PRIVACY IMPACT ASSESSMENT

CGI Atlas360 GSS

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: July 2022
(b) Name of system: CGI Atlas360 GSS Support System
(c) System acronym: CGI Atlas360 GSS
(d) Bureau: CA/EX/PAS
(e) iMatrix Asset ID Number: 328030
(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:

The CGI Atlas360 GSS system is a cloud-based system managed by the CGI Federal company to deliver Department of State Consular Affairs (CA) Global Support Strategy (GSS) services in a secure and centrally managed manner. The CGI Atlas360 GSS system is an integrated suite of services that provides a cost-efficient, global contact

center network which leverages a fully integrated Platform as a Service (PaaS) to meet the needs of Consular Affairs, posts, visa applicants, and overseas U.S. citizens. The suite of services provided can vary from country to country, such as: information services, appointment services, fee collections, document delivery services, greeters, and providing offsite facilitation centers (OFC) for applicant processing. For example, depending on the services offered at the specific Post and the required service, U.S. persons can establish an account to inquire about a passport issue or come to the post in person where a greeter will meet with them to discuss CA services required. Visa applicant services can consist of appointment scheduling, fee collection for services rendered, onsite greeter services by personnel at the OFC for processing of requests, and document delivery services to applicants.

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

CGI Atlas360 GSS collects the PII below on noncitizens and U.S. persons.

Noncitizen PII (visa applicants):

- Name (first and last)
- Nationality/Citizenship
- Date of birth
- Place of birth
- Passport Information (non-US passport)
- National ID
- Address
- Personal Email address
- Phone numbers (e.g., home, business, and/or cell)
- Medical information
- Financial information

U.S. Citizen/Legal Permanent Resident (Referred as U.S. Persons) PII:

- Name (first and last)
- Address
- Personal Email address
- Home phone
- Mobile phone
- Country of Birth
- Date of Birth
- Gender
- Nationality
- Medical Information
- Financial Information

Business information (CGI Atlas360 support team and CA consular staff):

- Name (first and last name)

- Business email address

(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

Consular Operations and Support Records

- Disposition Authority Number:
  DAA-0059-2020-0017-0002

- 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, CGI will maintain CGI Atlas360 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. Records include, but are not limited to, memorandum of agreements (MOAs); memorandum of understandings (MOUs); routine and general correspondence; legal correspondence; congressional inquiries; legislative referral; public inquiries; validation studies; fraud alerts; fraud detection and national security (FDNS) program; consular cash receipts and other accounting records; request for authorization; authorizations for a no-fee passport; request for information; status reports; accountability data for the issuance of diplomatic and official passports; requirements; surveys; plans; certificates, cards of identity, and registration; document authentication; information extracted from passport applications and used for issuing passports; assignment and workload management; performance measures; notification and access files; misdirected notification documents; tracking and monitoring of visa application process from foreign embassies and/or consulates for official U.S. government travelers; 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 seeking services can access the public-facing page of the CGI Atlas360 GSS system where they are prompted to create an account. The account creation process requires a limited set of PII. Once the account is verified by email response via CGI Atlas360 GSS, users will enter additional information to request the specific consular service. Visa applicants and U.S. persons can also provide information through email and/or a recorded voice call to an Atlas360 GSS call center that supports the post, where the information is entered into the system by CGI Federal 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 information will be housed in the approved Microsoft (MS) Azure Government FedRAMP High Cloud.

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

The PII is reviewed for accuracy during the interview process with the noncitizen visa applicant or the U.S person applying for the consular service. There is not a process to determine if visa applicants or U.S. person data are accurate before an interview. It is incumbent on the applicant to provide accurate information to receive the requested information or service.

Once registered, users with accounts can log in to their account and correct or amend their information for accuracy, until they go in for their appointment. Users who do not have accounts cannot use email or telephone to correct or amend the information they may have provided; but can amend during the interview process.

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

It is the responsibility of the individual requesting CA services to ensure that the information provided remains current in the CGI Atlas360 GSS system.

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

No, the CGI Atlas360 GSS system does not use commercial sources of information, nor is the information publicly available.

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

The PII items listed in Question 3(d) are 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 CGI Atlas360 GSS system to perform the function of providing requested CA services of U.S. persons living out of the country and visa services to immigrant and nonimmigrant applicants. Any requests by a Department of State Consular employee or contractor staff for additional PII data fields to fulfill the mission of providing American services to overseas individuals must be reviewed and approved by CA/Office of the Executive Director (EX) and added to the contractual required list of "approved/required" PII data fields.

5. Use of information

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

The PII is used to identify individuals overseas requiring assistance, and to schedule appointments, acquire fees for consular services, and to deliver documents to individuals requesting services.

(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 collected by the CGI Atlas360 GSS system is specifically designed to support and provide the contracted services for visa applicants such as appointment scheduling, fee collection, greeter, and document delivery services. As for American citizen services, there is no visa-related support; however, the CGI Atlas360 GSS system will collect U.S. persons PII to facilitate information dissemination, appointment scheduling, document delivery and greeter services.

(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 systems.

External: The CGI Atlas360 GSS facilitates the payment of fees for visa applicants with outside partners on behalf of the various Posts supported by the system. These external partners, for payment of fees and delivery services, will not be identified until such time as a country-region specific task order is awarded to CGI. Document delivery services are for visa applicants and American citizen services U.S, persons applicants. Payment services (financial institutions) are for visa applicants only. Once the partnerships have been established with the external payment partners, the visa applicants can select a method of payment using the CGI Atlas360 GSS system.

(b) What information will be shared?

Internal: N/A

External: Information is shared to support the document delivery by external courier services. Only the name, delivery address, and phone number will be shared externally for visa applicants and U.S. persons to expedite document delivery.

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 the visa applicant PII data with the external fee collection partners.

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

Internal: N/A

External: PII is shared with various Courier Service vendors for the purpose of document deliveries to visa applicants and U.S. persons who choose this service.

Visa applicants generally must pay an upfront fee for visa application processing. The CGI Atlas360 GSS fee collection service is required to interface externally to process visa-related payments with its fee collection partners.

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

Internal: N/A

External: The CGI Atlas360 GSS system transmits/discloses PII via Application Programming Interface (API) Gateway calls. The API Gateway is a single unified API entry point that allows external vendors/banks to interface with CGI Atlas360 GSS to provide successful / unsuccessful payment statuses of visa applications and for document delivery / tracking purposes. Data are transmitted to courier partners using encrypted data transfer (Transport Layer Security - TLS) and used only to process a given applicant's return service.

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

Internal: N/A

External: Electronically, the CGI Atlas360 GSS system uses application programming interface (API) token authentications, between system and any vendor, to transmit applicant information and unique secure subscription keys for each vendor. It also utilizes Federal Information Processing Standards (FIPS) 140-2 authentication and encryption of data in transit. CGI Atlas360 GSS also inherits security controls and safeguards from the Azure FedRAMP Cloud system as applicable.

7. Redress and Notification

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

Visa applicants and U.S. persons (registered users/record subjects) must agree to terms and conditions and privacy policy before they can create an account, in addition to being provided a link to State's privacy policy page. Those who do not have an account and who may have provided PII on an unsolicited or incidental basis are informed of the privacy policies via email or call center response, whichever is applicable.

(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 use the CGI Atlas360 GSS system, but if they do not wish to provide the PII necessary for a visa application or requesting American citizen services, they cannot proceed with using the CGI Atlas360 GSS system. The Atlas360 GSS system presents the privacy policy and privacy act statement prior to the creation of an account whereby the applicant must accept the terms of the policies in order to proceed to create an account.

Those who do not have an account and who may have provided PII on an unsolicited or incidental basis are informed of the privacy policies via email or call center response, whichever is applicable.

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

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

Registered applicants, who are the record subjects, can log in to their account and gain access to their information to update or confirm the accuracy of their PII up to the time of their appointment confirmation, after which they can only change their last and first names. If the applicant requires access to their information after their appointment, they may contact the Post via the CGI Atlas360 GSS call center by email or by phone. Applicants who do not have accounts can also contact the CGI Atlas360 GSS call center located at the Post.

Additionally, the published SORNs STATE-39, Visa Records; STATE-05, Overseas Citizen Services Records and Other Overseas Records, and STATE-26, Passport Records, include procedures on how to contact an office or individual for assistance with accessing or inquiring about the existence of records pertaining to the individual.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Registered applicants can log in to their account and correct or amend their information, until the time that they receive an appointment confirmation, after which they can change only their last and first names, by logging into their account. Applicants who do not have accounts can correct or amend the information they may have shared via email or phone call, on an unsolicited or incidental basis, by contacting the CGI Atlas360 GSS call

center. Individuals can also follow the record access procedures in SORNs STATE-39, STATE-05, and STATE-26, which include procedures on how to contact an office for assistance in addressing inaccurate information.

If no, explain why not.

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

The online help and user guide provide the procedures to registered applicants to correct their information. The online help and user guides are not available to individuals who do not have accounts but can call the CGI Atlas360 GSS call centers for live phone support. The Privacy Act Statement provided to the record subjects point to SORNs STATE-39, STATE-05 and STATE-26, which point to the necessary procedures record subjects must follow to correct their information.

8. Security Controls

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

The CGI Atlas360 GSS system complies with FedRAMP High security requirements and controls. The CGI Atlas360 GSS system includes features such as: well-established and secure authentication mechanisms, data encryption, access control, authorization, least privilege authorizations, separation of duties, event monitoring, audit and accountability, isolation, physical security, personnel security, awareness and training, configuration management, system and communications and information integrity, as well as record and field level history tracking. The CGI Atlas360 GSS system implements these features, among others, and inherits FedRAMP High security controls from the Azure for Government High cloud to ensure that data remain safe, intact, and accessed or edited only by authorized users.

(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 CGI Atlas360 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.

CGI Atlas360 GSS roles are defined according to the principle of least privilege. Roles for CGI employees are assigned and approved by CGI Federal management for those who need to access the system in their work capacity for the secure and efficient functioning of the system.

Access for the Department of State Washington DC-based employees must be approved by their supervisor and by the GSS Project Management Office (PMO) or are requested by Contracting Officer Representatives (CORs) via a Department of State email account. CGI task order managers (TOMs) working in concert with State Department overseas staff will determine the authorized consular users of the CGI Atlas360 GSS system and their level of access authorization including role and group membership where applicable.

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

Access to data by Department of State and CGI 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 the CGI Atlas360 GSS system based on least privilege and separation of duties. Once government or contractor personnel leave the project, their access to the CGI Atlas GSS 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 (US citizen 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 CGI Atlas360 GSS system from the public-facing websites and can only create an account for their own purpose to request consular services. Public applicant user's accounts are eventually disabled automatically after 35 days of inactivity.

Administrator-Privileged Users: Internal CGI users who perform administrative tasks and have permissions and access to all information to create/modify/delete records are tightly controlled. Administrator have logon identifications associated with their name that allows for auditing. Once personnel leave the project, their access to CGI Atlas is terminated in accordance with the CGI contract processes addressing release of contractors.

The CGI Atlas360 GSS system is designed and architected in a way that follows least privilege principles and ensures that logical access restrictions are consistently applied to administrator functionality. In addition, CGI Atlas360 GSS manages administrative logical access enforcement using the screening and account management approval

process. CGI administrator job descriptions/functions are clearly defined in functional statements and position descriptions, and critical functions are isolated such that malicious use of granted privileges would require collusion for all but a localized interruption.

CGI Internal Roles (e.g., Task Order Managers, Single Point of Contact Operations Staff, Call Center Agents/Supervisors): These roles are managed and assigned following the principles of separation of duties and least privilege. As such, any CGI Atlas360 GSS members requesting internal role, or administrative role, must have their formal request approved by their manager. In addition, the security team reviews all security access forms that are submitted to the user's supervisor for any access account permissions. 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 the mission is completed.

Department of State Consular (overseas) and Washington DC-based GSS PMO 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.

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

Within the MS Azure GovCloud, the software captures security-related events as part of the auditing process which safeguards the information by tracking changes according to time, date, identities, and changes to existing records. The Security Operations Center team is responsible for taking the appropriate action regarding events reported during auditing to prevent the misuse of the information system. The CGI Atlas360 GSS system incorporates the following events as part of auditing/logging at both the application and system level for the purpose of security compliance:

- Authentication/Login Status (i.e., success, failure)
- Number of Login Attempts
- Password Changes
- Authorization checks and Group (i.e., the team, organization, department, or account from which the activity originated)
- Actor (i.e., the unique identification (UID), username, or API token name of the account responsible for the action)
- Event name (i.e., the standard name for the specific event)
- Description (i.e., application pages)
- When (i.e., the server network time protocol (NTP) synced timestamp)
- Where (i.e., the country of origin, device identification number, or IP address)
- Device Identification (i.e., Mozilla, Internet Explorer, Google Chrome, Safari, etc.)
- Action (i.e., how the object has been altered)
- Action Type (i.e., create, update, or delete)

- Printing (where capable)
- Data files opened and closed
- Changes in user or file access permissions or privileges
- Only Call Center and authorized personnel can access audio files and emails (access is controlled through Role Based Access Controls using the principle of least privilege. Access is audited and monitored to preclude tampering and all files are encrypted in-transit and at rest)

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

☒Yes ☐No

The CGI Atlas360 GSS 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.

CGI contractor personnel and subcontractors accessing the CGI Atlas360 GSS system are required to take privacy and security training at least annually. Training is provided by the respective contractor supporting and accessing CGI Atlast360 GSS Support System.

For Department of State Consular users, in accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is 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.