

CALS PIA

1. Contact Information

A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

- (a) **Name of system:** Consular Affairs Legal Services
- (b) **Bureau:** Consular Affairs (CA)
- (c) **System Acronym:** CALS
- (d) **iMatrix Asset ID Number:** #5588
- (e) **Reason for performing PIA:**
- New system
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization
- (f) **Explanation of modification (if applicable):** not applicable

3. General Information

- (a) **Does the system have a completed and submitted Security Categorization Form (SCF)?**
Yes No

- (b) **What is the security Assessment and Authorization (A&A) status of the system?**

The Department of State operates CALS in accordance with information security requirements and procedures required by Federal law and policy to ensure that information is appropriately secured. In accordance with the Federal Information Security Management Act (FISMA) of 2002, CALS received a one year Authorization To Operate in December 2014 which will expire in December of 2015.

- (c) **Describe the purpose of the system:**

CALS uses a commercial off the shelf (COTS) product named ProLaw Thomson Elite. CALS software is the case management tool used by the Legal Affairs division of Passport Services. CALS supports CA/CST mission requirements for the Legal Affairs (LA) division (CA/PPT/L/LA) of Passport Services, Office of Legal Affairs and Law Enforcement Liaison (CA/PPT/L). The LA division essentially operates as a small law firm within Passport Services. The attorneys and paralegals handle cases received from a variety of sources including Litigations, Operational Support Requests, and the PPT (Passport Services). The cases managed

by the group include but are not limited to passport, employment, other types of litigation, revocations, and law enforcement holds.

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

The personally identifiable information (PII) elements collected and maintained by the CALS system are:

- Names of Individuals
- Passport numbers
- Birthdates of Individuals
- SSN or other identifying number
- Individual ID number from other sources
- Address/ Phone or similar information
- Email address of an individual(s)
- Images or Biometric IDs
- Substantive individual legal information
- Substantive individual family information, such as emergency contacts, and third party contacts
- Judicial Hearings
- Legal Defense

In general, the PII pertains to U.S. citizens and lawful permanent residents. CALS also contains the PII of individuals claiming U.S. citizenship but who have been found not to be U.S. citizens by the courts. In these instances, the PII pertains to foreign nationals and lawful permanent residents.

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

The following legal authorities authorize the collection of the information maintained by CALS:

- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
- 8 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218, (Passports)
- Executive Order 11295, of August 5, 1966 (Rules Governing the Granting, Issuing, and Verifying of United States Passports)
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 U.S.C. 6039E (Information Concerning Residence Status)

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

Yes No

If yes, provide the following information:

System of Records Number (SORN) Name and Number:

- SORN STATE-26 Passport Records, published March 24, 2015

If a SORN is not required, explain how the information is retrieved without a personal identifier.

The information is retrieved by searching with a personal identifier so a SORN is required.

- (g) **Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?**

Yes ___ No XIf yes, please notify the Privacy Division 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 X**A-13-003-02 Case Management System (CMS) Database**

Description: An on-line electronic information system arranged by last name containing data extracted from case files requiring review and processing by the office. Data, including last and first name, date and place of birth, type of case and other information related to the case, is used by CA/PPT/L/LA to track the life-cycle of each case.

Disposition: TEMPORARY. Delete when active agency use ceases.

DispAuthNo: N1-059-95-6, item 2

A-13-003-03 Chronological Files

Description: Arranged by month and year. Duplicate copies of communications, such as telegrams, airmails, letters and reports, maintained in chronological order by month and used for reference purposes only. The official record copy of the communication is filed elsewhere or by subject or case.

Disposition: Destroy when 1 year old or when no longer needed, whichever is sooner.

DispAuthNo: N1-059-95-6, item 3

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 (local, state, federal U.S. courts; congress; Interpol);

- (b) **If the system contains Social Security Numbers (SSNs), is the collection necessary?**

Yes X No ___

If yes, under what authorization?

- 26 U.S.C. 6039E (Information Concerning Residence Status)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 22 U.S.C. 213 (Application for Passport; Verification by Oath of Initial Passport)
- The Privacy Act of 1974, 5 U.S.C section 552a

(c) How is the information collected?

The State Department's Office of Legal Affairs creates a CALS case record when a State Department official, or a U.S. or foreign official from a non-Department of State organization, initiates a request to Legal Affairs to perform an action regarding an individual's passport. Initiators may be U.S. or foreign law enforcement officials, court systems, or Interpol. The requestor must supply relevant documentation to accompany the request. Legal Affairs attorneys and/ or staffers create a case record and enter the supporting documentation into CALS by either of these methods: 1) the file attachments are uploaded, or 2) the data elements from the supporting documentation are manually added, i.e. typed, directly into CALS.

The supporting documentation may be provided or supplemented by Department of State internal agencies, other U.S. agencies, courts, or law enforcement. The documentation may be derived from many sources including, but not limited to, passport applications, passport records, reports of investigations, court documents and documents filed or produced by or on behalf of plaintiffs. The information may have been created by the individual subject of record and then retained in a U.S. Department of State system. The information may also have been generated by officials in U.S. organizations such as law enforcement agencies or the courts, or foreign or international law enforcement entities, e.g. Interpol. The supporting documentation is transmitted to Legal Affairs via regular mail, email and/or fax.

(d) 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.

(e) What process is used to determine if the information is accurate?

The collected information includes litigation records, passport revocation cases, and law enforcement holds, and as such, the information needs to be accurate. The case records in CALS are regularly reviewed for accuracy and updated by the attorneys and paralegals throughout the case's life cycle. Quality checks are conducted against the submitted and created documentation at every stage of the case lifecycle in order to ensure they are accurate, complete, and current.

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

The Legal Affairs attorneys and paralegals regularly review, update, close or inactivate cases to keep the case record current and accurate. Although cases may be closed or inactive the information can still be accessed, updated, and inactive cases may be reactivated if necessary.

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

Yes, CALS users sometimes access publicly available commercial information such as Lexis-Nexus and incorporate the data into the CALS record. CALS also utilizes publicly available information from the U.S. courts. CALS, however, is not the original source of the information and is not publicly accessible. CALS access is restricted to officials of the Department of State, Office of Legal Affairs.

(h) Is notice provided to the individual prior to the collection of his or her information?

The individual whose PII pertains to the case will be notified by the Bureau of Consular Affairs' Passport Services Directorate, or if appropriate another State Department office regarding the final decision of the case.

Passport Records/ Passport Information

In the case of passport records, a passport applicant is advised of all the relevant privacy impact implications at the time the individual completes and signs the application. The applicant is notified of the following:

- their PII is being collected
- the purpose for which it is required
- the possible uses of the information
- the possibility that the data may be shared with other organizations/ agencies
- how the data is protected from unauthorized/ illicit disclosure
- the potential consequences if the applicant declines to provide the data (e.g. that their passport application may be declined).

When the CALS case record is created and the supporting documentation is entered, the original notifications displayed during the passport application process are sufficient to comply with all applicable government regulations and laws concerning the collection of personally identifiable information.

Furthermore, when an individual completes, signs and submits a passport application, they authorize the U.S. Department of State to utilize the information to adjudicate the passport application in accordance with U.S. law and Department regulations.

CALS records are only created by Legal Affairs staff when: a) a U.S. State Department direct hire employee or other U.S. government official, submits a request to the Office of Legal Affairs to address various related issues regarding an individual's passport, b) an authorized agency official submits a legitimate request to put a "hold" on a passport or execute some other action. Therefore, the individual is not notified that the information has been entered into CALS at the time the action is filed. However, the individual was notified of how the Department may use the personally identifiable information they provide on their passport application. In cases where U.S. government officials or courts submit requests to the Office of Legal Affairs, the individual may or may not be notified depending on the nature of the request. Individuals may be notified that a

passport is restricted or revoked in some cases after litigation. In other cases, an individual's passport may have been restricted or revoked without notification while law enforcement officials attempt to apprehend the subject.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

Yes No

Yes, at the time applicants complete the passport application, they are notified of their option to decline to provide the required information, and they are advised that to do so may cause the passport request to be denied. Passport applicants are also notified of the relevant privacy implications such as how the information may be used and shared with other agencies. Passport applicants are not given the option to selectively consent to or deny specific uses of the information. The passport applicant grants complete consent upon signing the application. The applicant's signature provides the authorization to the U.S. government to use and share the information.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The Office of Legal Affairs utilizes CALs to manage litigation and the resulting caseloads involving the Department. The data and PII pertains to passport records, and any possible actions such as passport issuance, denial, revocation, and holds. The collection and use of the information by Legal Affairs is well within the scope of the Department's responsibilities to issue, revoke, and manage passports of U.S. citizens. The PII is handled in accordance with federal privacy regulations regarding the collection, access, disclosure, and storage of PII.

5. Use of information

(a) The intended use(s) for the information is/are:

The information in CALs is utilized to track litigation, manage case workloads, generate reports, and auto-populate template letters related to litigation issues and legal cases involving the Department of State.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information relates to passport issues, litigation and cases of the Office of Legal Affairs.

(c) Does the system analyze the information stored in it?

Yes No

If yes:

1. What types of methods are used to analyze the information?

CALs users with the proper privileges can create case notes, reports, and generate metrics and statistics using CALs' tools.

2. Does the analysis result in new information?

Case Notes:

Yes, CALs users create new information when they enter case notes into the record.

Metrics and Reports:

Yes, CALs users with the proper privileges can analyze aggregated information and generate metrics and statistics based on attributes such as case status, time spent on a case, and worker caseload. This metric and reporting capability allows the Department to view and report on the work being performed by the Office of Legal Affairs. Metrics and statistics only pertain to the personnel and operations of Legal Affairs, not the individual subjects of the cases.

3. Will the new information be placed in the individual's record?

Case notes:

Yes, case notes become part of the individual's existing record but the notes do not contain PII, although PII is stored in other parts of the CALs' record. Case notes are only accessible to the CALs authorized users, and as such are not shared or disseminated.

Metrics and Reports:

No, metrics and reports can be generated but do not contain PII and do not become part of an individual's case record.

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, the Department will be able to make new determinations because the case notes allow State Department officials to make decisions about the individual's passport status and/ or privileges. Since the purpose of CALs and the mission of the Office of Legal Affairs is to handle passport issues, litigation, and decisions regarding individuals' records related to the department's official responsibilities, the new information generated by case notes is totally justified and falls well within the department's responsibilities for passports and the department's mission.

No, the Department will not make determinations about the individual based on the metrics and reports. The metrics and reports only generate new information based on aggregated statistics and pertain strictly to the office's workload, efficiency, and performance, not to individuals.

6. Sharing of Information**(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.**

The Attorney in the Passport Services Office of Legal Affairs' generates letters and notifications to inform case participants and/ or U.S. authorized government officials of decisions.

Dissemination is restricted to the specific participants and / or U.S. officials of the relevant case.

Recipients and organizations vary from case to case depending on which organization(s) and requestor(s) initiated the action. Information can be shared with the specific participants directly involved in the case or their designated representatives, i.e. the law firm or lawyers representing

the case subject. Information may also be shared within the State Department's Bureaus of Consular Affairs and Diplomatic Security as well as other U.S. government agencies to advise law enforcement of the individual's passport status.

(b) What information will be shared?

The Office of Legal Affairs generates letters, notices, and communications from CALs records to provide information to internal and external recipients regarding developments and decisions during the litigation process. The correspondence may contain, but is not limited to, the subject's full name, address, phone number and case decisions and outcomes.

(c) The purpose for sharing the information is:

Legal Affairs utilizes CALs to track and manage cases and to produce letters, notices and correspondence which may contain case information. The documents may be generated by the CALs system or created manually by an attorney or paralegal that copies some information from CALs and pastes it into a different application. Participants in the litigation process may be the individual whose PII is collected, official representatives of other government agencies, or the courts. Legal Affairs shares the information with the participants of the process in order to advise other parties of the Department's opinions, developments, decisions, and actions.

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

Documents are sent via traditional mail to specific internal or external recipients. The mail is handled in accordance with appropriate measures required by the U.S. government for the transmission of PII. CALs does not transmit any information. It is a standalone system, and the users enter information and drag copies of documents into the case files, but the data and documents do not go anywhere from there.

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

Internal recipients, i.e. within the Department of State, are compelled to comply with U.S. government requirements for the protection and use of PII. These safeguarding requirements include but are not limited to security training and internal Department policy for the handling and transmission of "Sensitive but Unclassified" information. In addition, all Department users are required to attend annual privacy and security awareness training to reinforce safe handling practices.

External recipients, i.e. outside the Department of State, include U.S. government organizations, law enforcement agencies, court systems, public or private organizations, and private individuals or their designated representatives participating in the litigation process. As is the case for internal recipients, external U.S. government agencies and organizations must comply with U.S. government policies regarding the protection of PII and "Sensitive but Unclassified" information. These external government agencies enforce safeguarding, security and training requirements comparable to those of the Department of State to protect PII and "Sensitive but Unclassified" information.

External non-governmental recipients include law firms, lawyers, or designated representatives acting on behalf of the individual in the course of case litigation. In general, such individuals are

bound by professional codes of ethics regarding confidentiality and disclosure. External recipients may also include the individual subject of record.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk: 1) accidental disclosure of information to non-authorized parties, and 2) deliberate disclosure and theft of information regardless of the motivation. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

The Department of State mitigates these risks by enforcing rules and requirements regarding:

- Frequent, regular security training for all personnel regarding information security, including the safe handling and storage of PII, “Sensitive But Unclassified”, and all higher levels of classification;
- Strict access control based on roles and responsibilities, authorization and need-to-know;
- Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

The system contains Privacy Act-covered records. Therefore, notification and redress are the right of record subjects. Procedures for notification and redress are published in the System of Records Notice (SORN) Passport Records (STATE-26), and, and in rules published within 22 CFR 171 Subpart D, Privacy Act Provisions.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes No

If yes, explain the procedures.

Individuals who wish to obtain their records or have them amended must submit a written request as outlined in the SORN STATE-26 Passport Records publication on the Department of State’s Freedom of Information Act (FOIA) website, www.foia.state.gov.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals are provided notice on the procedures to amend their records in STATE-26 Passport Records on the Department of State’s Freedom of Information Act (FOIA) website www.foia.state.gov.

8. Security Controls

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

CALS use is limited to a small group of personnel within the Office of Legal Affairs. It is accessible only by authorized users who are mandated to protect confidentiality and privacy.

Furthermore, the CALS system itself is secured within the Department of State intranet where risk factors are mitigated through the use of multiple layers of security controls including management security, auditing, firewalls, and physical security.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

As a matter of policy, the Department of State Chief Information Officer and Information System Security Officer require certain fundamental procedures for all systems. Potential users are screened and assigned privileges based on their roles, responsibilities and their need-to-know. Specific privileges for a given user are only granted after careful consideration of the user role. There are five types of CALS user roles: Administrator, Alternate Administrator, Default Security, Power Users, and View Only. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

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

CALS audit logs contain the "before" and "after" values when a change/update is made by an end user, the initial stamp of the user who made the change, and the time/date stamp. CALS administrators review the audit logs as necessary and take action if suspicious activity or suspected violations are identified.

(d) Explain the privacy training provided to authorized users of the system.

In accordance with Department of State computer security policies, CALS users are required to complete the Department’s Cyber Security Awareness Training and the Department’s PII Training at least once a year. These Department of State training programs reinforce the obligation of users of any Department of State computer system and those who have access to the data it contains to protect PII through appropriate safeguards to ensure security, privacy and integrity. The Department’s privacy training details a few of the numerous requirements covered under the “Rules of Behavior” related to PII.

Users are prohibited from the following activities:

- Browsing PII records without authorization or for purposes other than those directly connected with their official work-related responsibilities;
- Disclosing PII to others, including other authorized users, unless there is a need to do so in the performance of official duties;
- Removing PII from the workplace unless it is for an approved work-related purpose;
- Storing PII in shared electronic folders or shared network files;
- Storing PII on any computing device not owned by the government;
- Altering or deleting PII unless the action is part of their official duties and responsibilities.

Users are also required to take the following actions:

- Protect access to all media on which PII is processed;
- Store hard-copy PII in locked containers or rooms;
- Safeguard any PII (electronic or hard-copy) which is removed from the workplace in the performance of official duties;
- Protect against eavesdropping on telephones or other conversation when PII is discussed.

These lists are not exhaustive. The Department of State's privacy training courses cover all of the requirements for handling and safeguarding PII information mandated by Department of State policy and Federal regulations.

(e) Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users?

Yes No

(f) How were the security measures above influenced by the type of information collected?

The Department of State has long been concerned with the protection of individuals' personal information in accordance with U.S. government policies. CALS was implemented within the Office of Legal Affairs after careful consideration of the risk to PII information, user roles and the Office's mission to provide legal support during the litigation process. Passport records information and the PII passport records contained therein constitute the substantive portion of the information contained in CALS. In addition, CALS contains additional sensitive information other than passport data, such as case information obtained from court records and law enforcement agencies. Accordingly, Legal Affairs and computer system administrators restricted CALS access to a few individuals (approximately 20 or less) in a single office.

9. Data Access

(a) Who has access to data in the system?

Access to CALS is restricted to cleared Department of State direct hire and contractor employees within Legal Affairs. CALS is only available to approximately 20 users in this single office. The system and database administrators are the only users with direct access to the database for the purpose of performing maintenance. CALS end users utilize the CALS application functionality based on job requirements and roles.

(b) Access to data in the system is determined by:

- Job/ Role (Administrator, Alternate Administrator, Default Security, Power Users, and View Only)
- Need-To-Know
- Security class assigned to the individual.

CALS administrators review the individual's profile and assign access based on the above criteria.

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

Yes No

The Bureau of Consular Affairs' Office of Consular Systems and Technology (CA/CST) adheres to a formal, documented audit and accountability policy that addresses purpose, scope, roles, and responsibilities. In addition, there are documented procedures to facilitate the implementation of the policy and the audit and accountability controls.

CALS accounts are not granted to users in the application. Access to CALS is accomplished using a single sign-on procedure in the user's Windows Active Directory (AD) account. Windows AD manages and documents access, roles, and responsibilities.

In order to add a new CALS user, a CALS Application Administrator adds the new user's Network Login ID to the CALS Professional set up UserID field. The set up UserID must match the Windows Active Directory Network Login ID and the user's email account information in the global directory. If the information in the set up UserID field matches the Windows Network Login ID and email account information, the user will be able to access the CALS application.

(d) Will all users have access to all data in the system or will user access be restricted? Please explain.

There are five types of CALS user roles: Administrator, Alternate Administrator, Default Security, Power Users, and View Only. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

- Administrator – Members of the Administrator security class have full access to the application. They can change system wide preferences, add users, change security class of other users, add, edit and delete content, matters, and events. There are only three members of the Administrator security class within Legal Affairs.
- Alternate Administrator: This user is one step down from the Administrator. They have the same access as that of the Administrator except this user cannot change system wide preferences nor change the security class of another user.
- Power Users – This user is one step down from the Alternate Administrator. They can delete content, matter, and documents.
- Default Security – This is the role granted to regular users. They have the ability to add/change content, add/change matter, add/change documents.
- View Only – These users can only look at existing content. They have no update authority.

(e) What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing. Audit logs are reviewed at the Application, Database, and System level as follows:

Application level: CALs administrators review the application level audit logs as necessary and take the appropriate action if suspicious activity or suspected violations are identified.

Database level: Database administrators review the logs for indications of inappropriate or unusual activity on the CALs database, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

System level: System Administrators review logs for indications of inappropriate or unusual activity on the CALs systems, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.