PRIVACY IMPACT ASSESSMENT

UiPath Orchestrator PIA

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: December 15, 2021
(b) Name of system: Charleston UiPath Orchestrator
(c) System acronym: UiPath Orchestrator
(d) Bureau: Comptroller and Global Financial Services (CGFS)
(e) iMatrix Asset ID Number: 321223
(f) Child systems (if applicable) and 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):

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:

CGFS requires an unattended Robotic Process Automation (RPA) solution to assist with automation and execution of repetitive and manual processes within the bureau. The UiPath Orchestrator solution will be available Department-wide, but the current specific use is to support the repatriation effort related to the DS-5528 Evacuation Manifest and Promissory Note process.

The UiPath Orchestrator solution allows for the creation, testing, and deployment of these automations throughout CGFS. UiPath provides a central platform that can be used to manage and report on all RPA automations. It exports the PII from the DS-5528 into in a Microsoft Excel spreadsheet in order for it to be loaded and stored in the Global Financial Management System (GFMS) by the Allotment Accounting and Accounts Receivables team within CGFS.

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

The PII used by this system includes full name, social security number (SSN), personal address, passport number, personal phone number, personal email address, place of birth, and sex of DoS employees and family members.

The PII is needed for setting up the recievable transaction within the Global Financial Management System and to manage holds on passports for the Repatriation Loans program efforts related to the DS-5528.

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

22 US Code 2670 - Emergency expenditures

22 CFR § 51.60 - Denial and restriction of passports.

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

☒Yes, provide:

- SORN Name and Number:
  Records of the Domestic Accounts Receivable Tracking System, STATE-23
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  November 18, 1978

- SORN Name and Number:
  Personnel Payroll Records, STATE-30
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  February11, 1998

- SORN Name and Number:
  Global Financial Management System, STATE-73
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  July 15, 2008

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

(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)):
  DAA-GRS-2013-0003

- Disposition Authority Number:
  DAA-GRS-2013-0003-0001

- Length of time the information is retained in the system:
  Records are destroyed 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

- Type of information retained in the system:
  Data from the DS-5528 Evacuee Manifest and Promissory Note form. This includes the following information the U.S. Citizen: full name, SSN, personal address, passport number, personal phone number, personal email address, place of birth, sex, signature.

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?
22 U.S.C. 2651a (Organization of the Department of State)
22 U.S.C. 3921 (Management of service)
5 U.S.C. 301 (Management of the Department of State)
31 U.S.C. 3701-3720A (Claims of the United States Government)

(d) How is the PII collected?

PII is collected via the official DoS form DS-5528 (Evacuation Manifest and Promissory note). The U.S. citizen fills out the form by hand-writing in the information and handing it over to a State Department Consular Officer representative. Once the forms have been collected by a Consular Officer in Consular Affairs (CA), they are sent to the Charleston Financial Service Center (CFSC) where the Accounts Recievable Branch will receive the documents, scan the documents into digital forms, and make the digital forms available in a secure folder via UiPath.

UiPath does not collect the information directly from the individual.

(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?

UiPath cannot determine if the data are accurate, this is accomplished by the Accounts Recievable team within the Bureau of Comptroller and Global Financial Services (CGFS) before it is input into the system. This is done by cross referencing the data with the LexisNexis Consular Affairs database, which contains passport holders' information. Once the data have been validated/confirmed, they are entered into the Global Financial Management (GFMS) System.

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

UiPath does not collect the information directly from the individual. UiPath uses the most recent DS-5528 available to ensure the most current form and information is being used for automations.

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

No, this system currently does not use information from commercial sources or publicly available information.

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

CGFS conducted a thorough review of the DS-5528 promissory note process prior to automating with UiPath. This review follows a full Lean Six Sigma (LSS) process review that includes the identification and analysis on all PII elements thay may be needed for the process. Only required PII elements are used that are necessary to complete the process. In addition, PII is limited to only approved secured folder locations within the DoS network.

5. Use of information

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

The intended use of PII is to support the completion of the DS-5528 promissory note process in UiPath. UiPath automations will act as a pass-through of these data before they are output to a spreadsheet for review. Once reviewed and approved the data are placed in the existing GFMS flat file format and loaded via the GFMS form import process. GFMS is the system of record for all State Department Financial activity.

(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, this system is designed to automate existing DoS processes throughout CGFS. These processes may require the use of PII that is already inherent with the existing procedures. If they do, then this system will interact with these PII elements as an individual would during the automation.

(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: UiPath exports the PII from the DS-5528 into in a Microsoft Excel format. This file is then loaded and stored in the Global Financial Management System (GFMS).

External: PII will not be shared external to DoS.

(b) What information will be shared?

Internal: Data from the DS-5528 Evacuee Manifest and Promissory Note from will be shared. These data include full name, SSN, personal address, passport number, personal phone number, personal email address, place of birth, sex, and signature.

External: N/A

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

Internal: The information on the DS-5528 is shared with GFMS so the receivables, vendor codes, and repayments can be recorded.

External: N/A

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

Internal: UiPath outputs a spreadsheet with the data within the internal on-prem secured folder structure of OpenNet (Microsoft Windows Security management) and then with Global Financial Management System (GFMS) system. Notifications are sent via email to the recipients notifying them that the data are available in these secure locations.

External: N/A

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

Internal: PII is kept within a secured folder structure that ensures only the required parties are able to access it in OpenNet. The PII in DS-5528 is brought in using the existing Form-Import functionality. The data exist on a flat file and are stored in a secure location. The file is then imported into the GFMS system. PII remains encypted and protected in GFMS.

In addition, there are processes in place to properly remove access to secure PII folders when individuals leave the team, or processes are no longer valid.

External: N/A

7. Redress and Notification

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

Yes, the DS-5528 (Evacuee Manifest and Promissory Note) contains a Privacy Act Statement (PAS) that states the legal authority, purpose, routine uses, and disclosure on the document used to collect the information.

(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?
Consent is granted when the individual fills out the form. However, if the form is not filled out, the individual will not be able to be assigned the debt and will be unable to repay.

If no, why are record subjects not allowed to provide consent?

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

Record subjects cannot gain direct access to information in UiPath. Information provided by the individual on form DS-5528 is maintained by Accounts Receivables, and requests regarding recievables are handled via the external site at https://cgfsaccountsreceivablebranch.state.gov/index.htm. Individuals may also follow the procedures outlined in SORNs State-30, State-23, and State-73 to gain access to 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.

Individuals can use the contact information provided on the DS-5528 form to contact CGFS to notify of or request changes to information. In addition, individuals can also use the external site at https://cgfsaccountsreceivablebranch.state.gov/index.htm to contact the Accounts Receivable (AR) team. Lastly, individuals may follow the procedures outlined in SORNs State-30, State-23, and State-73 to correct their information.

If no, explain why not.

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

Individuals are notified of the procedures to correct their information via the original DS-5528 Evacuee Manifest and Promissory Note form and the public-facing site (https://cgfsaccountsreceivablebranch.state.gov/index). SORNs State-30, State-23, and State-73 also provide notice of correction procedures.

8. Security Controls

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

Access to OpenNet, where UiPath resides, is restricted to cleared DoS personnel. In addition, access to data is administered by the CGFS Information System Security Officer (ISSO) and managed within the secure folder and active directory structure of the Microsoft Windows 10 environment. Folders within this environment are granted access to users based on a case-by-case basis by the ISSO.

(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).

- System Administrator - This role will control the setup and management of the server and will be responsible for the systems infrastructure and operation. This role will be executed by a member of the Global Systems Operations department within CGFS. This role does not have access to the PII in this process.
- Security Administrator - This role will manage the security and assignment of roles for all application users. It will be executed by the ISSO. This role does not have access to the PII in this process.
- Instance Owner - This role will control the functional setup and management of all Departmental user groups within Orchestrator. It will manage the modern folders structure and be responsible for the overall management of the application from a functional and RPA Center of excellence perspective. Modern folders is functionality within UiPath Orchestrator that allows folder to be assigned to users separately based on security/access. This allows for different users/departments to have their automations isolated within their own folder structure. It will be executed by the Systems Coordination and Implementation (SCI) Team within CGFS. This role does not have access to the PII in this process.
- Automation Manager - This role will oversee a specific department or group of Bot processes within Orchestrator. For example, an Automation Manager will oversee all bot processes for the Disbursing Office. A single Group Manager may oversee

multiple groups. This role will be executed by the Systems Coordination and Implementation (SCI) team. This role does not have access to the PII in this process.

- Bot User - This role will provide general application functionality to a user within a specified group. This role can be executed by a representative from any CGFS Department. This role will have access to the PII in this process.

(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 following steps are taken to limit system and data access to only individuals with a need to know:

- Access request is sent to the Information System Security Officer (ISSO) within CGFS.
- ISSO reviews the request, and confirms with data-owner that access is needed.
- ISSO grants or denies access based on their review.
- If granted, ISSO adds user credentials in Active Directory to the folder and grants read or write access based on need.
- Once user no longer needs access to this data, the ISSO removes the user from the folder.

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

Access to data is role-based, and granted by the ISSO, with each role only accessing what is absolutely necessary to perform the intended function.

- System Administrator – Has administration rights to establish and maintain the environment
- Security Administrator – Establishes the security and assigns roles for the environment
- Instance Owner – Can create folders, add, and manage automations, has access to all groups
- Automation Manager – Can create folders, add, and manage automations, has access only to a subset of assigned groups
- Bot User – Can execute automations only for a subset of assigned groups

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

PII is not stored in the Charleston based UiPath Orchestrator, as it acts as a passthrough. However, access to the PII data located within the secure windows folder location is granted on a case-by-case, need-only basis. The case-by-case basis will be determined by a request from the Instance Owner, and the requesting CGFS office (e.g. Accounts Receivables) to the Security Administrator Role. This request will state the official need for access to Orchestrator, and the length of time for the required access. In addition, the SQL Server backend will maintain detailed logs of all system operations and automations for auditing purposes.

(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 DoS cleared staff accessing the system will have taken the mandatory PS-800 Cyber Security Awareness course, which has a privacy component, annually and PA-318 Protecting Personally Identifiable Information course biennially. In addition, all users in the CGFS RPA program are trained on best practices and security procedures regarding the use of PII via the ISO 9001:2015 Standard currently implemented within CGFS. ISO 9001 is the Quality Management System currently utilized by CGFS. The training is conducted by tQMS staff within the CGFS/OMA team, and interal audits are conducted with each CGFS office annually.