unique identifier in the system and can retrieve those files when flagged in their queue for review and dissemination. Files that have been flagged for review are stored in a protected folder that only RHR operators and Admins can access. Operators/Admins are alerted to the flagged file(s) via the CDS Dashboard. Once reviewed, the previously flagged files will continue to their intended destination if able to be transferred. CDS provides data transport services but stores no data.

(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 (e.g., (XX-587-XX-XXX)): A-03-003-04

- Disposition Authority Number: DAA-GRS-2013-0005-0004 (GRS 3.1, item 020)

- Length of time the information is retained in the system:

  Temporary. 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: The system keeps a transaction log internally

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?

PII is not collected by CDS. The system only transfers files that may potentially have PII within them.

(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?

There is no process in place to determine if the PII transferred via CDS is accurate. The purpose of the system is to transfer files that are sent/received from OpenNet to ClassNet and from ClassNet to OpenNet. The accuracy of the information is dependent upon the source systems and processes by which the information is obtained.

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

There is no way to determine if the PII sent/received within a file transferred by CDS is current. The purpose of the system is to transfer files that are sent/received from OpenNet to ClassNet and from ClassNet to OpenNet. The currency of the information is dependent upon the source systems and processes by which the information is obtained.

(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 the information publicly available.

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

This was not considered for the CDS system. The purpose of the system is to transfer files that are sent/received from OpenNet to ClassNet and from ClassNet to OpenNet.

5. Use of information

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

CDS does not have any intended use for the PII that may be transferred in files via CDS. The information that passes through CDS is used to support the process of cross domain

data transfer requirements and is ultimately at the discretion of the owner of the information.

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

The purpose of the system is to transfer files that are sent/received from OpenNet to ClassNet and from ClassNet to OpenNet. The files and their contents are not searchable.

(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?
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

(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.

External: No PII is shared.

(b) What information will be shared?

Internal: No PII is shared.

External: No PII is shared.

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

Internal: No PII is shared.

External: No PII is shared.

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

Internal: No PII is shared.

External: No PII is shared.

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

Internal: No PII is shared.

External: No PII is shared.

7. Redress and Notification

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

The CDS system does not directly collect or retain PII from individuals. Notice is provided by the source systems and processes by which the information is originally collected.

(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?

CDS does not interact directly with the record subjects of the PII being transferred by CDS. Consent is obtained at the point of collection for those source systems that process the PII.

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

Record subjects do not have access to their information transferred by CDS. To gain access to their information, records subjects should follow the specific procedures outlined for those source systems and processes that originally collected their information.

(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.

CDS only transfers data from OpenNet to ClassNet and from ClassNet to OpenNet. Records subjects should follow the specific procedures outlined for those source systems and processes that originally collected their information to correct inaccurate or erroneous information.

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

Records subjects are notified of the procedures to correct their information by the source system and/or processes that originally collected their information. The record access procedures are outlined in the System of Records Notices of the source systems and processes that originally collected the information.

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.

(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).

CDS has three roles:

- **CDS Administrator Role**: Creates RHR Operator accounts, grants access to Reliable Human Review (RHR) Operators and can open files that were rejected by the system for transfer from high-to-low and view any potential PII and/or security concerns that may be included within the transferred file if/when necessary.

- **Reliable Human Review (RHR) Operator Role**: RHR operators are granted access to CDS by the CDS administrators. They review high-to-low transfer files that were rejected by CDS. They override rejection of documents that they determine are not classified. Once RHR Operators have deemed that a requested file can proceed with transfer to the intended low-side enclave, only the RHR Operator can override the rejection. The intended recipient navigates to their respective secure file share location to retrieve the file(s) sent.

- **CDS User Role**: Individuals using the CDS transfer service. Users can send-to-self and to other authenticated and credentialed Department of State users along with

being able to retrieve file(s) that have successfully transferred and are awaiting retrieval via the share folder link. The user determines the intended recipient, and the system ensures the files are only accessible to the individual specified. Once delivered, users have 15 days to retrieve the file(s). If the user does not access the file(s) within 15 days, the file(s) are deleted.

(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 only CDS personnel who will be able to access this information are the CDS administrators and the RHR operators. RHR operators are a part of the Tier 2, MSO 2.5 Engineering Team along with Tier 3 MSO-MD Technical Support Team who are responsible for the monitoring and resolution of RHR. CDS Administrators are Tier 3 CDS Engineering Support Team members assigned by the system owner. RHR operator and CDS Administrator roles are granted upon request by a government staff member from the Main State Messaging Center office via the CDS System Engineer. These roles are filled by both contractor and government staff. Users authorized to access an interface to CDS can initiate requests for processing of files and can retrieve only files designated for their receipt from themselves or other authorized users.

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

CDS Administrators are granted access by the CDS Product Owner duty position. The CDS Product Owner is a designated representative of the Director, IRM/OPS/MSO. CDS Administrators have a local console login where they can access rejected files. From there, they can access the Trusted Gateway Service web interface which requires a second login. They have full rights to the system to make configuration changes, apply software updates, create user accounts, etc.

RHR Operators are granted access by the CDS s administrators. RHR Operators also have a local console login which they use to access rejected files. From there, they can access the Trusted Gateway Service web interface which requires a second login.

CDS users can access the system via single sign-on on OpenNet and ClassNet. CDS is available enterprise-wide and does not require an account with the system. CDS users access the interface to request files for processing and to retrieve files from another interface folder designated for their receipt.

(e) What monitoring, recording, auditing safeguards, and other controls 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.

(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 system roles must take the mandatory annual security awareness training, PS800, that the Department of State requires upon hire. All users are also required to take the course PA318, Protecting Personally Identifiable Information, biennially.