PRIVACY IMPACT ASSESSMENT

CONSULAR AFFAIRS CRISIS MANAGEMENT SYSTEM

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: August 2022
(b) Name of system: Consular Affairs Crisis Management System
(c) System acronym: CACMS
(d) Bureau: Consular Affairs (CA/CST)
(e) iMatrix Asset ID Number: 329221
(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:

CA Crisis Management System (CACMS) will be used by the Department of State to provide assistance and information to U.S. persons and non-U.S. persons overseas when a crisis occurs. CACMS gives the Department of State user the capability to create and maintain a running log of events associated with the crisis at hand to inform concerned family members, friends, and members of Congress, among others who need to learn the status of the crisis situation and the welfare and whereabouts of particular

individuals. Moreover, CACMS also provides reporting and analytics to inform concerned family members, friends, members of Congress, and others of particular cases as well as analytics to support Department logistics and data driven decision-making.

Additionally, CACMS gives the Department of State user the capability to create and maintain cases to allow consular crisis management and task force staff to conduct welfare calls, identify necessary crisis assistance, identify how to refer individuals to routine consular services without the presence of a Mission in-Country, and identify individuals requiring evacuation or repatriation assistance.

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

U.S. Person PII:

- Name
- Alias Names
- Address
- Gender
- Last known address
- Phone number
- Email address
- Date of Birth
- Place of Birth (Country and City)
- Citizenship
- Proof of Citizenship
- Passport number
- Family information
- Identification (Consular Record of Birth Abroad (CRBA) Birth Registration Number (BRN), US Passport Book/Card Number, Alternate ID Type/Number, Date of Issuance, Date of Expiration)

Non-U.S. Persons PII:

- Name
- Alias Names
- Address
- Gender
- Physical appearance (height, weight, hair color, eye color)
- Last known address
- Phone number
- Email address
- Date of Birth
- Place of Birth (Country and City)
- Citizenship
- Proof of Citizenship
- Preferred language

- Passport number
- National identification (ID)/Alternate ID Type/Information

Contact information of representatives (both U.S. Citizens and non-U.S. Persons) of individuals requesting consular services may be collected: name, address, email, phone, affiliation/and or organization.

Department of State Crisis Caseworker: Name, title, and email.

(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)
- 22U.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)
- 22 U.S.C. 2671(b)(2)(A)(ii) (Emergency expenditures)

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

☒Yes, provide:

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

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

☐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.)

Schedule Number: A-15-001-03 – American Citizens Services Case Files
Disposition Authority Number: N1-059-09-40, item 2

Length of time the information is retained in the system: TEMPORARY. Cut off when case closed/abandoned. Destroy 20 years after cut off or when no longer needed, whichever is later. (Supersedes NARA Job No. NCI-59-77-28, Items 2, 3,4,5,6, 8a, 9a, and 9b and NARA Job No. NCI-84-78-9, items 1,2,3,4, and 5)
Type of information retained in the system:
Case files covering the following citizen services: arrest cases; citizenship issues; death notifications; financial assistance cases; loss of nationality cases; lost and stolen passports; property cases; citizen registrations; and welfare and whereabouts cases. Case level data includes biographic information, case information, and case activity log.

Schedule number: B-09-002-08a, Immigrant Visa Overseas (IVO) System Issuances
Disposition Authority Number: N1-084-09-02, item 8a
Length of time the information is retained in the system: TEMPORARY. Cutoff at end of calendar year when issued. Destroy 5 years after cutoff or when no longer needed, whichever is sooner.
Type of information retained in the system: The IVO system is an electronic case management application designed to track and manage the actions taken during the immigrant visa application and adjudication process at overseas posts. IVO maintains immigrant visa issuance and refusal case record data on local area network databases. The record copies of electronic immigrant visa case records are maintained in the Consular Consolidated Database.

Schedule number: B-09-002-2b: Intermediary Records
Disposition Authority Number: DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)
Length of time the information is retained in the system: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
Type of information retained in the system: Immigrant Visa, Non-immigrant Visa, and Consular Consolidated Database hard copy and electronic input records, including applications, supplemental questionnaires, refusal worksheets and supporting or related documentation and correspondence, relating to persons who have been refused immigrant or nonimmigrant visas (including quasi-refusals), under the following section(s) of law: INA subsections 212(a)(1)(A)(i), (iii), and (iv); (2); (3); (6)(C), (E), and (F); (8); (9)(A) (if alien convicted of an aggravated felony), and (C); and 10(D) and (E); 222(g); Title IV of the Helms-Burton Act (22 USC 6021 et seq.); any cases requiring the Department's opinion code00 (Except quasi-refusal cases under (6)(C)(i)); INA subsection 212(a)(10)(C); Quasi-Refusals under 212(a)(6)(C)(i); 212(a)(9)(B); INA subsection 212(f); and Section 5(a)(1) of the Tom Lantos Block Burmese JADE (Junta's Anti-Democratic Efforts) Act of 2008.

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?

CACMS collects information via a webform on its public facing website from U.S. persons, non-U.S. persons or representatives requesting Consular Affairs services during an overseas crisis. The information from the webform is automatically uploaded into the system once the applicant pushes "submit." Applicants are notified that once the request is completed and submitted, they are indicating consent of the Privacy Act statement and sharing of their PII. Information can also be obtained by the Crisis Caseworkers via phone or email from the individual requiring assistance, or from an affiliate of the individual in a crisis.

(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 CACMS is hosted on the approved Department of State authorized Salesforce service cloud platform.

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

Information is presumed accurate upon completion of the CACMS intake form by the individual requesting assistance during a crisis out of the country. To further validate, checks for accuracy, data and information are checked against information provided, such as passport information and birth certificates. Non-U.S. person information is checked against national identification information provided.

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

CACMS data is kept current via enrollment of the required service requested by the individual. Constant communications are maintained with the individual in crisis or their representative. If the status of an applicant changes during the process of rendering the requested service, the consular crisis management and task force staff are notified by the individual or their representative via the mode of communication (e.g., phone, text, email) that they had identified to update information in CACMS.

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

No. The system does not use commercial information, nor is the information publicly available.

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

The PII listed in 3d are the minimum necessary to perform the actions required by this system. Concerns about collecting and maintain PII include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were assessed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for CACMS to provide the necessary assistance in a crisis.

5. Use of information

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

The PII collected enables CACMS staff to identify and contact U.S. persons and non-U.S. persons requesting consular services during an out of the country crisis. The PII is also used to facilitate and connect U.S. persons and non-U.S. persons with the specific Department of State office to provide the requested service during the crisis.

(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 information collected supports the Department in identifying and contacting U.S. persons and non-U.S. persons requesting consular services during a crisis while out of the country and putting the individuals in touch with the specific Department of State office to assist in providing the service during the crisis.

(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 ☐ N/A

(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: The term "internal sharing" traditionally refers to the sharing of information with the Department of State but external to the owning organization (referred to as "bureau"). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau. With that understanding, information in the CACMS system is shared internally with other CA systems as follows: ConsularOne Applications and Data (CAD); ConsularOne Centralized Services (CCS); Consular Consolidated Database Vital Passport Records Repository (CCD/ViPRR); State Enterprise Identity, Credential, and Access Management (SE-ICAM); and Consular Affairs Cloud Salesforce (CACSF).

CACMS also shares information with the Department of State Office of Management Strategy & Solutions, Center for Analytics (M/SS CfA) and CA's Office of Congressional and Public Affairs (CPA).

External: CACMS information is provided to family members or representatives of the individual.

(b) What information will be shared?

Internal: The information in 3d will be shared with the Consular Affairs systems, the Office of Congressional and Public Services, and the M/SS Center for Analytics addressed in paragraph 6a above.

External: The information in 3d is provided to family members and representatives of the out of country individual in a crisis situation.

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

Internal: Information shared with the systems and entities identified in paragraph 6a to assist in verifying the applicant's information to conduct eligibility and status checks to provide required support and services to U.S. persons and non-U.S. persons out of the country.

The information is shared with the Department of the Office of Management Strategy & Solutions Center for Analytics (M/SS CfA) to conduct analytics to support Department logistics and data driven decision-making. Information is also shared with the Office of Congressional and Public Affairs to provide reports to address Congressional inquiries.

External: Information is shared with family members or representatives of the out of country individual in a crisis to provide updates on the individual and the crisis situation.

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

Internal: CACMS is hosted on the Department of State authorized Consular Affairs Cloud Sales Force service platform in the Federal FedRAMP approved Salesforce Government Cloud Plus. The information shared database to database for CA systems by Department approved secure transmission methods for the handling and transmission of sensitive but unclassified (SBU) information.

The information is transmitted secured via Hypertext Transfer Protocol Secure (HTTPS) encrypted using Secure Socket Layer/ Transport Layer Security (SSL/TLS) to the Center for Analytics and CA's Office of Congressional and Public Affairs.

External: Information provided to family members and representatives are provided via the means in which the U.S. person requested to be sent e.g., email, telephone, etc.

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

Internal: The CACMS system safeguards entail secure protocol connections (Hypertext Transfer Protocol Secure (HTTPS)) which provides secure encryption interfaces. The Department of State security program involves the establishment of strict rules of behavior outlined in the security controls for each major application, including CACMS. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability and data integrity. In addition, Department employees must have a Personal Identity Verification/Personal Identification Number (PIV/PIN), as well as a separate password to access CACMS data.

Safeguards in place for the M/SS CfA include sharing arrangements on the security, use, and transmission of PII. Sensitive information provided by email to CA's Office of Congressional and Public Affairs is encrypted as permitted by internal Department of State policies for handling and transmission of Sensitive But Unclassified information**.**

External: Sensitive information provided by email to family members and representatives is secured in accordance with internal Department of State policies for handling and transmission of Sensitive But Unclassified information**.**

7. Redress and Notification

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

Yes, CACMS provides a Privacy Act statement on the first page of the webform. Individuals providing information via the phone are made aware of the Privacy Act Statement.

(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?
Individuals provide information voluntarily to acquire consular services during a crisis while out of the country. Consent is granted by providing the information via CACMS or other methods such as telephone to acquire out of country services during a crisis. If the information is not provided, the office of Consular Affairs may not be able to provide the required services to individuals in the out of the country crisis situation.

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

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

Individuals cannot access their information once submitted in the system. However, the individual can follow processes outlined in SORNs STATE-05 and STATE-39 to request 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.

Procedures are in place to allow the individual in the crisis to provide updated information to the Task Force via their preferred mode of communication (phone, text, email). Individuals can also follow the redress procedures in SORNs STATE-05 and STATE-39 regarding correcting their information.

If no, explain why not.

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

Notifications to individuals to correct records are provided by the task force caseworker via CACMS (email) or via phone during the adjudication process for the requested service during the out of country crisis. Additionally, individuals can follow processes outlined in SORNs STATE-05 and STATE-39 to request access to their information.

8. Security Controls

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

CACMS is hosted on the Department of State authorized Consular Affairs Salesforce service Cloud platform in the Federal FedRAMP approved Salesforce Government Cloud Plus where risk factors are mitigated using defense in depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information to perform official duties.

Access to CACMS applications is controlled at the application level with additional logical access controls configured in Salesforce that limit user access to data. All user accounts and access must be approved following the account approval process established for CACMS.

In accordance with the Federal Information System Management Act (FISMA), 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. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(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 CACMS 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 crisis management case workers, system security administrators and database administrators have access to the CACMS system via service accounts based on their position. The crisis case workers provide aid in processing intake information to provide services to individuals in a crisis out of the country The system security and database administrators provide CACMS daily maintenance, security, and backup functions of the system.

(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.

Access to CACMS is role-based and restricted according to approved job responsibilities and requires managerial concurrence. Supervisors and local Information System Security Officers (ISSO) determine the access level needed by a user (including managers) to ensure CACMS access correlates to the user's particular job function, manager's approval, and level of clearance.

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

In accordance with Department of State policy, CACMS employs the concept of least privilege for each user by allowing only authorized access to information in the system necessary to accomplish assigned job and tasks as approved by the manager. All roles have been analyzed to determine the specific data set and corresponding functions that will be required in accordance with the person's job and level of security approved by the supervisor and the local ISSO. When a user or service account is added to a particular database role, access is limited to only the data and functions allotted.

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

The Salesforce FedRAMP authorized cloud platform performs audit services on CACMS servers capturing events, logs, access attempts, an all actions, exceeding the Department of State requirements. Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information in CACMS. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures
- Logons after-hours or at unusual times
- Failed attempts to execute programs or access files
- Addition, deletion, or modification of user or program access privileges
- Changes in file access restrictions

The purpose of the audit trail is 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 CACMS Security Plan includes information and procedures regarding access to data in CACMS.

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

All system administrators must take the IA210 System Administrator Cybersecurity Foundations Course which has a privacy component. In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. 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.