Privacy Impact Assessment
for the
United States
Citizenship and Immigration Services
(USCIS)
Person Centric Query (PCQ) Service

June 22, 2007

Contact Point
Harry Hopkins
Office of Information Technology (OIT)
United States Citizenship and Immigration Services
(202) 272-8953

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Rice/Chertoff Initiative is an information sharing initiative between the Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) and Department of State (DOS), Bureau of Counselor Affairs to share immigration and visa data between agencies. To support this information sharing initiative, the USCIS Office of Information Technology (OIT) is developing a new service called the Person Centric Query (PCQ) Service that will improve the existing business information sharing capabilities between DHS and DOS. The PCQ Service will provide authorized DHS/DOS users with a consolidated view of all information about an individual in selected USCIS and DOS data bases. This new service will improve efficiency of user searches, facilitate information sharing, increase the quality and accuracy of the underlying data, and increase the security of the information being shared among systems.

Introduction

USCIS provides the Person Centric Query Service through the USCIS Enterprise Service Bus (ESB)[1], an infrastructure that supports the use of individual services within a Service Oriented Architecture. The data retrieved by the PCQ Service is related to an individual's immigration and visa status. The PCQ Service is a composite service which allows users to submit a single query for all transactions involving an immigrant across a number of USCIS and DOS systems and returns a consolidated and correlated view of the immigrants' past interactions with the government as he or she passed through the U.S. immigration system.

The PCQ Service was initially built in support of the Rice/Chertoff Initiative, which is an information sharing initiative between USCIS and DOS, Bureau of Counselor Affairs. These two agencies signed a Memorandum of Understanding (MOU) to share immigration data and visa data. The PCQ Service will enhance the already existing information sharing that takes place between the agencies. This data sharing arrangement will allow the parties to increase processing efficiency and maintain a comprehensive picture of an applicant's status from visa application to naturalization. The PCQ Service will present a consolidated response to a query listing the name of the underlying system and the relevant information reported from that system. This will reduce the number of queries a user must make on each underlying IT system and will help improve the accuracy of the underlying systems because the information across systems can be easily compared and processing errors or possible fraud can be identified.

Currently, USCIS has a number of disparate systems which contain transactions involving an immigrant's interaction with the U.S. immigration process. These disparate systems are application and forms based. In order for an adjudicator to view all immigrants' interaction with the U.S. immigration process, the user must log into separate systems and perform a set of complex queries against each system. The user would then have to correlate the result data manually to see a person centric response.

The PCQ Service is a service made available through the USCIS ESB. The PCQ Service interfaces with a number of existing IT systems. The PCQ Service queries the underlying IT systems and presents the results of the queries sent through the PCQ Service as a consolidated set related to a single individual. The PCQ Service removes the complexity of accessing these individual systems separately by presenting a single

[1] See www.dhs.gov/privacy for the PIA for Enterprise Service Bus published on June 22, 2007.

access point. The underlying connected IT systems use a variety of different technologies including mainframe database systems, Oracle based server systems, and newer service oriented systems.

The PCQ Service conducts queries using: Name (with Date of Birth), Alien Number, or Receipt Number. The PCQ Service queries the connected immigration systems (belonging to DHS or DOS) for person centric immigration information matching the submitted query criteria. This service will be accessible via a Web Service (SOAP over HTTPS) to allow a PCQ Service Client to invoke the service, or via a Web User Interface (HTML over HTTPS). A "PCQ Client" can be either an end user (a person) or another system invoking the query on behalf of an end user. When another system is invoking the query, the necessary privacy assessments will be completed prior to the connection being made.

Prior to any PCQ Client being granted access to this service for a particular need the business system owners of each of the underlying connected IT systems must first specifically grant the PCQ Client access via a signed agreement. The signed agreement outlines the appropriate uses of the information in conformance with privacy and security requirements. The data is aggregated and stored momentarily in memory until it is returned to the requester at which point the temporarily aggregated data is discarded. For PCQ Clients that are persons, the results of the PCQ Service will be displayed on the screen and will not be available once the session ends. For PCQ Clients that are other systems, the data will be transferred into that target system and retained according to the terms of the specific agreements with the owners of each underlying connected IT system as well as the operating rules that govern the requesting system. As noted above, prior to the transfer of information to a system, all privacy compliance documentation will be completed. In addition, both types of PCQ Clients must adhere to the PCQ Service Rules of Behavior which explicitly state that the data may not be re-forwarded or re-shared, and that the data may not be stored on any device.

The following is a list of the "connected IT systems" for the Person Centric Query service.

- CLAIMS 3 - Computer-Linked Application Information Management System 3.0
- CIS - Central Index System
- AR-11 – Alien's Change of Address System
- CLAIMS 4 - Computer-Linked Application Information Management System 4.0
- CISCOR – CIS Consolidated Operational Repository
- MiDAS – Microfilm Digitization Access System
- NFTS – National File Tracking System
- DoS CCD – Department of State Consular Consolidated Database
- ISRS – Image Storage and Retrieval System

These connections will not affect the operation of the underlying connected IT systems. The PCQ Service simply is a means to query data from these systems without having to go into each application user interface and perform a separate query. Instead, the PCQ Service provides one location to query all applications at once. The usefulness and ability to retrieve information easily and quickly may increase the uses of data and increase the efficiency of users' existing duties. At all times, the use of data by the PCQ Clients integrated with the PCQ Service will be compatible with the purposes for which the data was originally collected as well as with the agreements governing access and the operating rules for each PCQ Client.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

The PCQ Service will provide response data from underlying IT systems relating to a specific individual query. The query instructs the PCQ Service to query the connected IT systems and aggregate the results and return the aggregated results to the PCQ Client. PCQ then immediately discards this data.

The information is presented so as to easily identify from the source system from which the information has been retrieved.

1.2 From whom is information collected?

The PCQ Service aggregates data from the underlying connected IT systems. The data retrieved by the PCQ Service is related to an individual's immigration and visa status. This information is primarily from the Alien File (A-File) record. The PCQ Service is a composite service which allows users to submit a single query for all transactions involving an immigrant across a number of USCIS and DOS systems and returns a consolidated and correlated view of the immigrant's past interactions with the government as he or she passed through the U.S. immigration system.

1.3 Why is the information being collected?

The PCQ Service will allow PCQ Clients to increase processing efficiency and maintain a comprehensive picture of an applicant's status from visa application to naturalization. Currently, in order for an adjudicator to view all immigrants' interaction with the U.S. immigration process, the user would have to log into separate systems and perform a set of complex queries against each system. The user would then have to correlate the result data manually to get a person centric view of the immigrant. The PCQ Service is a composite service which allows users to submit a single query for all transactions involving an immigrant across a number of USCIS and Dept. of State systems and return a consolidated and correlated view of the immigrants' past interactions with the government as he or she passed through the U.S. immigration system.

The ability of the PCQ Service to provide a consolidated whole picture view of an immigrant will reduce the opportunity for individuals or groups to fraudulently (or through processing error) obtain immigration benefits under the Immigration and Nationality Act. This ability will also help in making benefit determination as well as help determine current immigration status of an immigrant.

1.4 How is the information collected?

The PCQ Service will query the connected IT systems. The PCQ Service contains a "Query Orchestrator" component which mediates the queries to and from the connected IT systems. Alien Number along with First Name, Last Name, Date of Birth, and Country of Birth are used to correlate and match records together to a single immigrant. The correlated set of records is what is returned to the PCQ Client.

1.5 What specific legal authorities/arrangements/agreements define the collection of information?

The authority to collect information through the PCQ Service is set forth in the Immigration and Nationality Act, 8 USC 1101, 1103, 1304 et seq., and implementing regulations found in 8 CFR.

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

The user communities for the PCQ Service (the consular officers at the Bureau of Consular Affairs, Department of State (CA-DoS) as well as USCIS adjudicators) already have access to the same information via the existing USCIS applications (CLAIMS 3, CIS, AR-11, CLAIMS 4, MiDAS, NFTS) user interfaces.

The PCQ Service mitigates the risk of erroneously bringing data from Person 1 into the aggregated record of Person 2 by using a strong matching algorithm which includes matching Alien Number along with First Name, Last Name, Date of Birth, and Country of Birth to tie together records pertaining to a single immigrant. The response query clearly lists the source system and its associated response information. This allows the user to easily compare information across source systems and identify a possible algorithm error, processing error, or fraud.

The information available through PCQ will only be data that is already available to the PCQ Clients. In addition prior to any PCQ Client being granted access to the PCQ Service, the business system owners of the connected IT systems must first grant the new PCQ Client access through a connection agreement.

The PCQ Service ensures that PCQ Clients are pre-authorized for access to each underlying data source in each of the underlying connected IT systems and that each PCQ Client cannot use the PCQ Service to access any data the PCQ Client is not already pre-authorized to access by the system owner.

The response to queries is limited to a fixed set of parameters. These parameters are extensively reviewed to ensure only the information needed is returned to the user. The only way to add additional attributes to view would be to modify the configuration of the system. This would be done only as a new release of the PCQ Service. If significant changes are made to the type of data provided by the PCQ Service or if there is a significant change to how the data is used, this PIA would be updated to reflect the new use of data. Changes in the data structures of the underlying connected IT systems will require changes to the PCQ Service.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

Information gathered by the PCQ Service from connected IT systems is used for two purposes. The first is to service a query request by the PCQ Client and return a consolidated/correlated set of the data from the existing, connected IT systems hosted by USCIS.

The second use of the information is to render and present this data on the graphical interface. The use of the data is the same as when users were querying the data by going directly to the connected IT systems. The value of the service is the ability to provide a single service to query and retrieve the data from the multiple connected IT systems.

In both instances the consolidated response from the PCQ Service is used to help make benefit determinations as well as help determine current immigration status of an immigrant. The PCQ Service can also help in providing consolidated information when immigration fraud is suspected or processing errors have occurred.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern (Sometimes referred to as "datamining")?

The Person Centric Query Service does not perform any data analysis. It is possible that a PCQ Client may use the data provided by the PCQ Service in a separate system that performs data mining type functions – that is beyond the scope of the PCQ Service and would be discussed in any privacy compliance documentation for that separate system.

2.3 How will the information collected from individuals or derived from the system be checked for accuracy?

The PCQ Service mitigates mistakenly correlating multiple immigrants' records as belonging to one immigrant by using a strong matching algorithm which includes matching Alien Number along with First Name, Last Name, Date of Birth, and Country of Birth to tie together records pertaining to a single immigrant. In addition the PCQ Service provides a comparison view which allows the user to view the person centric data across the number of systems to determine if an improper mismatch may have occurred due to incorrect data stored in the connected systems.

The PCQ Service data that is transported is retrieved directly from the underlying connected IT systems and is delivered 'as is' except for reformatting to standardize the representation of the data. Any checks for accuracy of the data are performed in the underlying connected IT system. Thus the PCQ Service cannot and does not provide any assurance that the data it delivers is accurate. How data quality is managed at the data layer of the connected IT systems is out-side the scope of the PCQ Service. Each underlying IT system manages data quality differently, and the PCQ Service does not impose any data quality requirements on to the connected IT systems.

If an end user determines that erroneous information is being stored by the connected IT system, the user can correct the information by signing into the system via the native application and correcting the erroneous data. If the user does not have update privileges it may request that the change be made by notifying the appropriate data management staff, following the policies for data changes that are in effect for the system.

2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.

The PCQ Services mitigates mistakenly correlating multiple immigrants' records as belonging to one immigrant by using a strong matching algorithm which includes matching Alien Number along with First Name, Last Name, Date of Birth, and Country of Birth to tie together records pertaining to a single immigrant. In addition the PCQ Service provides a comparison view which allows the user to view the person centric data across the number of systems to determine if an improper mismatch may have accorded due to incorrect data stored in the connected IT systems.

PCQ Clients must adhere to the PCQ Service system Rules of Behavior. The Rules of Behavior explicitly state, among other constraints, that the data may not be re-forwarded or re-shared with any other user, and that the data may not be stored on any device.

Section 3.0 Retention

3.1 What is the retention period for the data in the system?

The PCQ Service performs the query to the connected IT system, on behalf of the PCQ Client person centric query request, aggregates the results in memory, and sends the information to the requesting PCQ Client. The PCQ Service then immediately discards all queried data from memory. As stated in the PCQ Service Rules of Behavior, PCQ Clients are not permitted to replicate or store any information retrieved from the PCQ Service in a separate database or in any other electronic format. Data retrieved is for viewing purposes only. PCQ Clients are also not allowed report-printing capability from the PCQ Service.

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

There is no data collected and maintained within the PCQ Service therefore data retention schedule is not applicable.

3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The PCQ Service performs the query to the connected IT system on behalf of the PCQ Client, aggregates the results in memory, and sends the information to the PCQ Client. The PCQ Service then immediately discards all queried data from memory.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The PCQ Service queries A-File data from systems owned by USCIS and the Department of State's Bureau of Consular Affairs. The DHS Internal users of this data would be users within USCIS as well as other DHS components, such as Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP). Users of the PCQ Service within USCIS are those with adjudication responsibilities. Users of the PCQ Service within ICE are those with immigration investigation purposes. Users of the PCQ Service within CBP may be those with border enforcement purposes.

The DHS Internal user community for the Person Centric Query Service already has access to the same information and more via the user interfaces of existing USCIS applications (CLAIMS 3, CIS, AR-11, CLAIMS 4, MiDAS, NFTS).

All users with access to the data are U.S. Citizens with a valid and current DHS background investigation and a current 5C/6C level security clearance.

The Audit logs will only be accessible to USCIS IT Security upon request, otherwise only PCQ Service administrators will have access to these logs and only for archival and storage management purposes.

4.2 For each organization, what information is shared and for what purpose?

Prior to any end user group being granted access to this service for their particular needs the business system owners of the connected IT systems must first agree to the access for this new population of users by signing a connection agreement with the PCQ OIT Program Manager. Their agreement to disclose or not disclose information from their connected IT system via the PCQ Service may depend on whether or not the sharing of their information is in line with the system's published Privacy Impact Assessments.

The PCQ Service is only available to authorized users who have been granted the appropriate privileges to access data from the underlying source systems being requested. Authorization determination is made via a combination of the following.

1. Does the user have a job function which requires access to the data?
2. Does the user's supervisor agree that the user should have access to the data?
3. Is the user within a user population for which the system owner of the connected IT system has authorized information disclosure?
4. Does the user have the appropriate security clearances to access the data?

Some users may not have access to request data from every connected IT system and the data from these systems is not requested by the PCQ Service when those users make requests. The data that can be queried is a small subset of the data actually stored in the underlying connected IT systems. This data is primarily person centric data relating to the A-File data stored in the connected IT systems. The purpose of

sharing the data is to provide a consolidated source for the multiple potential sources of USCIS data. Wild card queries are not allowed as currently designed.

4.3 How is the information transmitted or disclosed?

Data associated with the PCQ Services is collected via FIPS 140-2 compliant, secure mechanisms where possible depending upon the source system from which the data is gathered. Service response data is delivered to consumers securely using industry standard secure connections (HTTPS).

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

All data gathered by the PCQ Service from the underlying connected IT systems is encrypted in route from the connected IT systems to the resulting consuming human or system. All access to the PCQ Service is controlled via user ids with strong passwords and roles that are associated with those user ids. User ids may only be added, deleted or modified in the USCIS ESB system using the ICE Password Issuance and Control System. All maintenance of authentication and authorization data is audited.

Prior to a PCQ Client being granted access to the PCQ Service, the business system owner of the connected IT systems must first grant access to the underlying connected IT system and sign a connection agreement with the PCQ OIT Program Manager. The agreement to disclose or not disclose information from the connected IT system via the PCQ Service also depends on whether or not the information sharing aligns with the applicable privacy compliance documentation. This PCQ Client pre-authorization is required before any user group can be granted access to the PCQ Service.

PCQ Clients must adhere to the PCQ Service system Rules of Behavior. The Rules of Behavior explicitly state, among other constraints, that the data may not be re-forwarded or re-shared with any other user, and that the data may not be stored on any device.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

The PCQ Service queries data from systems owned by USCIS and the Department of State's Bureau of Consular Affairs. The non-DHS external users of this data would be users within the Department of State's Bureau of Consular Affairs. Users of the PCQ Service within the Department of State's Bureau of Consular Affairs are those with VISA and Passport adjudication responsibilities, as well as those with Fraud Detection and investigation responsibilities. All users with access to the data are U.S. Citizens with a valid and current DHS background investigation and a current 5C/6C level security clearance.

The Department of State's Bureau of Consular Affairs already has access to the same information and more via the native USCIS applications (CLAIMS 3, CIS, AR-11, CLAIMS 4, MiDAS, NFTS) user

interfaces. The purpose of sharing this data via the PCQ Service is to provide a consolidated source for the multiple sources of USCIS data.

The Audit logs will only be accessible to USCIS IT Security upon request, otherwise only ESB administrators will have access to these logs and only for archival and storage management purposes.

5.2 What information is shared and for what purpose?

The PCQ Service will support the information sharing initiative between the Bureau of Consular Affairs (CA) of the Department of State (DoS) and U.S. Citizenship and Immigration Services (USCIS) of the Department of Homeland Security (DHS). These two organizations have signed a Memorandum of Understanding (MOU) for the purpose of sharing immigration data and visa data. The purpose of this data sharing arrangement is to:

1. enable the parties (USCIS and CA) to increase processing efficiency and maintain a comprehensive picture of an applicant's status from visa application to naturalization,
2. reduce the opportunity for individuals or groups to fraudulently (or through processing error) obtain immigration benefits under the Immigration and Nationality Act, as amended (INA),
3. provide consular officers with information on USCIS adjudications of benefits or petitions and other decisions relating to nonimmigrant and immigrant visas, and naturalization cases.

Prior to any end user group being granted access to this service for their particular needs the business system owners of the connected IT systems must first agree to the access for this new population of users by signing a connection agreement with the PCQ OIT Program Manager. Their agreement to disclose or not disclose information from their connected IT system via the PCQ Service may depend on whether or not the sharing of their information is in line with their published Privacy Impact Assessments.

The PCQ Service is only available to authorized users who have also been granted the appropriate privileges to access data from the systems being requested. Authorization determination is made via a combination of the following:

1. Does the user have a job function which requires access to the data?
2. Does the user's supervisor agree that the user should have access to the data?
3. Is the user within a user population for which the system owner of the connected IT system has authorized information disclosure?
4. Does the user have the appropriate security clearances to access the data?

Some users may not have access to request data from every connected IT system and the data from these systems is not requested by the PCQ Service when those users make requests. The data that can be queried is a small subset of the data actually stored in the underlying connected IT systems. This data is limited to person centric attributes and case related information. The purpose of sharing the data is to provide a consolidated source for the multiple potential sources of USCIS data. Wild card queries are not allowed as currently designed.

5.3 How is the information transmitted or disclosed?

The PCQ Service will transmit information to external consumers. To the extent possible, all connections within the PCQ Service and between the system and external suppliers or consumers of data are via DHS approved secure transmission mechanisms. This means that all interconnected IT systems, to the extent possible, are connected using FIPS 140-2 compliant mechanisms. For the PCQ Service, the Department of State end users will connect via Secure Socket Layer (SSL) mechanisms using Microsoft Internet Explorer to access the PCQ Service.

5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

A signed Memorandum of Understanding (MOU) is in place between the Department of Homeland Security (DHS) and the Department of State that covers the information shared by this system. This MOU accurately reflects the scope of data shared in this PCQ Service.

5.5 How is the shared information secured by the recipient?

Data delivered by the PCQ Service to the Department of State's Bureau of Consular Affairs is encrypted during transmittal. Users must sign an agreement that they will abide by all DHS policies and regulations concerning the security of the data delivered.

The Department of State's Bureau of Consular Affairs is also bound by the Rules of Behavior for the PCQ Service which prohibits the Department of State's Bureau of Consular Affairs, or any user to re-distribute or store the data being returned by the PCQ Service.

5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

The PCQ Service is available to end users only via a web browser interface. The user interface for end users directly connecting to the PCQ Service is designed to be intuitive and easy to understand. As such, actual training requirements are minimal. However, external users must adhere to the PCQ Service system Rules of Behavior. The Rules of Behavior explicitly state that the data may not be re-forwarded or re-shared with any other user, and that the data may not be stored on any device. Further, external users must complete and sign the standard G-872 form which initiates the user account provisioning and approval process, the granting of PCQ Service access and PCQ Service Roles.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The PCQ Service does not store data; it is simply a conduit for the delivery of data stored in various connected IT systems. All data queried by the PCQ Service from the underlying connected IT systems is aggregated in memory and then encrypted in route to the resulting consuming PCQ Client. The data is then immediately erased from computer memory running the PCQ Service when the service request completes.

PCQ Client must adhere to the PCQ Service system Rules of Behavior. The Rules of Behavior explicitly state, among other constraints, that the data may not be re-forwarded or re-shared with any other user, and that the data may not be stored on any device.

Prior to any PCQ Client being granted access to this service for its particular needs, the system owners of each connected IT system must first grant the PCQ Client access by signing a connection agreement with the PCQ OIT Program Manager. The agreement to disclose or not disclose information from the connected IT system via the PCQ Service also depends on whether or not the information sharing aligns with the applicable privacy compliance documentation. This PCQ Client pre-authorization is required before any user group can be granted access to the PCQ Service.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The data retrieved by the PCQ Service system from the underlying connected IT systems is covered by the following system of records:

- DHS/USCIS Alien File (A-File) and Central Index System (CIS) System of Records last published on January 16, 2007 (72 FR 1755),
- DHS/USCIS Biometric Storage System (BSS) System of Records last published on April 6, 2007 (72 FR 17172),
- Jusice/INS-001 INS Index System last published October 5, 1993 (58 FR 51847), and
- Jusice/INS-013, INS Computer Linked Application Information Management System (CLAIMS) last published November 4, 1997 (62 FR 59734).

6.2 Do individuals have an opportunity and/or right to decline to provide information?

The data retrieved by the PCQ Service system from the underlying connected IT systems is primarily person centric data relating to the A-File data stored in the connected IT systems. The A-File may include applications for immigration benefits. Individuals who submit applications for USCIS immigration benefits are asked to provide their consent to enable USCIS to release information provided to USCIS, to assist in the determination of an individual's eligibility for a benefit. The following is an example of the language found on USCIS benefit application benefits:

> YOUR CERTIFICATION: I certify under penalty of perjury under the laws of the United States of America, that the foregoing is true and correct. Furthermore, I authorize the release of any information from my records that U.S. Citizenship and Immigration Service need to determine eligibility for the benefit that I am seeking. (Source: Form I-130 (Rev 10/26/05) Y Page 2)

An individual has the right to decline to provide the required information and consent; however, failure to do so may result in the denial of the requested benefit request.

6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?

The data retrieved by the PCQ Service system from the underlying connected IT systems is primarily person centric data relating to the A-File data stored in the connected IT systems. The A-File may include applications for immigration benefits.

A Privacy Act Statement detailing authority and uses of information is presented to the individual on the form they use to apply for an immigration benefit. The application also contains a signature certification and authorization to release any information from an individual record that USCIS needs to determine eligibility, including biometric and biographic information. All USCIS applications include a Privacy Act Statement and a signature release authorizing "…the release of any information from my records that USCIS needs to determine eligibility for the benefit…" See the Section 6.2.

Consent is given for any use to determine eligibility, when the individual signs the application. An individual has the right to decline to provide the required information and consent; however, failure to do so may result in the denial of the requested benefit request.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The stand alone systems that are connected to the PCQ Service collect personally identifiable information as a required part of the adjudication process, which must occur prior to the granting of an immigration benefit. The privacy risk that an individual may not be fully aware that their information will be used by the PCQ Service is associated with this particular collection of information. In order to mitigate

this risk, USCIS provides a Privacy Act Statement on its applications. The application also contains a signature certification and authorization to release any information provided by the individual. To further mitigate this risk, USCIS has issued updated PIAs and SORNs for two of the systems (A-File and BSS) and will be issuing updated SORNs and PIAs for the information in CLAIMS and INS Index System in the future.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own information?

The PCQ Service does not maintain any mechanism other than the PCQ Service for the display of information. It is not anticipated that individuals represented in the underlying connected IT systems will also be users and therefore no procedures are in place for individuals to access their own information. The PCQ Service merely provides a means to view data which is collected and resides across the multiple connected IT systems.

Individuals may seek access to information provided to USCIS through the means published in the applicable system of records. In order to gain access to one's information stored in the source IT systems, a request for access must be made in writing and addressed to the Freedom of Information Act/Privacy Act (FOIA/PA) officer at USCIS. Individuals who are seeking information pertaining to themselves are directed to clearly mark the envelope and letter "Privacy Act Request." Within the text of the request, the subject of the record must provide his/her account number and/or the full name, date and place of birth, and notarized signature, and any other information which may assist in identifying and locating the record, and a return address. For convenience, individuals may obtain Form G-639, FOIA/PA Request, from the nearest DHS office and used to submit a request for access. The procedures for making a request for access to one's records can also be found on the USCIS web site, located at www.uscis.gov.

An individual who would like to file a FOIA/PA request to view their USCIS record may do so by sending the request to the following address:

U.S. Citizenship and Immigration Services
National Records Center
FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

7.2 What are the procedures for correcting erroneous information?

The underlying connected IT systems are fully responsible for any data that they provide to the PCQ Service. The PCQ Service is a 'read only' service and no procedures are in place for updating any information in the PCQ Service.

Individuals have an opportunity to correct their data during interviews otherwise they may submit a redress request directly to the USCIS Privacy Officer who refers the redress request to USCIS' Office of Field Operations or Office of International Operations. When a redress is made, the change is added directly to the existing information stored in the underlying IT systems. If an applicant believes their file is incorrect but does not know which information is erroneous, the applicant may file a Privacy Act request as detailed in Section 7.1.

7.3 How are individuals notified of the procedures for correcting their information?

Since no mechanisms or procedures exist in the PCQ Service to update any data, no mechanism or procedures exist to correct data. If erroneous data is discovered through the consolidation of data process of the PCQ Service, USCIS end users have the ability of logging into the underlying connected IT systems and correcting the information as is currently the process.

Individuals are notified of the procedures for correcting their information on USCIS application instructions, the USCIS website, and by USCIS personnel who interact with them.

7.4 If no redress is provided, are alternatives available?

If erroneous data is distributed by the PCQ Service, it is the responsibility of the underlying system owner to ensure that the data is corrected. Users may contact the owners of the underlying connected IT systems to have data corrected in accordance with standard operation procedures of the underlying system.

7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.

No access, correction or redress rights are provided for by the PCQ Service

Individuals are provided the opportunity to access their own information (stored in the connected IT systems) through the Freedom of Information Act and Privacy Act process. Thereafter, an individual may seek to have the erroneous information corrected by submitting a Privacy Act request for the system with erroneous data.

Section 8.0 Technical Access and Security

8.1 Which user group(s) will have access to the system?

The end users for the PCQ Service can be USCIS Adjudicators or DHS employees or contractors needing access to this information as part of their job duties. This information can be made available to USCIS Adjudicators, Dept. of State VISA and Passport Adjudicators, Fraud Detection Units within Dept. of State and within DHS, and well as other personnel from other components of DHS requiring access.

8.2 Will contractors to DHS have access to the system?

Only to the extent that contractors are used for adjudication responsibilities will contractors have access to the system. This access must be granted on an individual by individual basis by the supervisors of the users who request access. In addition the Operations and Maintenance (e.g. the operators) contractors working on supporting the PCQ Service infrastructure may also have access to the system

8.3 Does the system use "roles" to assign privileges to users of the system?

A role is available for each of the individual underlying systems to which the PCQ Service has access. Users are granted these roles individually. Users may only view data from an underlying system to which they have been granted the appropriate role. This information is kept in an Active Directory database which contains the PCQ Clients that can authenticate with the PCQ Server. The Active Directory database contains information on the access control privileges for each PCQ Client that has access to the PCQ Service.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The PCQ Service is only available to authorized users who have been granted the appropriate privileges to access data from the systems being connected. Authorization determination is made via a combination of the following.

1. Does the user have a job function which requires access to the data?
2. Does the user's supervisor agree that the user should have access to the data?
3. Is the user within a user population for which the system owner of the connected IT system has authorized information disclosure?
4. Does the user have the appropriate security clearances to access the data?

These qualifications and procedures follow the existing procedures for USCIS employees to gain access to USCIS systems.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

Assignment of roles is provided on an official use only and applied for using the Password Issuance Control procedures managed by Password Issuance and Control System (PICS). The system may only grant roles that have been predetermined by the implementation of the PCQ Service. There exists one role for each of the underlying connected IT systems. Full auditing is performed by the PCQ Service when any user information (including the addition or deletion of roles) is updated. This auditing is implemented in accordance with DHS policies and procedures as documented in the DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

The Person Centric Query Service is provided through the USCIS Enterprise Service Bus (ESB). The USCIS ESB's full auditing capabilities have been implemented and used by the PCQ Service in accordance with the DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook. This includes the auditing of any maintenance (addition, delete, or change) of user authentication and authorization data and the auditing of specific details for each query requested of the system and response provided by the system. The USCIS ESB maintains this audit data on the servers in use by the system and these servers have been secured according to standards established by DHS policies. This helps ensure that no unauthorized access occurs on these servers and that the audit data is securely maintained.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

PCQ Service end users must undergo annual Security Awareness Training as provided by USCIS. This training includes general privacy training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

This system has been implemented in accordance with the FISMA requirements and has successfully completed its Certification and Accreditation and has received its Authority to Operate (ATO) on May 4th, 2007.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

PCQ Service access and security controls are established to mitigate privacy risks associated with authorized and unauthorized users, namely misuse and inappropriate dissemination of data. Authorized users are broken into specific user roles with specific access rights. Audit trails are kept in order to track and identify unauthorized uses of system information. Data encryption is employed at every appropriate step to ensure that only those authorized to view the data may do so and that the data is not compromised while in transmission. The PCQ Service complies with the DHS security guidelines, which provide hardening criteria for securing networks, computers and computer services against attack and unauthorized information dissemination.

Section 9.0 Technology

9.1 Was the system built from the ground up or purchased and installed?

The PCQ Service system was implemented using Commercial, Off-The-Shelf (COTS) software with a considerable amount of configuration to conform to USCIS system requirements.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Decisions concerning the implementation of integrity, privacy and security have been made with full knowledge of the DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook. To the extent practical and available, all such policies have been implemented except as noted in the PCQ Service System Security Plan and Plan of Action and Milestones.

9.3 What design choices were made to enhance privacy?

All data that is passed between one system component to another (expect where the components reside on the same physical hardware) have been designed and implemented using secure communications mechanisms as provided for in the DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook.

Conclusion

The USCIS PCQ Service will support the information sharing initiative between the Bureau of Consular Affairs (CA), Department of State (DoS) and U.S. Citizenship and Immigration Services (USCIS), Department of Homeland Security (DHS). These two organizations have signed a Memorandum of Understanding (MOU) for the purpose of sharing immigration data and visa data. The purpose of this data sharing arrangement is to:

1. enable the parties (USCIS and CA) to increase processing efficiency and maintain a comprehensive picture of an applicant's status from visa application to naturalization,
2. reduce the opportunity for individuals or groups to fraudulently (or through processing error) obtain immigration benefits under the Immigration and Nationality Act, as amended (INA),
3. provide consular officers with information on USCIS adjudications of benefits or petitions and other decisions relating to nonimmigrant and immigrant visas, and naturalization cases.

Other uses of the Person Centric Query Service will be for sharing information residing within USCIS systems with other DHS components such as U.S. Immigration and Customs Enforcement and Customs and Border Protection.

The PCQ Service does not in itself collect or maintain individually identifying data. However, the data that is gathered and transmitted by the system does contain privacy data. Therefore, the system is designed to ensure that all transmittal of data is performed over secure mechanisms as provided by the DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook. Further, the system fully implements all required procedures and mechanisms relating to user authentication and authorization and fully implements all required procedures and mechanisms with regard to auditing of the use of the system except as noted in the System Security Plan and in the system's Plan of Action and Milestones.

Responsible Officials

Harry Hopkins, Office of Information Technology

Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security