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: November 2022  
(b) Name of system: GDIT Yatri GSS Support System  
(c) System acronym: Yatri  
(d) Bureau: CA/EX  
(e) iMatrix Asset ID Number: 331364  
(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): 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:  

Yatri is a cloud-based system, owned and operated by General Dynamics Information Technology (GDIT), Inc., that provides consular services supporting the Department of State Global Support Strategy (GSS) contract for visa services and U.S. persons requesting assistance out of the country.
The primary function of Yatri is to facilitate the dissemination of information necessary for non-immigrant and immigrant visa applicants to schedule interviews at post consular locations. Additionally, Yatri, and GDIT support personnel assist U.S. persons out of the country with call center support for information services, document delivery, appointment scheduling and greeter services. Where applicable, Yatri collects consular fees from non-immigrant applicants and coordinates both inbound and outbound courier correspondence between applicants and the consular offices at posts.

In addition to the GSS visa applicant services, Yatri provides features for limited consular personnel to review live service agents call recordings and closed-circuit television (CCTV) recordings captured at GDIT operated Offsite Facilitation Centers (OFC) that provide support to visa applicants only.

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

The following PII is collected on visa applicants and U.S. persons:

<table>
<thead>
<tr>
<th>Data Collected</th>
<th>Non-Immigrant &amp; Immigrant Visa Applicants</th>
<th>U.S. Persons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name (first and last)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Nationality/Citizenship</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Place of Birth</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Gender</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Passport Information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Home Address</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Personal E-mail Address</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>National Identification Number</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Home Phone Number</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Work Phone Number</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Mobile Phone Number</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Delivery Address (if address differs from home address)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Educational Information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Financial Account Information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Personnel/Employment</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Family Information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Medical Information</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Photos</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

It is possible that visa applicants provide U.S. persons PII as part of a sponsor and/or a petitioner role.
(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 22 U.S.C 2651a (Organization of Department of State)
- 22 U.S.C. 211a (Authority to Grant, Issue and Verify Passports)
- 22 U.S.C. 3904 (Functions of the Service)
- 22 U.S.C. 2715 (Procedures regarding major disasters and incidents abroad affecting United States citizens)
- 22 U.S.C. 4802(b) – Responsibilities of the Secretary of State – Overseas Evacuation

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

☒ Yes, provide:

SORN Name and Number: Visa Records, STATE-39.
SORN publication date: November 8, 2021

SORN Name and Number: Overseas Citizens Services Records and Other Overseas Records, STATE-05.
SORN publication date: September 8, 2016

SORN Name and Number: Passport Records, STATE-26.
SORN publication date: March 24, 2015

☐ 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:
  Submitted to NARA
- Disposition Authority Number:
  Pending Approval

- Length of time the information is retained in the system:
  Temporary. Destroy when 2 years old but longer retention up to 7 years is authorized if required for business use. However, per GSS contract requirements, GDIT will maintain GDIT Yatri GSS system information for the life of the contract.

- Type of information retained in the system:
  Visa applicant information and American citizen information. Records providing ancillary support to the operation of CA mission programs and initiatives at posts. Records include, but are not limited to, routine and general correspondence; legal correspondence; public inquiries; consular cash receipts and other accounting records; request for information; status reports; document authentication; information extracted from visa / passport applications and used for issuing visas and passports; assignment and workload management; performance measures; tracking and monitoring of visa application process and all related records.

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?

      Visa applicants and U.S. persons requesting services can access the Yatri public facing website where limited PII (name, address, personal/work phone number, email, service requirement) is collected to create an account. The PII is automatically uploaded into the
system once the applicant clicks “submit”. Additionally, visa applicants and U.S. persons can also provide their PII to create an account in person, through email and/or a recorded voice call to a GDIT GSS call center that supports the post where the information is entered into the system by GDIT support personnel.

(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.

The Yatri system’s information is housed in the FedRAMP certified/authorized Amazon Web Services (AWS) GovCloud High Impact Level environment.

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

To verify the accuracy of the visa applicant data, the visa applicant’s PII is manually cross-referenced with various Department of State forms and other CA source systems. For U.S. persons, it is incumbent on the applicant to provide accurate information to receive the requested information or service. U.S. persons’ information is also validated during the interview and process of delivering the requested service.

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

Yes. It is the responsibility of the individual requesting CA services to ensure that the information provided is current in accordance with the Yatri guidance to complete the requested information. An applicant’s name, gender, date of birth, and passport number, are locked as soon as a paid application fee is associated with the applicant record. Once an applicant has paid, these fields cannot be changed, except for a one-time update to the passport number.

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

No, Yatri does not use information from commercial sources nor is the information publicly available.

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

The PII listed 3d is the minimum necessary to perform the actions required by this system. Concerns about collecting and maintaining PII include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach.
These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function of providing select CA services to U.S. citizens living outside of the U.S. and visa services to immigrant and nonimmigrant applicants. Any requests for additional PII must be approved by CA/EX and added to the contractual required list of “approved/required” PII.

5. Use of information
   (a) What is/are the intended use(s) for the PII?

   The immigrant and non-immigrant PII is used to validate applicants to provide requested services, to facilitate the appointment scheduling process and the consular fee collection required to process visas, and to deliver and return documents.

   The PII collected from out-of-the country U.S. persons is used to assist in providing requested consular services, appointment scheduling services, and information services provided by the GDIT GSS call center service desk staff, greeter-related staff support services and fee collections.

   (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 PII in Yatri supports identifying and validating applicants, the collection of applicant fees, scheduling consular appointments, to return and deliver documents, and to assist U.S. persons with CA-related services while abroad.

   (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: No information is shared internally with other CA or Department of State bureaus or systems.

External: PII is shared with outside partners including partners that facilitate fees and partners that facilitate courier delivery services on behalf of various posts.

(b) What information will be shared?

Internal: N/A

External:

- Partners to facilitate fees: Document delivery and visa-related fee payments are processed using anonymized personal identification number (PIN) that is in random sequence of alpha-numeric characters, which eliminates the need to share PII with the external fee collection partners.
- Courier Services: Only the name, delivery address, and personal or work phone number will be shared externally for visa applicants and U.S. persons to expedite document delivery.

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

Internal: N/A

External:

- Partners to facilitate fees: The Yatri fee collection service is used to process related payments with its fee collection partners.
- Courier Services: Information is shared with various courier service vendors for the purpose of document deliveries to visa applicants and U.S. persons who choose this service.

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

Internal: N/A

External: Data is transmitted to courier partners using encrypted data transfer (Transport Layer Security – TL) and used only to process a given applicant’s return service. The exchange of information with partners to facilitate fees is either in JavaScript Object Notation (JSON) or Comma Separated Values (CSV) format (both encrypted).
(e) What safeguards are in place for each internal or external sharing arrangement?

Internal: N/A

External: Data is encrypted during transmission to fee payment and courier service partners, and at rest, using secure socket layer (SSL) certificates and public key infrastructure (PKI). All vendors that receive, transmit, or process visa applicant PII are required to secure the data. Each vendor is required to verify/confirm that the data in their possession is secured in compliance with their respective contracts annually.

7. Redress and Notification

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

Yes. During the visa applicant account registration process, applicants are required to acknowledge and accept the terms of the Privacy Act Statement (PAS) on the Yatri public facing website in addition to being provided a link to the Department’s privacy policy page. Applicants that call in for services will be read the PAS presented on the Yatri public facing website prior to collection of their information.

The PAS is also available to callers as a pre-recorded Interactive Voice Recording (IVR) option. Additionally, before connecting a caller to the call center, a pre-recording warning instructs the caller that they should only provide full name, personal or work phone number, and email address to the GDIT support personnel.

(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?

Applicants may accept or decline to provide the PII for use within the Yatri public facing website or provide the required information via phone, email, or in-person; however, if they do not wish to provide the PII necessary for a visa application or requesting appointments, they cannot proceed with using Yatri or receiving the requested service.

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

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

Applicants can access their information up to the time of their appointment by authenticating and accessing the system via username/password. This will grant the applicant access to only their PII that they entered into the system and the applicable state
and status of their record. Applicants can provide updates to the information during their appointment.

U.S persons can also follow the record access procedures in SORNs STATE-39, STATE-05 and STATE-26, regarding points of contact to inquire about 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.

The Yatri public facing website provides procedures regarding how to and when changes to information can be made by entering the system. The following applies:

Name, gender, date of birth, and passport number, are locked as soon as a paid application fee is associated with the applicant record. Once an applicant has paid, these fields cannot be changed, except for a one-time update to the passport number. Passport numbers are allowed to change once to support the scenario where the applicant’s original passport is being replaced with a new passport and the new passport does not yet exist. In this scenario, the first passport number entered by the applicant represents the original passport, and the second passport number entered in Yatri represents the new passport. The ability for applicants to enter a second passport number is locked (turned off) one (1) day before the applicant’s appointment, or as soon as the applicant enters a second passport.

Applicants can change their return delivery address information up until a return Air Waybill (AWB) number is generated in Yatri. A return AWB is generated when the mission has finished the adjudication process, and the travel documents are in route back to the applicant. Once the documents are sent back to the applicant the return address fields are locked.

The applicant's contact information (email address and phone number) may be updated until the travel group record is archived.

U.S persons can also follow the record access procedures in SORNs STATE-39, STATE-26 and STATE-05 regarding points of contact for individuals wanting to correct their information.

If no, explain why not.

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

Yatri provides details and procedures on how to correct user information within the online help section/screens. Applicants can also call the GDIT GSS Yatri call centers for
live phone support to correct their information. Lastly, U.S. persons can follow the procedures in SORNs STATE-39, STATE-26 and STATE-05 regarding points of contact for individuals wanting to correct their information. Notice of these procedures is provided to the record subject in the Privacy Act Statement associated with the form utilized for data collection.

8. Security Controls

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

Yatri is hosted in in the AWS GovCloud which complies with the FedRAMP high baseline controls. The government cloud meets the security requirements to host all required PII and allows the GSS program to deploy the controls required as part of the federal high security baseline. Data is encrypted at rest and in transmission, and all relevant access controls have been implemented to ensure that data remain safe, intact, and accessed or edited only by authorized users. All system accounts and access are granted in accordance with established Department of State account management policies.

(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).

Access to the GDIT Yatri GSS system is role-based, and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor.

Department of State Consular employees and contract employees have access by use of the principle of least privilege, based on prescribed roles to conduct required business to support the delivery of visa and American citizen services. External public users consist of applicants who create self-service accounts to request consular services.

(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.

INTERNAL USERS

Department employees and GDIT employees: Yatri employs a robust account management structure to create, modify and issue rights to users. The IT Helpdesk is responsible for the verification and creation of accounts. Requests for new accounts are submitted by the user’s manager to the GSS Support Ticket Tracking System. The System administrator reviews each request and grants the level of access to either Yatri, or the AWS Infrastructure, based on the authority level of the ticket requestor. Additionally, each post has a Coordinator that requests Yatri application access for Department of State consular users. Consular personnel requests for access must be sent by the Contracting Officer Representative (COR) or the Department of State GSS Program Manager. If a ticket’s requestor does not occupy a program position or function
commensurate with the necessary authority-level to request a new user, the ticket is rejected until approval from a resource with the correct authority level is included in the ticket authorization approval trail.

**External users:**

U.S. persons and visa applicants only have access to Yatri via the public facing website. They must create a username and password before they are allowed to enter their personal information into the system. Once registered, users may view and update their personal information up until 24 hours prior to their scheduled consular appointment. Registered users can only see their information. They do not have the ability to view or modify the data of other users or what is in Yatri.

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

Access to data by Department of State and GDIT personnel user roles listed in 8(b) is based on the position, role, and need to perform officially assigned duties as described. Supervisors and the Project Management Office must approve the employee roles, permissions, and access to Yatri based on least privilege and separation of duties. Once government or contractor personnel leave the project, their access to the system is terminated. Access to data is determined on an approved need-to-access/know basis with well-defined roles and permissions as described below.

**Public Applicant Users (U.S. persons and non-US citizen):** Users of this type/role only have access to their own information (only their own PII). These users can only access Yatri from the public-facing websites and can only create an account for their own purpose to request consular services. Public applicant accounts, also known as self-service accounts, do not have a need to access Yatri on a regular and/or predictable basis. For instance, there may be missions with appointment wait times that are 1.5-2 years out. That means an applicant that makes an appointment today may not need to interact with Yatri for another year and half. Additionally, once a visa is issued, it might be valid for 1, 2, 3 or more years, and cases can go dormant over multiple years. Therefore, Yatri will not fully disable self-service user accounts, unless prompted by the applicant.

However, Yatri will invalidate self-service user passwords after one (1) year of inactivity. Once a password is invalidated, the applicant is required to reset their password following a reset code sent to their account’s associated email address.

**Department of State Consular (overseas) and Washington DC-based Users:** Since the Department (CA/Office of the Executive Director (EX)) is the owner of the GSS program and provides oversight to the entirety of the GSS program, these users must be approved by Department of State supervisors and/or CORs.

**GDIT contractor roles:** The Yatri GDIT personnel system users gain access through either primary or secondary access roles. These access roles allow for more granular management of rights/permissions and ensure that each type of user has only access to
the amount of PII commensurate with their given system role and function as specified in the contract. These roles are managed and assigned following the principles of separation of duties and least privilege. As such, every GDIT employee internal role, or administrative role, must have their formal request approved by their manager. All accounts are monitored, both through auditing and routine reviews of users and their level of access. These roles are mission-based/country-specific and are disabled/deleted once upon departure of the individual.

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

Yatri has a built-in logging system that logs all account history within the application and database. The data in these logs include user data (creation, modification, etc.), what sections of the application are accessed by the user, and what actions the user performed while logged in the system.

In the AWS environment, the CloudWatch, CloudTrail (with alerts), and the Security Hub-monitor Yatri infrastructure components can detect behavioral anomalies and suspicious activity to document unintended modification or unauthorized access to the system.

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

☒ Yes ☐ No

The Yatri System Security Plan (SSP) contains the procedures, controls, and responsibilities regarding access to data in the system.

(g) **Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.**

GDIT users that have access to the Yatri application must complete GDIT-provided Privacy and Rules of Behavior training annually to maintain system access.

Department of State Consular users, in accordance with Department of State computer security policies, must take the mandatory security training (PS800 Cyber Security Awareness) required for all Department of State personnel. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially.

The State Department’s standard “Rules of Behavior” regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.