1. Contact Information

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

2. System Information

(a) Name of system: Consular Launchpad for Enterprise Analytics and Reporting
(b) System acronym: CLEAR
(c) Bureau: Consular Affairs
(d) iMatrix Asset ID Number: 6126
(e) Child systems and iMatrix Asset ID Number (if applicable): N/A
(f) Reason for performing PIA:
   ☐ New system
   ☐ Significant modification to an existing system
   ☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable):

3. Purpose

(a) Describe the purpose of the system.

   The Consular Launchpad for Enterprise Analytics and Reporting (CLEAR) system is a portal that provides a centralized interface for Consular Affairs (CA) dashboards, reports, and ad-hoc reporting and analysis tools. It provides the framework supporting various services for CA users to access consular data extracted from other CA sources such as Consular Consolidated Database, (CCD), Consular Affairs RFID Tracking (CART), Overseas Consular Support Applications Automated Cash Register Systems (ACRS), and the Pre-Immigrant Visa Overseas (IVO) Technology (PIVOT) and systems for additional insight into operations, for decision making, and performance of duties supporting CA functions.

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

   U.S. Persons PII:
   • Names of Individuals
   • Personal Phone Number
• Personal Email Address
• Personal Address
• Full Social Security Number
• Passport Number/Information
• Nationality
• Place of Birth
• Date of Birth
• Educational Information
• Mother’s Maiden Name
• Social Media Account Handles
• Gender
• Race
• Financial Information (Partial credit card numbers and financial institution account numbers)

Non-U.S. Persons PII:
• Names of Individuals
• Personal Address
• Personal Phone Numbers
• Personal Email address
• National ID
• Nationality
• Place of Birth
• Date of Birth
• Educational Information
• Gender
• Social Media Handles
• Business Contact Information (Employer, address, phone number and email)
• Financial Information (Partial credit card numbers and financial institution account numbers)

(c) How is the PII above collected?

The information in the CLEAR system is collected directly from the following CA systems: Consular Consolidated Database (CCD), Consular Affairs RFID Tracking (CART), Overseas Consular Support Applications Automated Cash Register Systems (ACRS), and the Pre-Immigrant Visa Overseas (IVO) Technology (PIVOT) system. The CLEAR system is merely a centralized interface for various systems within the Bureau of Consular Affairs.

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

The information in the CLEAR system is used to generate reports and compile metrics related to consular operations and transactions, such as the processing of visa and passport applications so consular professionals can perform various types of analyses, including fraud detection, resource allocation, and determination of the cost of services.
(e) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

☒ Yes  ☐ No

If no, please explain:

4. Authorities and Records
   (a) What are the specific legal authorities and/or agreements that allow the information to be collected?

• 22 U.S.C &sect; 3927 (Chief of Mission)
• 8 U.S.C. 1101-1537 (Immigration and Nationality Act of 1952, as amended)
• 22 U.S.C. 2656 (Management of foreign affairs)
• 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
• 22 U.S.C. 211a et seq. (Passport application and issuance)
• 22 U.S.C. 2705 (Documentation of citizenship)
• 22 U.S.C. 2651a (Organization of Department of State)
• 26 U.S.C. 6039E (Information Concerning Residence Status)
• Executive Order 9397, November 22, 1943
• Executive Order 13478, November 18, 2008 (amending E.O. 9397)

(b) If the system contains Social Security numbers (SSNs), list the specific legal authorities that permit the collection of Social Security numbers.

• 26 U.S.C. 6039E (Information Concerning Resident Status)
• Executive Order 9397, November 22, 1943
• Executive Order 13478, November 18, 2008 (amending E.O. 9397)

(c) In regular business practice, is the information routinely retrieved by a personal identifier (e.g., name, Social Security number, etc.)?

☒ Yes, please indicate relevant System of Records Notice (SORN) below.

- SORN Name and Number:

  STATE-05 Overseas Citizens Services Records and Other Overseas Records
  09/08/2016
  STATE-26 Passport Records 03/24/2015
  STATE-39 Visa Records 11/08/2021

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

(d) 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.

(e) List the Disposition Authority Number(s) of the records retention schedule(s) submitted to or approved by the National Archives and Records Administration (NARA) for this system?
DispAuthNo : DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)

5. Data Sources, Quality, and Integrity

(a) What categories of individuals below originally provide the PII in the system? Please check all that apply.

☒ Members of the public (U.S. persons which includes U.S. citizens or LPRs)
☐ U.S. government employees/contractor employees
☒ Other (people who are not U.S. citizens or LPRs)

(b) Do the individuals listed in 5(a) provide PII on individuals other than themselves? Please check all that apply.

☐ Members of the public
☐ U.S. government employees/contractor employees
☐ Other
☒ N/A

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

The CLEAR system pulls data from the following source systems (CCD, CART, ACRS, IVO and PIVOT) and relies on those source systems to maintain and supply accurate data. The accuracy of the PII is the responsibility of the source systems.

(d) What steps or procedures are taken to ensure the PII remains current?

PII is updated in the source systems by individuals requesting consular services or when a new application is filed or updated. Updated information for currency is retrieved from the CA source systems and as such it is the responsibility of the source systems to ensure the PII remains current.

(e) Was the minimization of PII in the system considered?

☒ Yes ☐ No

If no, please explain.
(f) Does the system use information, including PII, from commercial sources?

☐ Yes  ☒ No

If yes, please list the commercial sources.

(g) Is the information, including PII, collected from publicly available sources?

☐ Yes  ☒ No

If yes, please list the publicly available sources.

(h) Does the system analyze the PII stored in it?

☒ Yes  ☐ No

If yes:

(1) What types of methods are used to analyze the PII?

The reports from the CLEAR system displays metrics based on category comparisons of trends and averages of information from CA source systems depicting data relationships. The resulting analyses of information is available to Consular personnel displayed in adhoc reports, dashboards, and trend data.

(2) Does the analysis result in new information?

Yes. The reports from the CLEAR display metrics based on a category, comparisons based on trends and averages, and bring together data from different systems to show relationships of the data. The system analyzes and compare stored information, producing trends, averages, and data relationships at a high level for policy and decision-making. No new information is developed about an individual based on the system’s analysis.

(3) Will the new information be placed in the individual’s record?

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

(i) If the system will use test data, will it include real PII?

☐ Yes  ☐ No  ☒ N/A - this system does not use test data
If yes, please provide additional details.

6. Redress and Notification

(a) Explain whether a notice is provided to the record subject at the point of collection of their information.

The information in the CLEAR system is obtained from source CA systems so there is no notice provided within the system. When the information collected by a source system involves PII on U.S. persons, there is a Privacy Act Statement displayed on the form in which the individual is seeking a consular service. It is the responsibility of the source system to provide notice to U.S. persons when collecting PII to provide consular services.

(b) Are opportunities available for record subjects to decline to provide the PII?

☐ Yes ☒ No

If no, please explain why not.

The CLEAR system does not collect information directly from the record subjects. The information in CLEAR is acquired from the source CA systems. Consent is acquired via the source CA systems where the applicant applies for consular services.

(c) Are opportunities available for record subjects to consent to particular uses (other than authorized uses) of PII?

☐ Yes ☒ No

If yes, please explain.

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

The CLEAR system does not collect information directly from record subject nor do record subjects have access to the CLEAR data.

Individuals can follow procedures outlined for the source system where they applied for the specified CA service to gain access to their information. Additionally, SORNs STATE-26, and STATE-05 provide U.S. persons procedures on how to contact an office for assistance to gain access to their information.

(e) Are procedures in place to allow a record subject to correct or amend their information?

No
If yes, explain procedures and how record subjects are notified.

If no, explain why record subjects are not able to correct their information.

Record subjects do not have access to the CLEAR system, nor is data collected by the CLEAR system from record subjects. If corrections are needed, record subjects can make changes to correct information via the source system of origin where the information is captured.

7. Sharing of PII

(a) To what entities (outside of the owning office) will the PII be transmitted? Please identify the recipients of the information.

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

(b) For each of the entities in 7(a), list the PII from 3(b) that will be transmitted.

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

(c) For each of the entities in 7(a), what is the purpose for transmitting the information?

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

(d) For each of the entities in 7(a), list the methods by which the information will be transmitted.

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

(e) For each of the entities in 7(a), what safeguards are in place for each method of internal or external transmission?

<table>
<thead>
<tr>
<th>Internal (Within the Department)</th>
<th>External (Outside of the Department)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

8. Security Controls

(a) How is all of the information in the system secured?
The information in the CLEAR system is secured within the Department's intranet which mitigates risk factors through defense-in-depth layers of security including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring.

The CLEAR system is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institutes of Standards and Technology (NIST 800-53) and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need to perform official duties.

(b) 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.

(c) Below, list the general roles that access the system (e.g., users, managers, developers, administrators, contractors, other). Include what PII is accessed, the procedure for each role to access the data in the system, and how access to the data in the system is determined for each role.

Access to CLEAR is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. Department CLEAR users, system administrators, database administrators, and application security managers have access to CLEAR based on prescribed roles to conduct required business and the sustainment and maintenance of the CLEAR system.

(d) After receiving initial access, describe the steps that are taken for the roles defined above to maintain access.

Accounts are reviewed and validated by the supervisor and local Information System Security Officer (ISSO) for compliance with account management control requirements.

For access to CLEAR, management approval is required; approval is based on position and need to know. The Application Security Manager is responsible for managing the local systems accounts as approved by the supervisor and the business unit data owners. This local responsibility includes establishing, activating, modifying, reviewing, disabling, and removing accounts.
Via the CA Privileged Management (PUM) system, each quarter CACST Government personnel must validate and approve the read-only access to Oracle database accounts/accounts/database privileges for the members of the Enterprise Reporting team, which is the CACST/NSDD contractor team supporting CLEAR. Separately, the Enterprise Reporting team sends reconfirmation emails twice a year to CA recipients of reports to check if the distribution lists are still current and the reports still needed.

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

☒ Yes  ☐ No

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

☒ Yes  ☐ No

(g) **Privacy Related Training Certification**

- Do all OpenNet users of this system take the course PA318 Protecting Personally Identifiable Information biennially?

☒ Yes  ☐ No

- Do all OpenNet users of this system take the course PS800 Cybersecurity Awareness Training annually?

☒ Yes  ☐ No

- Are there any additional privacy related trainings taken by any of the roles identified in 8(c) that has access to PII other than their own for this system?

☐ Yes  ☒ No

If yes, please list the related trainings here: