1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: December 22, 2009

(b) Name of system: International Parent-Child Abduction System

(c) System acronym: IPCA

(d) IT Asset Baseline (ITAB) number: 39 (IPCA)

(e) System description:

The International Parental Child Abduction (IPCA) System tracks information about child abductions, from the initial stage through final resolution by the courts. The application tracks all documents, correspondence, and legal proceedings, and allows journal entries to be tracked by caseworkers.

The Office of Overseas Citizens Services, Children's Issues (CA/OCS/CI) at the Department of State assists parents, attorneys, other government agencies, and foreign governments in the return of abducted children and prevention of future international abductions. The information collected in IPCA is shared by CI with the FBI, Interpol, other federal agencies, and foreign governments as required. The IPCA software is used only by the Office of Children's Issues (CI) within the Bureau of Consular Affairs of the Department of State. CI is responsible for the management and tracking of information related to international abduction and potential abduction cases, including their related subjects, action items, legal proceedings, documents, notes and so forth.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): Annual Assessment

(h) Date of previous PIA (if applicable): November 3, 2008

3. Characterization of the Information

The system:

- ☐ does NOT contain PII.

☒ does contain PII.

a. What elements of PII are collected and maintained by the system?

IPCA maintains information on U.S. citizens, non-U.S. citizens, and U.S. Government employees. IPCA maintains the same information on children and parents involved in an international abduction, regardless of the child's citizenship status. Information pertaining to non-U.S. citizen children who are abducted and believed to be in the United States is maintained in IPCA as well.

Once a case file is opened in IPCA, the following information is collected and maintained in the database:

Department of State Employee (assigned to the case)	• Name • Relevant contact information
Left-Behind-Parent (LBP)	• Name • Date and Place of Birth • Visa information if available • Contact information, relatives • Attorney of Record for the LBP
Taking Parent (TP)	• Name • Date and Place of Birth • Visa information if available • Contact information, specific location (if available), known relatives • Attorney of Record (for TP)
Missing Child	• Name • Date and Place of Birth • Visa information if available • Circumstances of abduction

b. What are the sources of the information?

The sources of the information for the IPCA system include: state and Federal law enforcement agencies, the Department of State caseworkers (inputting information from the LBP), other Department of State bureaus with relevant information to the case (such as passport or visa information), Members of Congress, foreign governments, foreign Central Authorities under the Hague Convention, state and Federal court records and other interested parties with information relevant to locating the missing child, including the left-behind parent and his/her attorney and NGOs (non- profit agencies). Occasionally, information is gathered from foreign court records, foreign government agencies and ministries, and foreign NGOs.

c. How is the information collected?

Information is initially collected from the LBP. Once a case is opened, the information is supplemented with legal documentation from the LBP and/or his attorney, and any additional relevant information from Consular Affairs (passport and visa records). The CA/OCS/CI caseworker then gathers relevant information from law enforcement sources and international databases on the TP and missing child. All data is stored in the IPCA database.

d. Why is the information collected and maintained?

CI is the Central Authority for the United States under the Hague Convention on the Civil Aspects of International Child Abduction. CI's duties under the Convention are to facilitate the location and return of internationally abducted children to their state of habitual residence. The information collected in IPCA is the minimum required to meet the business objectives of the CA/OCS/CI. The information in IPCA is necessary for the maintenance of a central repository of all relevant information gathered in the process of locating the missing child.

e. How will the information be checked for accuracy?

The information in IPCA is checked for accuracy by the caseworker assigned to each case. The caseworker verifies the parent-child relationship and any other family data through various documentation requests (i.e. such as court orders or other legal documents from the LBP and/or attorneys of record). Additionally, CA/OCS/CI reviews appropriate passport and visa records and contacts federal/state law enforcement agencies directly involved, such as Interpol U.S., and the U.S. mission in the country where the child was allegedly abducted.

f. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 22 U.S.C. 1731 – Protection of Naturalized Citizens
- 22 U.S.C. 3904(1) – Functions of Service
- 22 CFR 71.1 – Protection of Americans Abroad
- 18 U.S.C. 1204 – U.S. Federal Law and Parental Child Abduction International Parental Kidnapping Crime Act (IPKCA)
- 42 U.S.C. 5779 (Reporting Requirement) and 42 U.S.C. 5780 (State Requirements) – National Child Search Assistance Act of 1990 (NCSA)
- 18 U.S.C. 1073 – Parental Kidnapping Prevention Act (PKPA), authorizes the issuance of Federal Fugitive Felony Warrants (i.e.: Unlawful Flight to Avoid Prosecution (UFAP))
- 42 U.S.C. 11601 – International Child Abduction Remedies Act (ICARA), implemented the Hague Abduction Convention in the United States in accordance with federal regulations found at 22 CFR 94, International Child Abduction.
- 22 CFR 51.28. (Two Parent Signature Rule), requires that parents or legal guardians execute the U.S. passport application for a child under the age of 16.

g. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The collection of PII by IPCA is the minimum required to satisfy the purposes of the system and the mission of the CA/OCS/CI. CA/OCS/CI requires this personal information to create a comprehensive case file on a missing child, to try and locate that child. IPCA collects and maintains the minimum PII necessary to facilitate the mission of meeting the Department's obligations under the Hague Abduction Convention.

The nature of the PII collected and maintained resulted in a security categorization of "Moderate" for the application. The security categorization establishes a specific set of security controls that are required to be in place before operation of the application system. The controls are subject to rigorous testing, a formal certification and accreditation process,

and authority to operate is authorized by a Senior Agency Official. Moreover, controls are reviewed annually, and accredited every three years or sooner if the Application (System) has implemented major changes to the existing Application (System), as defined by OMB Circular A-130.

Only authorized users with a need to know are granted access to the application. Users are periodically reminded by both the Department and the Bureau of Diplomatic Security of their responsibilities in the protection of the data in the IPCA application.

4. Uses of the Information

a. Describe all uses of the information.

The information in IPCA is used by the CA/OSC/CI employees to manage active abduction cases and maintain a central repository on all documentation relating to an open case.

b. What types of methods are used to analyze the data?

All IPCA Reports are selected and run from the IPCA Reports screen. On this screen, users select the type of report and any report criteria necessary to retrieve the desired information. Such reports would be used to review and document the details of a specific case. Only authorized users, based on the user's role, would have access to these reports.

Routine statistical reports are generated on total counts of abduction/access cases by country for use by OCS management, CI abduction unit, Department principles, and Congress. These reports are available to relevant interested parties, including foreign governments. Data and/or case summaries provided to relevant interested parties would be contingent upon Privacy Act Waiver (PAW) allowing dissemination of case specific data.

c. What new information may be produced?

No new information is produced. IPCA is a case management system only.

d. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

IPCA uses information collected from Members of Congress, foreign governments via Dip Notes, foreign Central Authorities under the Hague Convention, state and Federal court records and other interested parties with information relevant to locating the missing child, including the left-behind parent and his/her attorney and NGOs (non- profit agencies). Occasionally, information is gathered from foreign court records, foreign government agencies and ministries, and foreign NGOs. IPCA uses this information to create a comprehensive case file on a missing child and relevant family members.

e. Is the system a contractor used and owned system?

IPCA is the property of the Bureau of Consular Affairs, Office of Overseas Citizens Services, Children's Issues (CA/OCS/CI), and is owned by the Department of State. The system is not a contractor owned system, but contractors maintain the operations of the system.

f. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Appropriate use is regulated by security controls in place for IPCA. All users are exposed to basic information system security awareness training before authorizing access to the system and an annual refresher course.

All users are authorized to perform only functions commensurate with their IPCA job requirements. In an effort to restrict users to only these required functions, logical access controls are utilized in accordance with the principle of least privilege and the concept of separation of duties. The IPCA does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

5. Retention

a. How long is information retained?

The retention period of data is consistent with established Department of State policies and Guidelines as documented in the Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records. This chapter will have to be referenced for the disposition schedule for an American Citizen record based upon the data and the record/file type.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The utility of the information/data enclosed in the database, about a missing child and international abduction will not extend over the allotted time defined in the Department's Disposition Schedule of Overseas Citizen Services Records, Chapter 15. Moreover, there is low privacy risk as a result of degradation of its information quality over an extended period of time. The remaining risks are mitigated through the controls described in paragraph 10.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The information is only shared within the originating office as necessary to carry out the office's work (CA/OCS/CI).

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

IPCA data is not transmitted to any other system and is available only to authorized users of the application. Authorized users have roles assigned to them specific to their job function. Thus, strong segregation of duties is in place.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Internal sharing occurs only with authorized users who are cleared government employees or contractors with work-related responsibility, specific to the access and use of the

system's data. No other internal disclosures of the information/data within the State Department are made.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

A CI caseworker may share some of the information in IPCA with external law enforcement if necessary to help locate or facilitate the return of a missing child.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

IPCA does not have an automated information exchange with external entities.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The external user community of IPCA is limited to law enforcement agencies which are assisting in the location of missing children. These agencies use the information provided by OCS/CI, but there are no external users of the IPCA system. The uses of the IPCA information by the external entities are in accordance with relevant statutory authority and purpose, such as the National Child Search Assistance Act of 1990 (NCSA) (42 U.S.C. 5779 (Reporting Requirement) and 42 U.S.C. 5780 (State Requirements). The NCSA requires local, state and federal law enforcement agencies, when informed of an abduction, to immediately enter the appropriate data into the National Crime Information Center (NCIC) database without requiring a waiting period. Sharing the information that is necessary to help locate a missing child with relevant law enforcement agencies is listed as a routine use in STATE-05, Overseas Citizen Services Records, last amended May 2, 2008 at 73 FR 24342.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

The information in this system is covered by STATE-05, Overseas Citizen Services Records, last amended May 2, 2008 at 73 FR 24342-24345.

☐ does not constitute a system of records covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Yes, notice provisions of the Privacy Act and the Paperwork Reduction Act do apply to the System.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes**,** the Left Behind Parent may decline to provide the required information. However, such actions would prevent him/her from utilizing the assistance of CA/OCS/CI in locating their

missing child. No notice is provided to the Taking Parent until they are located by law enforcement entities.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Conditional consent is not applicable to the official purpose of IPCA.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Individuals who contact CA/OCS/CI and request their assistance in locating a missing child implicitly consent to the information collection. All information collected about the LBP and missing child is voluntary. Notice is not provided to the TP, until they are located by law enforcement agencies. Once they are located, the TP can contact CA/OCS/CI for redress issues. These notice mechanisms are reasonable and adequate based on the sensitive nature of the information contained in IPCA. Based on the purpose and use of IPCA, it is necessary to obtain the TP's information without their consent in order to quickly and safely locate the missing child.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Department notification procedures dictate that individuals who have reason to believe that the Bureau of Consular Affairs may have security/investigative records pertaining to them should write to the Director, Office of Information Programs and Services, A/ISS/IPS, SA-2, Department of State, Washington, DC 20522–6001. The individual must specify that he/she wishes the Overseas Citizen Security Records to be checked. At a minimum, the individual must include: Name; date and place of birth; current mailing address and zip code; signature; and a brief description of the circumstances, which may have caused the creation of the record.

Record Access and Amendment Procedures: Individuals who wish to gain access to or amend records pertaining to them should write to the Director; Office of Information Programs and Services (address above).

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

There is no risk associated with Notification and Redress as it is a part of the SORN (Overseas Citizen Security Records Number STATE-05).

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access?

Access to the system is limited to authorized Department of State staff having a need for the system in the performance of their official duties. All authorized government users maintain

a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to IPCA requires a unique user account assigned by Consular Affairs.

Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes a rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g., curiosity browsing). Completed applications are also reviewed and approved by the information system security officer (ISSO) prior to assigning the logon. Activity by authorized users is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

b. What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

The system maintains a system log of events for the backend database and operating system as well. Database and system administrators are responsible for reviewing system audit logs. Audit logs are reviewed on a bi-weekly basis.

c. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system, and must complete refresher training yearly in order to retain access.

Every user must attend a security briefing prior to receiving access to Department of State networks and a badge for facility access. This briefing is sponsored by DS/SI/IS, which also includes the Privacy Act of 1974. Users must also take a Departmental information system security briefing and quiz prior to receiving access to a DoS network.

d. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

No such residual risk is anticipated.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

IPCA operates under standard, commercially-available software products residing on a government-operated computing platform not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are employed in IPCA.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No such risk is anticipated. The safeguards are described in paragraph 10 above.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates IPCA in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, IPCA is certified and accredited through October 21, 2010.