Privacy Impact Assessment
for the

Automated Threat Prioritization Web Service

DHS/ICE/PIA-028

June 6, 2011

Contact Point
Luke McCormack
Chief Information Officer
U.S. Immigration and Customs Enforcement
(202) 732-3100

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Office of the Chief Information Officer (OCIO), in coordination with the Offices of Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO) within U.S. Immigration and Customs Enforcement (ICE), is developing and implementing the Automated Threat Prioritization (ATP) web service, which is an information technology (IT) tool that uses configurable and scalable search and data sharing capabilities to improve and automate existing IT systems. ATP electronically receives, processes and transmits criminal history information about individuals who are the subjects of a broad range of enforcement actions or whose criminal history is required to be evaluated by law to determine eligibility for a benefit or credential. For example, this service is intended to enhance and support ICE's investigative and enforcement operations by automating criminal history data processing and aid in its prioritization of enforcement actions. ICE is conducting this Privacy Impact Assessment (PIA) because the ATP service will transmit and process Personally Identifiable Information (PII.) This PIA, however, only describes the general functionality of the ATP service and not its implementation.

Overview

Background

Within ICE, agents and officers gather and manually review criminal history information about individuals who are subjects of investigations, criminal aliens being apprehended and removed from the United States, or persons of interest in other law enforcement activities. In some enforcement contexts, ICE uses criminal history information to help prioritize its enforcement actions. In order to expedite the manual review of criminal history information and aid its prioritization of enforcement actions, ICE is implementing the ATP web service that will standardize and automate criminal history information processing activities.

A web service is an IT service developed to provide a behind-the-scenes data processing function and capability. Web services like ATP are not applications or databases and therefore they do not have user interfaces, nor are they searchable by an end user. The web services are connected to information systems (hereafter referred to as "calling systems"), which submit requests to or "call" the web service, thereby triggering the web service's specific function. By its very nature, a web service can be connected to any information system, if authorized. A web service also uses a well-defined set of business rules that govern what information it receives, transmits, and/or processes. A web service has only a limited number of authorized users who can access the web service's back-end maintenance module in order to update these business rules as necessary based on changes in law, regulations or policy.

Automated Threat Prioritization Web Service

ATP is a web service that receives and parses criminal history information about an individual subject, converts raw criminal history records into a more structured and easily comprehensible format, and, if requested by the subscribing agency, calculates and assigns a recommended risk level

determination based on the subject's criminal history. ATP only interfaces with a subscribing agency's calling system. It does not search or retrieve information from the Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC) directly. The calling system provides ATP with criminal history information it has already gathered from NCIC.

The ATP service is initiated by a calling system that submits an electronic request to ATP to parse and evaluate criminal history information (e.g., past arrests, criminal offense codes, convictions, incarcerations, etc.) about a subject. In the request to ATP the calling system provides basic identifying information about the subject such as their name, driver's license number, Alien Registration Number (A-Number), and date of birth, as well as the subject's criminal history record (also known as a "rap sheet"). Once received from the calling system, ATP automatically parses the criminal history record by evaluating text contained in the rap sheet (e.g., NCIC codes,[1] conviction data, sentencing data, etc.) for each offense listed. Based on the severity of the offenses listed in the subject's rap sheet (using the business rules developed by the subscribing agency), ATP can provide to the calling system the parsed criminal history record for the subject and, if requested and authorized, a recommended risk level determination. Because ATP is only interfacing with one calling system at a time, it does not match subjects and criminal history records; it only processes the information received from the calling system.

In the event the subject's criminal history record cannot be parsed by ATP (e.g., due to no criminal history record, missing data, improper formatting, etc.), ATP returns to the calling system the unparsed criminal history record provided in the request, an appropriate error message (if necessary), and/or a "Not Applicable" risk level recommendation. Once the transaction is complete, no data persists in ATP. The calling system functions as the official repository for the information received, transmitted and/or processed via ATP. Further, it is incumbent upon the receiving user via the calling system to review the information returned from ATP and take any further action based on their prescribed and authorized uses of the information.

In order to support the future expanded uses of ATP, ICE developed ATP as a configurable web service that allows subscribing agencies in coordination with ICE to define what information is transmitted between the calling system and ATP. For instance, a new calling system may not have use for receiving the recommended risk level determination from ATP, therefore ATP can be configured to return the parsed criminal history record without the risk level determination. Each new calling system that uses ATP will be reviewed to ensure there is adequate legal authority to share the information received and processed via ATP as well as determine the appropriate protections necessary to safeguard the information. Subscribing agencies and the calling systems that use ATP will be listed in the Appendix to this PIA.

Rules & Requirements of ATP

The following general rules and requirements apply to the subscribing agencies and calling systems that may use ATP:

[1] NCIC codes are four-digit uniform offense classification codes created by the FBI whose literal translations best describe the offense(s) committed.

- Prior to processing any criminal history information via ATP, subscribing agencies will coordinate with ICE to review and establish the appropriate agreements and procedures to govern the subscribing agencies' use of ATP. Subscribing agencies will also ensure any/all agreements related to the use of ATP are properly vetted and approved by their agency.

- Subscribing agencies will ensure their PIAs describe at a minimum their use of ATP, authority to collect criminal history information processed via ATP, the calling system which will connect to ATP, and any sharing of information received from ATP. Subscribing agencies and calling systems that use ATP must also be listed in the Appendix of this PIA.

- As required, subscribing agencies will amend their Privacy Act System of Records Notice(s) (SORN) and other applicable privacy compliance documentation governing their calling system that is intended to use ATP.

- Subscribing agencies will coordinate with ICE to ensure calling systems at a minimum meet and satisfy the security controls and requirements prescribed in DHS Management Directive 4300A, Sensitive Systems Policy Directive.

- Subscribing agencies will ensure their calling system records transactions with ATP (e.g., that a request is submitted, a response is returned, whether a recommended risk determination level is generated, etc.).

- Subscribing agencies must have prior written authorization through a Memorandum of Understanding or other information sharing agreement with the FBI to access and use criminal history information from NCIC. Subscribing agencies will also ensure their calling system records an audit trail associating the end user of the calling system with the NCIC record pulled by the subscribing agency.

- Subscribing agencies must develop their own set of business rules for calculating and assigning recommended risk determination levels that are approved by their agency.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The legal authorities that permit or define the information processed through ATP are the same as those that authorize the operation of the calling system. Subscribing agencies must also have prior written authorization from the FBI to access and use criminal history information before using ATP. Additionally, all subscribing agencies of ATP must develop their own set of business rules for calculating and assigning recommended risk determination levels.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The SORN(s) that govern the collection and use of information processed through ATP is the same as the SORN(s) that govern the calling system.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

No. ICE is currently in the process of conducting the Security Authorization (SA) for ATP. As part of the SA process, the system security plan for ATP will be completed. It is anticipated the SA for ATP will be completed by July 2011 and be valid for three years.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Data processed via ATP does not persist within ATP once the function of the web service is completed, but rather it resides in the calling system. The retention of the data processed by ATP is therefore governed by the records retention schedule of the calling system.

The retention of criminal history information by the subscribing agency is governed by the calling system's retention periods or as otherwise defined in the information sharing agreement between the FBI and the subscribing agency.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The PRA does not apply to ATP because the system is not collecting information directly from the public.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The ATP web service described in this PIA receives, transmits and processes information about individuals who are subjects of a broad range of enforcement actions or whose criminal history is required

to be evaluated by law to determine eligibility for a benefit or credential. Specifically, ATP may receive, transmit and/or process the following categories of information:

- *Subscribing Agency/Requestor Information* – May include name of requestor, name of the calling system, agency, subscribing agency's identifier, and date of request.
- *Biographic Information* – May include the following about subjects of requests: name, date of birth, address, phone number, social security number (SSN), driver's license number, and fingerprint identification number (FIN).
- *Immigration-Related Information* – May include the following about subjects of requests: A-Number, country of citizenship or nationality, immigration status, and green card number.
- *Criminal History Information* – May include the following about subjects of requests: criminal arrests and arrest dispositions, NCIC codes for crimes charged and convicted, FBI Number, and sentencing data.
- *Recommended risk level determinations* – A calculated number (e.g., Level 1, 2, or 3) generated by ATP based on criminal history information received from NCIC via the calling system, which is configurable based on requirements of the subscribing agency. This information may or may not be returned to future calling systems that use ATP as determined by the requirements of each subscribing agency.
- *Audit Information* – Returned at the request of the subscribing agency, and may include the name of the calling system, subscribing agency's identifier, date of request and response, time of request and response, request ID (generated by ATP), and type of criminal history information returned (e.g., arrests, dispositions).

2.2 What are the sources of the information and how is the information collected for the project?

The calling system is the source of information processed through ATP. All requests processed through ATP are initiated by ICE or other subscribing agencies, and the information about the subject provided in the request is generally collected from the subject him or herself. The calling system retrieves the criminal history information from NCIC and submits it to ATP.

The transmission of information to and from ATP occurs via encrypted, direct system connections that use a transport layer security (TLS) protocol. When a request is received, ATP uses standardized business rules (developed by the subscribing agency) to evaluate the rap sheet(s) and parse the criminal history information. Specifically, ATP automatically reads the rap sheet identifying individual criminal charges and the associated dispositions for those charges (also known as "arrest cycles"). ATP then converts the rap sheet by arrest cycle into a more structured and easily comprehensible format, which is then returned to the calling system.

Additionally, when a request is submitted by a subscribing agency, the web service captures the subscribing agency's identifier, embeds the name of the calling system in the request message, and generates a request ID (i.e., transaction ID). The subscribing agency's identifier and request ID allow ATP to tie together the request from the subscribing agency and the results generated by ATP. Using the name of the calling system, the response is returned to the appropriate calling system.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. ATP does not use information from commercial sources or publicly available datasets.

2.4 Discuss how accuracy of the data is ensured.

Subscribing agencies may use various techniques and methods to gather information about individuals (e.g., searching various databases, commercial sources, open source data, etc.) who are the subject of requests sent to ATP. Depending on the circumstances, the means of collecting the subject's data may involve direct collection from the subject him or herself or from other reliable data sources. Each subscribing agencies' collection methods and sources will raise different accuracy issues, which will be addressed in their PIAs describing the use of ATP.

Generally, criminal history information received by ATP will be reviewed by federal law enforcement personnel who understand that the data may not be accurate, complete and timely; therefore those individuals will use their training and experience to validate the accuracy of that data using information gathered from other sources. Individuals may also request access to and seek amendment of their criminal history record from the FBI (as described in Questions 7.1 and 7.2), which helps ensure the accuracy of the criminal history information obtained from NCIC.

In addition, the information transmitted between the calling system and ATP is sent via a secure, encrypted direct system interconnection which minimizes the risk of data alteration or modification when in transit and increases consistency of the data used. Technical mechanisms (as described in Question 2.2) are also employed to ensure information submitted to and processed by ATP is properly returned to the correct calling system.

Finally, the end users (i.e., requestors from subscribing agencies) do not have access to the back-end maintenance module that governs the processing of information via ATP. By not granting end users such access, ICE is able to further maintain the accuracy and integrity of ATP.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk of the over-collection of PII.

Mitigation: This is mitigated by several factors including: data processed via ATP does not persist in the web service, that ATP receives and processes only information provided by the subscribing agencies and does not search any other systems, the ability to configure ATP to return specified information to the subscribing agency, and the review and establishment of agreements and system connections based on the authority to collect and share the information processed via ATP.

Privacy Risk: There is a privacy risk of gathering and associating criminal history information that is inaccurate or incomplete with an individual, or associating the wrong individual with a criminal history record.

Mitigation: This risk is partially mitigated by the fact that individuals may request access to and correction of their criminal history record in NCIC under the Privacy Act. This risk is also mitigated by the fact that ATP only interfaces with one calling system at a time. It does not match subjects and criminal history records; it only processes the information received from the calling system. It is incumbent upon the subscribing agencies to provide the associated criminal history information for the subject of a request.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

ATP uses information from the calling system (requestor, biographic, and criminal history information) to:

- Parse criminal history information about an individual subject;
- Convert raw criminal history records into a more structured and easily comprehensible format; and
- Calculate and assign a recommended risk level determination based on the subject's criminal history (if requested by the subscribing agency).

ATP uses requestor information (e.g., name of the calling system and subscribing agency identifier) to ensure information received and processed by the web service in response to a request is returned to the correct calling system. ATP also uses biographic (e.g., name, date of birth, FIN) and immigration-related (e.g., A-number) information provided by the requestor to confirm the identity of the subject and ensure the parsed criminal history information remains properly associated with the subject. ATP then uses the criminal history information received in the request (e.g., NCIC codes, sentencing data, etc.) to automatically calculate a recommended risk level determination, which can be returned to the subscribing agency as requested and authorized. ATP also generates Audit Information that can be returned to the calling system (if requested by the subscribing agency) and used to account for disclosures

to external entities as well as to support auditing functionality/activities across systems, as necessary (e.g., security violations, etc.).

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No. ATP does not use technology to conduct electronic searches, queries or analysis to discover or locate a predictive pattern or an anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No. ATP does not have outward-facing user interfaces. Internally, only certain authorized ICE employees can access the maintenance module for ATP in order to update the business rules that govern the operation and processing of information by ATP.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that PII will be accessed by unauthorized individuals or for unauthorized purposes.

Mitigation: This is mitigated by the review and establishment of agreements and system connections based upon the subscribing agency's authority to collect information processed and transmitted via ATP. Subscribing agencies must also have prior written authorization from the FBI to access and use criminal history information before using ATP. It is also incumbent upon the subscribing agency to define and govern the users of their calling system to ensure proper authorization and access to the information returned from ATP. Additionally, ATP does not have front-end user interfaces and therefore does not open any new avenues of access to the information received and processed by ATP.

Privacy Risk: There is a risk that the underlying criminal history information submitted to ATP may be inaccurate, which could result in the assignment of an incorrect recommended risk determination level to a subject of a request.

Mitigation: This risk is mitigated by the fact that ATP uses the criminal history information provided by the subscribing agency in the request. It is incumbent upon the subscribing agency to ensure the criminal history information pulled from NCIC and submitted as part of the request to ATP pertains to the subject of the request. This risk is also mitigated by leveraging the knowledge and experience of the subscribing agency personnel (i.e., requestors) who are trained to exercise experience, discretion and judgment, when reviewing and cross checking the information provided to and returned from ATP.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Notice of the ATP service is provided by this PIA. Additionally, subscribing agencies will provide notice by ensuring their PIAs describe their calling system that will use ATP, the purpose(s) for using ATP, and any sharing of information received or processed via ATP. Subscribing agencies will also publish updates to their respective privacy compliance documentation (e.g., SORNs), as necessary.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

For law enforcement reasons, the opportunities for individuals to consent to uses, decline to provide information, or opt out of this project are limited or nonexistent.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk individuals may not be aware their information is processed and transmitted via ATP.

Mitigation: The risk is mitigated primarily by the public notice provided through this PIA. Individuals may also be notified by the subscribing agency at the point of collection of the original data that their information may be shared for criminal justice and law enforcement purposes. Additional notice may be limited or nonexistent because providing such notice could compromise the underlying enforcement purpose of the subscribing agency and may put ongoing investigations at risk.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Data processed via ATP does not persist there once the function of the web service is completed. The retention of the data is governed by the records retention schedule of the original calling system.

Subscribing agencies retain criminal history information consistent with the retention periods for the calling system or as otherwise defined in the information sharing agreement between the FBI and the subscribing agency.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There are no privacy risks related to retention of data in ATP because data processed via the web service does not persist there once the function of ATP is completed. The retention of the data is governed by the records retention schedule of the original calling system.

Mitigation: Because ATP does not have user interfaces and is used to process and transmit information from calling systems, ICE determined there was no need to retain the data in ATP upon completion of its function thereby eliminating any privacy risks related to retention. Also by not retaining the data in the web service the privacy risks of over-collection and data minimization are further reduced.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The extent of external sharing via ATP is limited to ATP's receipt and return of information provided by subscribing agencies in requests submitted to ATP. ATP returns the same Biographic and criminal history information received in the initial request from the calling system to the requestor. As requested and authorized, ATP may also share with the subscribing agencies a recommended risk level determination about the subject of a request via secure, direct system connections with the calling system. Additionally, ATP has the ability to return Audit Information to the calling system in order to support auditing functionality/activities across systems, as necessary (e.g., security violations, etc.).

As described in Question 2.2, the transmission of information to and from ATP occurs via encrypted, direct system connections that use a TLS protocol to ensure the proper safeguarding of information processed through ATP. Other technical features are also implemented to ensure information processed via ATP is returned to the appropriate calling system.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The sharing of information via ATP is compatible with the original purpose(s) for which the information is collected by the subscribing agencies' calling systems that use this web service. All

external sharing falls within the scope of published routine uses defined in the SORNs governing the subscribing agencies' calling systems that use ATP.

6.3 Does the project place limitations on re-dissemination?

Typically there are no limitations on re-dissemination of the information processed via ATP. Any further sharing and re-dissemination of this information is permitted as authorized by the subscribing agencies' SORN(s).

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

ATP does not maintain a record of the disclosures outside of DHS. Because ATP is a web service, it does not store data and no disclosure is occurring. It is the responsibility of the subscribing agency to maintain an accounting of any disclosures to external entities. While the request and response transmitted between the calling system and ATP inherently reflects a disclosure (i.e., the subscribing agency will know when a request is submitted to ATP and when a response is received), it is unknown how and whether other subscribing agencies have audit mechanisms in place to automatically account for disclosures via their systems. As such, ATP offers the ability to capture and return to the calling system Audit Information (if requested by the subscribing agency) including the name of the calling system, subscribing agency identifier, request ID, time and date the request is received, and time and date the response is sent.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of unauthorized or improper dissemination of information processed via ATP.

Mitigation: This risk is mitigated by the review and establishment of agreements and system connections based upon the subscribing agency's authority to collect information processed and transmitted via ATP. The ATP web service is also configurable based on the agreements established in order to limit the information processed and transmitted by ATP to only what is necessary and authorized to support the mission of the subscribing agency. It is incumbent upon the subscribing agency to define and govern the users of their system(s) to ensure proper authorization and access to the information returned from ATP.

To further mitigate this risk, as described in Question 2.2, the subscribing agency's identifier and request ID allow ATP to tie together the request from the subscribing agency and the results generated by ATP. Using the name of the calling system, the response is returned to the appropriate calling system.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Since the data processed via ATP is not retained in the web service, individuals don't have the ability to request access to such information. Individuals may, however, request access to records about them in the calling system that uses ATP by following the procedures outlined in the SORN(s) governing the calling system. All or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interest.

In addition to the procedures above, individuals seeking notification of and access to any record contained in an ICE calling system that uses ATP, or seeking to contest its content, may submit a request in writing to the ICE Freedom of Information Act (FOIA) Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia). If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW, Building 410, STOP-0550, Washington, DC 20528. For calling systems/applications that are owned by other DHS components or federal agencies, individuals should contact the FOIA offices for those components and agencies directly.

Individuals may request access to their criminal history record by following the procedures outlined in the NCIC SORN (JUSTICE/FBI-001, October 30, 2006, 64 FR 52343; 66 FR 33558; 70 FR 7513, 7517; 72 FR 3410), or by submitting a FOIA request or a FBI Identification Record Request directly to the FBI. Instructions for submitting a FOIA request and a FBI Identification Record Request are available at foia.fbi.gov and www.fbi.gov/hq/cjisd/fprequest.htm, respectively.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Since the data processed via ATP does not persist in the web service, individuals do not have the ability to access such information to seek correction of such information. Individuals may, however, obtain access to the information maintained in the calling system pursuant to the procedures outlined in the SORN(s) governing that calling system, and they may seek correction of any incorrect information in the system by submitting a request to correct the data. The data correction procedures are also outlined in the SORN(s) for the calling system. All or some of the requested information may be exempt from amendment pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Amendment of the records could interfere with ongoing investigations and law enforcement activities and may impose an impossible administrative burden on investigative agencies.

In addition to the procedures above, individuals seeking notification of and access to any record contained in an ICE calling system that uses ATP, or seeking to contest its content, may submit a request in writing to the ICE Freedom of Information Act (FOIA) Office. Please contact the ICE FOIA Office at (866) 633-1182 or see the ICE FOIA Office's website for additional information (http://www.ice.gov/foia). If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, SW, Building 410, STOP-0550, Washington, DC 20528. For calling systems/applications that are owned by other DHS components or federal agencies, individuals should contact the FOIA offices for those components and agencies directly.

Individuals may seek to correct or amend their criminal history record by following the procedures outlined in the NCIC SORN.

7.3 How does the project notify individuals about the procedures for correcting their information?

The procedures for submitting a request to correct information are outlined in the SORN(s) governing the calling systems using ATP and in this PIA in Questions 7.1 and 7.2.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have access to information about them processed via ATP or be able to correct their information.

Mitigation: Individuals can request access to information about them through the FOIA process described in Questions 7.1 and 7.2 above and may also request that their information be corrected.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

As described in the Overview, how and what information is processed and shared through ATP is configurable based on the subscribing agency and their calling system. All subscribing agencies and their calling system are individually reviewed prior to sharing or processing any information via ATP. ICE coordinates with subscribing agencies to ensure such users have the proper authority to access and use the information processed through ATP. Additionally, ICE works with subscribing agencies to ensure new calling systems at a minimum meet and satisfy the security controls and requirements prescribed in the DHS Management Directive 4300A, Sensitive Systems Policy Directive.

Subscribing agencies also have the option to receive an audit trail of ATP's activities (e.g., the subscribing agency's identifier, name of the calling system, time and date the request is received, time and date the response is sent, request ID, etc.) in order to support any subscribing agencies' reviews of user activity that suggests or indicates unauthorized access or misuse of information processed via ATP.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All ICE personnel and contractors complete annual mandatory privacy and security training, specifically the Culture of Privacy Awareness and the Information Assurance Awareness Training.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

ATP does not have user interfaces. However, for operation and maintenance purposes, certain authorized ICE employees have access to the back-end maintenance module for ATP in order to update the business rules that govern the operation and processing of information through ATP. Access to the maintenance module for ATP is limited to certain ICE personnel that support the development and continued updating of the business rules for ATP. These ICE personnel do not have access to any PII processed via ATP from within the maintenance module. Furthermore, maintenance module users can only be added via a System Change Request (SCR), which must be approved by ICE's Change Control Board (CCB). Any changes or modifications to the business rules via the maintenance module must also be approved by ICE's CCB and implemented through an SCR.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Program managers for both internal and external subscribing agencies that use or intend to use ATP coordinate with ICE (including the ICE Privacy Office and Offices of the Chief Information Officer and Principal Legal Advisor) to review and assess new uses of information consistent with DHS established procedures (e.g., using Privacy Threshold Analyses). Subscribing agencies are responsible for coordinating with their respective Privacy Officers or Points of Contact and complying with any additional privacy requirements regarding the use of ATP. As required, existing and new subscribing agencies using ATP will ensure their PIAs describe their use of ATP. When necessary, the ICE Privacy Office, other subscribing agencies' Privacy Officers or Points of Contact will work with the program managers, their respective counsel and the DHS Privacy Office (for components of DHS) to publish amendments to the SORN(s) that govern their calling system.

Additionally, program managers, agency Privacy Officers or Points of Contact (both internal and external to DHS), and respective counsel review interconnection service agreement (ISAs) for the various

internal and external calling systems that interface with ATP to ensure adequate protections are in place to safeguard information transmitted between ATP and the calling system.

Responsible Officials

Lyn Rahilly
Privacy Officer
U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix: List of Systems Using ATP

The following subscribing agencies are using ICE's ATP web service to parse criminal history records for subjects of a various range of enforcement activities or whose criminal history is required to be evaluated by law to determine eligibility for a benefit or credential. Each subscribing agency use is listed below along with the corresponding calling system that transmits to and receives the information from ATP, the PIA conducted for that particular use, the SORN that covers the use and the authority for collection and use of the information transmitted and processed via ATP.

ATP Use 1

Subscribing Agency & Date:	DHS/ICE – July 2011
System Name:	Alien Criminal Response Information Management System (ACRIMe)
PIA:	Alien Criminal Response Information Management System (ACRIMe) (DHS/ICE/PIA-020)
SORN:	Alien Criminal Response Information Management System of Records (DHS/ICE-007)
Purpose:	Immigration and law enforcement investigations/activities.

ATP Use 2

Subscribing Agency & Date:	DHS/ICE – July 2011
System Name:	Enforcement Integrated Database (EID)
PIA:	Enforcement Integrated Database (EID) (DHS/ICE/PIA-015)
SORN:	Immigration and Enforcement Operational Records System (DHS/ICE-011)
Purpose:	Immigration and law enforcement investigations/activities.