



Privacy Impact Assessment (PIA)

**For: International Parental Child Abduction
System (IPCA)**

Version 02.03.00

Last Updated: November 25, 2014

1. Contact Information

Department of State Privacy Coordinator
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

- a. **Date PIA was completed:** November 25, 2014
- b. **Name of system:** International Parental Child Abduction System
- c. **System acronym:** **IPCA**
- d. **IT Asset Baseline (ITAB) number:** # 39
- e. **System description (Briefly describe scope, purpose, and major functions):**

The International Parental Child Abduction (IPCA) System tracks information about international parental 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 application is currently used only by the Office of Children's Issues (CI) within the Bureau of Consular Affairs, and by certain staff with the Bureau of Diplomatic Security's Criminal Investigative Liaison office (DS/CR/CIL) who support Children's Issues, at 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 reauthorization
- g. **Explanation of modification (if applicable):** Triennial Assessment
- h. **Date of previous PIA (if applicable):** December 22, 2009

3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

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

IPCA includes 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.

The sources of the information for the IPCA system include: state and Federal law enforcement agencies, the Department of State caseworkers (inputting information obtained from the Left-Behind Parent (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 abducted child, including the Left-Behind Parent and his/her attorney and Non-Governmental Organizations (NGOs). Occasionally, information is gathered from foreign court records, foreign government agencies and ministries, and foreign NGOs.

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)	<ul style="list-style-type: none"> • Name • Contact information
Left-Behind-Parent (LBP)	<ul style="list-style-type: none"> • Name • Date and Place of Birth • Visa information if available • Contact information, relatives • Attorney of Record for the LBP • SSN • Passport Number
Taking Parent (TP)	<ul style="list-style-type: none"> • Name • Date and Place of Birth • Visa information if available • Contact information, specific location (if available), known relatives • Attorney of Record for TP • SSN • Passport Number
Abducted Child	<ul style="list-style-type: none"> • Name • Date and Place of Birth

	<ul style="list-style-type: none"> • Visa information if available • Circumstances of abduction • Contact information, specific location (if available), relatives • SSN • Passport Number
--	---

b. How is the information collected?

Access to IPCA is restricted to cleared Department of State direct hire employees and contractors. The caseworker collects information from the Left-Behind-Parent and inputs it into the system. The information is collected via face-to-face interviews, submitted documents (for example, applications), and phone or Skype interviews. Once a case is opened, the information is supplemented with legal documentation from the LBP and/or his/her 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. CA/OCS/CI monitors the progress of the case through the court system or the mediation process keeping in mind that the Department's role in IPCA cases is to provide consular assistance as well as to encourage compliance with the Hague Abduction Convention. All data is stored in the IPCA system.

c. Why is the information collected and maintained?

The State Department's Office of Children's Issues (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 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 abducted child and managing the case through all stages to final resolution.

d. 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 documents (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.

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

The following authorities provide for the administration of the program supported by IPCA:

- International Parental Kidnapping Crime Act of 1993(IPKCA), Pub.L. 103–173 , Dec. 2, 1993, 107 Stat. 1998
- National Child Search Assistance Act of 1990 (NCSA); Pub.L. 101–647 , Title XXXVII, Nov. 29, 1990, 104 Stat. 4966
- Parental Kidnapping Prevention Act of 1980 (PKPA), Pub.L. 96–611 , §§ 6 to 10, Dec. 28, 1980, 94 Stat. 3568

- International Child Abduction Remedies Act (ICARA), Pub.L. 100–300 , Apr. 29, 1988, 102 Stat. 437 (implemented the Convention on the Civil Aspects of International Child Abduction, done at The Hague on October 25, 1980, in the United States in accordance with federal regulations found at 22 CFR 94, International Child Abduction.); 42 U.S.C. §§ 11601-11610.
- 42 U.S.C. 5779 (Reporting Requirement) and 42 U.S.C. 5780 (State Requirements) 18 U.S.C. 1073 – Flight to Avoid Prosecution or Giving Testimony.
- 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.

f. 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 CA/OCS/CI. CA/OCS/CI requires this personal information to create a comprehensive case file on an abducted child in order to attempt to locate that child and track the progression of the case. IPCA collects and maintains the minimum PII necessary to facilitate the mission of meeting the Department’s obligations under the Convention on the Civil Aspects of International Child Abduction (Hague Abduction Convention).

In general, the privacy of personal information can be at risk of compromise if the information is accessed by unauthorized users, browsed without authorization, transferred to portable/removable media, or disseminated over unsecure networks. The following table documents the security controls and procedures in place to protect the information.

IPCA Protection and Mitigation Strategies

Potential Risks	Protection or Mitigation Strategy
Unauthorized Access	<p>The IPCA application is restricted to system/ database administrators, and users in the Office of Children’s Issues (CI) and the Criminal Investigative Liaison office who support children’s issues at the Department of State. IPCA is accessed via OpenNet. OpenNet’s security controls include firewalls and Network Intrusion Detection Systems (NIDS) which limit the risk of unauthorized access.</p> <p>Only authorized personnel can gain access to the facility. All employees are issued an APPTIS Swipe Card to enter the facility. An access roster that provides a listing of authorized personnel is posted on the door of the room. Entry to the room is maintained by APPTIS and controlled by a card reader locking devices. Overall physical security of the computer room is consistent with a facility processing data up to SBU.</p> <p>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.</p>
Unauthorized Browsing	<p>IPCA servers monitor events on IPCA, detect attacks, and provide identification of unauthorized use of the system. IPCA servers audit</p>

Potential Risks	Protection or Mitigation Strategy
	<p>user actions and user activity history.</p> <p>At the database level, auditing is turned on and tracks user name, Operating System session username, timestamp, and actions taken on objects. All audit statements are stored in the database archive log file.</p>
<p>Transfer to Portable/ Removable Media</p>	<p>Information system media associated with IPCA (replicated data and backup tapes) is managed and maintained by Data Engineering (DE). Multiple layers of physical protection, user training and access controls are used to protect backup tapes, including marking as specified by the Department and CA. The IPCA backup tapes are marked and kept in an approved Media Storage room located in the Beltsville Information Management Center (BIMC) in Beltsville, Maryland, and the Charleston Data Redundancy Site (CDRS) now located in the Enterprise Services Operations Center East (ESOCE) facility. Tapes are archived for a period of thirty days prior to being recycled, destroyed or sanitized. Access to backup tapes is restricted to the system administrators.</p>
<p>Unauthorized dissemination over unsecure networks</p>	<p>IPCA's only connections are within the Department's secure OpenNet. There are no unsecure connections and IPCA is not internet-facing.</p>

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.

These risk factors are mitigated through the use of Technical, Management, and Operational security controls. See Table 1 - IPCA Protection and Risk Mitigation Strategies. The IPCA application data is protected by multiple layers of security controls including OpenNet security, IPCA application security, Department site physical security and management security.

4. Uses of the Information

a. Describe all uses of the information.

The information in IPCA is used by CA/OCS/CI employees and certain DS/CR/CIL employees who support CI 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? What new information may be produced?

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.

These reports are used to review and document the details of a specific case. Only authorized users, based on the user's role, have access to these reports.

Routine statistical reports are generated on total counts of abduction/access cases by country for use by OCS management, the CI abduction unit, Department principals, and Congress. These reports are available to relevant interested parties, including foreign governments. Data and/or case summaries provided to relevant interested parties are contingent upon existence of a Privacy Act Waiver (PAW) allowing limited dissemination of case specific data. No new information is produced. IPCA is a case management system only.

c. 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 Diplomatic Notes, foreign Central Authorities under the Hague Abduction Convention, state and Federal court records and other interested parties with information relevant to locating the abducted child, including the left-behind parent and his/her attorney and NGOs (non-governmental organizations). Occasionally, information is gathered from U.S. visa records, foreign court records, foreign government agencies and ministries, and foreign NGOs. IPCA uses this information to create a comprehensive case file on an abducted child and relevant family members.

d. Are contractors involved in the uses of the PII?

IPCA is the property of the Bureau of Consular Affairs, Overseas Citizens Services Directorate, Office of Children's Issues (CA/OCS/CI), and is owned by the Department of State. The system is not a contractor owned system, but CA/CST contractors develop, maintain and provide technical support for the system. Contractors within CA/OCS/CI also use IPCA and have access to PII stored within the database.

e. 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 receive information system security awareness training before they are authorized to access the OpenNet system, through which the IPCA database may be accessed. Additionally, an annual refresher course is mandated for all OpenNet users.

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 database does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

Contractors involved in the design, development, and maintenance of IPCA are required to have a Moderate Risk Public Trust access authorization. This includes a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and Homeland Security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of IPCA hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by the Bureau of Diplomatic Security (DS).

At the application level, access to IPCA is controlled by the IPCA database Administrators; however, the Consular Shared Tables (CST) application assists IPCA in its authentication process. Each IPCA user must be identified to OpenNet via a network level login. Once the IPCA user has authorization to access OpenNet, the user must have an application-level login within the IPCA database for validation purposes and to ensure the role based access permissions have been assigned properly. Incorporating the user's name into the User ID format provides direct accountability within IPCA, whereas the authentication to the database is handled by CST.

After a user is properly identified by the IPCA database and authenticated by CST, the user is authorized to perform all functions commensurate within job requirements. However, to ensure that users are restricted to only those required functions, the CST employs logical access controls. These logical access controls are system-based mechanisms. They are used to specify who or what is to have access to a specific system resource and the type of access that is permitted. Given that the CST functions as a consolidated repository for the validation of access to Consular systems, user roles are identified during deployment with Oracle scripts.

Furthermore, CST restricts system access based on pre-defined roles and all IPCA users are granted roles based on their data access needs. These roles are distributed to the OCS/CI office:

Role	Function
IPCA_Admin Staff	This is the IPCA system maintenance role. This role is assigned to system managers. This role does not perform authorizations but is the only role allowing access to certain system parameter screens needed for software upgrades and adjustments.
IPCA_Officer	This is the highest authorizing role. This role has certain functions allowing the ability to review document inventories and usages. This is also the only role that can reactivate a spoiled document number.
IPCA_OMS	This is an authorizing role. All officers other than IPCA Manager are normally assigned this role.

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. The Records Disposition Schedule contains the following information regarding disposition of records related to child abductions:

"A-15-002-02 Child Custody/Abduction Case Files

Description: Cases reflect applications filed for the return of children abducted to countries that are party and not party to the Hague Abduction Convention. Included are requests for assistance in locating children taken by the other parent, legal proceedings, information of available courses of action, monitoring the welfare of a child, information on child custody laws and procedures in the host country, and related correspondence.

Disposition: Transfer to the RSC after the case is deemed closed and no action has taken place for 1 year for transfer to the WNRC (Washington National Records Center). Destroy when 15 years old.

DispAuthNo: N1-059-97-14, item 2"

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 an abducted child and international parental child abduction will not extend over the allotted time defined in the Department's Records Disposition Schedule for Overseas Citizen Services, Chapter 15. The allotted retention time is 15 years. 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 Table 1 - IPCA Protection and Risk Mitigation Strategies and Section 10: Controls on Access.

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 IPCA application is currently used only by the Office of Children's Issues (CI) within the Bureau of Consular Affairs, and by certain staff with the Bureau of Diplomatic Security's Criminal Investigative Liaison office (DS/CR/CIL) who support Children's Issues, at the Department of State. The information is shared within the originating office as necessary to carry out the office's work (CA/OCS/CI). Information is also shared with the Office of the Legal Advisor (L), the Bureau of Diplomatic Security (DS), other offices within the Bureau of Consular Affairs' Overseas Citizen Services Directorate (CA/OCS) and CA leadership as needed. In addition, read-only access to the information (not the IPCA application) is available to post employees and locally-engaged-staff (LES) via the CCD application.

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

IPCA data is available to authorized users via the IPCA application and to State Department employees and locally-engaged-staff (LES) at post via CCD. Authorized users have specific roles assigned to them based on their job functions. 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 as mentioned in Section 6(b). No other internal disclosures of the information/data within the State Department are made. Risks to privacy from internal sharing and disclosure are mitigated by numerous technical, operational, and management security controls implemented as part of the Department's cyber security program. See Table 1 - IPCA Protection and Mitigation Strategies in Section 3(f) for details regarding the protection and risk mitigation measures.

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?

Information stored in IPCA may be shared with external law enforcement, foreign governments, Congress, other federal agencies and non-governmental organizations to help locate or facilitate the return of an abducted child. The information collected in IPCA is also shared with the FBI, Interpol, other federal agencies, and foreign governments as the cases progress and actions or collaboration with other legal and governmental entities become necessary. For example, information regarding the location of abducted children may be shared with the FBI, Interpol or foreign governments. Legal decisions may be shared when appropriate with domestic or foreign organizations.

The uses of the IPCA information by external entities are in accordance with relevant statutory authority and purpose, such as the National Child Search Assistance Act of 1990 (NCSA), specifically, 42 U.S.C. § 5779 (Reporting Requirement) and 42 U.S.C. § 5780 (State Requirements).

b. 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 an abducted child with relevant law enforcement agencies is considered a "routine use" and permitted under those regulations. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

External organizations or persons do not have access to the IPCA application. IPCA does not have any external connections and does not permit an automated information exchange with external entities. Only relevant information is shared externally by other appropriate means, including emails, letters, phone calls, in-person meetings and diplomatic notes. Information is shared with foreign and domestic organizations or individuals which have a need-to-know because they are participants in the process or implementers of the decisions. For example, U.S. domestic and foreign law enforcement organizations need information regarding the whereabouts of parents or abducted children. U.S. domestic and foreign child welfare NGOs or lawyers representing either parent, need information regarding case status and case decisions. Information is provided to these entities by officials acting on behalf of the Department of State via emails, letters, phone calls, in-person meetings or diplomatic notes.

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

External users of IPCA information receive the case information directly from officials acting on behalf of the Department of State. The information is transmitted via emails, letters, phone calls, in-person meetings or diplomatic notes. As such, information could be intercepted, transcribed inaccurately, or misused. However, external users are restricted to organizations or persons participating in the case and with a genuine need-to-know. See the table in section 3f, Protection and Mitigation Strategies. Additionally, emails and diplomatic notes are sent via a secure network.

8. Notice

The IPCA system:

- contains information covered by the Privacy Act.
Provide number and name of each applicable system of records.
STATE-26, Passport Records
[STATE-05, Overseas Citizens Services Records](#)
- does NOT contain information 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 (LBP) may decline to provide the required information. However, such actions would prevent him/her from utilizing the assistance of CA/OCS/CI in locating his/her abducted child. No notice is provided to the Taking Parent (TP) until he/she is 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?

Individuals do not have the right to condition the use of the information that they provide as it does not comport with 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 its assistance in locating an abducted child implicitly consent to the information collection. All information collected about the LBP and the abducted child is voluntary. Notice is not provided to the TP until he/she is located by law enforcement agencies. Once the Taking Parent (TP) is located, he/she may 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 his/her consent in order to quickly and safely locate the abducted 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, Bureau of Administration, A/ISS/IPS, SA-2, Department of State, Washington, DC 20522-6001. The individual must specify that he/she wishes the Overseas Citizen Services 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 generated the records.

Record Access and Amendment Procedures: Individuals who wish to gain access to and/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 included in both System of Records Notices (SORNs) applicable to IPCA (Overseas Citizen Services System of Records Notice, STATE-05 and the Passport Directorate's System of Records Notice, STATE-26).

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to the system is limited to authorized Department of State staff having a need to use 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 the Bureau of Consular Affairs.

Each prospective authorized user must first sign a user access agreement before a user account may be issued. The individual's supervisor must sign the agreement certifying that access is needed for the performance of official duties. The user access agreement includes the 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). 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 privacy orientation or training for the system is provided authorized users?

All IPCA users must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain access, users must complete annual refresher training.

All users must read and accept the Computer Fraud and Abuse Act Notice and the Privacy Act Notice describing the expected use and monitoring of these systems prior to being granted access.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

c. 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.

IPCA does not utilize any technology known to elevate privacy risk. The current IPCA safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

a. What is the security assessment and authorization (A&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 on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act (FISMA) of 2002, the triennial assessment and authorization of this system was completed and an Authorization-To-Operate (ATO) was granted on October 31, 2014. This document was updated as part of the triennial reauthorization of the system.