Privacy Impact Assessment
for the

United States Citizenship and Immigration Services (USCIS) Enterprise Service Bus (ESB)

June 22, 2007

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

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

Abstract

The US Citizenship and Immigration Services (USCIS) Enterprise Service Bus (ESB) is being developed by the USCIS Office of Information Technology (OIT) to facilitate information sharing and integration between USCIS systems, and across DHS components and other Agencies, such as the Department of State. The ESB is a set of commercial off-the-shelf software (COTS) that will provide a standardized infrastructure to connect to multiple systems and services. This is a new infrastructure component within USCIS that will be incrementally enhanced to provide support for multiple service interfaces. This Privacy Impact Assessment (PIA) will be updated to reflect those material changes.

Introduction

The Enterprise Service Bus (ESB) is being developed by the USCIS Office of Information Technology (OIT) within USCIS. The core ESB infrastructure allows for facilitating information sharing and building integration services with little or no modifications to the systems being integrated.

The ESB contains a set of common services which include auditing services, exception handling services, and security services. The ESB will enable USCIS to implement greater security and privacy measures into the data usage and transfer process by providing a centralized mechanism for authenticating and authorizing service access and interface access. The ESB security services accomplishes common authentication and authorization to services deployed on its infrastructure. Unlike a "Single Sign-On" infrastructure, this security infrastructure provides a common role-based security framework for the ESB hosted services. Single Sign-On (SSO) is a specialized form of software authentication that enables a user to authenticate one time and gain access to the resources of multiple software systems.

The ESB consists of various off-the-self commercial products that work together to provide an easy to use interface that hides the complexity of the legacy systems. For example, the initial service that will be hosted by the ESB is the Person Centric Query (PCQ) Service. PCQ will be an interface to nine (9) existing systems and will gather and present the resulting data as a consolidated set. The nine underlying systems from which the data is gathered are implemented in a variety of different technologies including legacy mainframe database systems, Oracle based server systems, and newer service oriented systems. The ESB hides the complexity of accessing these individual systems with a single service oriented interface. This allows an external system or human to make a single query request to the PCQ Service hosted by the ESB and receive a single result set that is the consolidated data from the nine disparate systems.

As the ESB matures it will host additional new services as well as reuse existing services already deployed on the ESB. The reuse of components in the ESB is a major contributing factor to the reduction of cost and time in implementing new hosted services.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

There are two types of data collected by the ESB. The first is operational data (used for authentication and authorization) that consists of a login id, password, user/system site code (identifies the

physical location of the user), first name, last name (of the user), organization, and the list of roles used to determine permissions for a user or system connecting to a deployed service. This data is used to authenticate and authorize user access by authorized government users and systems to services made available on the ESB.

The second type of data is audit data consisting of the request from each user to each system/service. This one-way transaction data can be used to reconstruct the transaction any time an ESB hosted service is invoked. This data does not include the response to the query. No information originating from the connected data systems will be collected and maintained within the ESB.

The data stored in the ESB Database for auditing and logging purposes includes three (3) types of logs. The first is a generic log which contains the ESB process which is processing the event, the time of the event, and a generic description of the event. The second is a login log which contains audit information of when a person has initiated a login session for a set of services on the ESB. It contains the ESB process which is processing the event, the time of the event, and the login id of the user signing onto the system. The third is a query/access log which contains information specific to those systems that may have be been accessed via a service. The audit contains the time of the access, and the login id under which the access occurred, the systems which were accessed, and the systems which responded to the access request. This data is only accessible to IT Security and can be queried by login id and time.

The most relevant data stored in the ESB Active Directory for authenticating and authorizing access to data and services are the login id, the password for the login id, and the list of allowed access roles for the login id. Other data such as site code, first name, last name and organization code is also collected, but not used by the ESB.

1.2 From whom is information collected?

The data collected by the ESB is operational data (used for authentication and authorization) and audit data. The operational data is collected from the authorized government user as part of the user id credentialing process. This user or system credentialing process takes place once prior to system access.

Audit data will be collected on the service invocations performed in order to reconstruct the transaction any time an ESB service is invoked. No content data from the underlying systems/services are included in this audit data.

1.3 Why is the information being collected?

The operational (authentication and authorization) information is collected to protect access to ESB services which may provide access to sensitive data. The ESB can be used to prevent unauthorized access of data. The audit data is collected to assist in the reconstruction of events should unauthorized access occur. Any reconstruction of events is a manual process performed by IT Security when ever there is suspicious activity on the network or system.

1.4 How is the information collected?

The information collected by the ESB is initially generated by the Password Issuance and Control System (PICS). That system provides all the data collected by the ESB which includes the user id, initial

password, and authorized systems to which that user or system has access. Any user or system owner wishing to access an ESB hosted service must submit a PICS account request form (DHS Form G-872c) requesting granting of access to an ESB hosted service(s). This DHS Form is then processed by the Headquarters PICS (HQ PICS) Security Officers following standard operating procedures for PICS account creation. This is the standard operating procedure for granting user access to USCIS enterprise applications.

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

The authority to collect this information is 5 U.S.C. 301 regarding government organization and employee conduct.

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 ESB does not collect the responses to queries. This reduces the amount and type of information maintained. The ESB is only collecting and maintaining the minimum data necessary to authorize access to services and audit service access events.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

There are two (2) types of data used by the ESB for two distinct purposes. The first is operational data used for authentication and authorization. This is the role based security data provided by PICS that gives the ESB its capability to determine which users have access to which services. The second type of data is audit data consisting of a full set of information that can be utilized to reconstruct any query and the list of systems that responded to the query. The audit data is used in the event there is suspicious activity on the network.

The only other use of data not described above is information transported through the ESB to enable systems to communicate across the ESB. All privacy impact associated with such data transport, system connection, or information access for a particular ESB hosted service shall be provided in a separate PIA associated with the program or application requiring such a service to be deployed and hosted by the ESB.

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 USCIS ESB does not perform any data analysis. Data is not changed "in route" other than to provide standardized formatting of the data, such as date and time formatting.

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

The data for role based access control (RBAC) of services controlled and managed by the ESB, will be checked for accuracy by the PICS administrator when processing the PICS account request form (DHS Form G-872c). The form is used by users and system owners to request granting of access to ESB Service(s).

For data that may be transferred through the ESB, that data is queried from the underlying services, legacy systems, or other service or data providers is delivered 'as is' except for reformatting to standardize the representation of the data. Any checks for accuracy of the data are accomplished at the originating site, and are out of scope of the ESB or the services the ESB controls. The ESB cannot and does not provide any assurance that the data it delivers is accurate.

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 data for RBAC of services controlled and managed by the ESB is protected by encryption and access control. Only ESB administrators will have access to this data and the most critical portion of this data, the password, is stored using un-reversible encryption.

The data delivered by the ESB have numerous security controls implemented to ensure that the data from the underlying connected systems remains intact from when it is first queried from the original underlying source system until it is delivered to the consuming application or end user. The primary method of this control is the use of secure socket layer (SSL) processing between all components that do not reside on the same physical machine. This ensures that data may not be altered during communications. The SSL mechanisms involved are all FIPS 140-2 compliant as per DHS policy.

ESB audit logs will only be reviewed if there is suspicious activity that leads to a need to review. This review is performed by IT Security if they determine that there may have been a security breach. Any reconstruction of events is a manual process performed by IT Security. The audit logs will only be accessible to IT Security upon request, otherwise only ESB administrators will have access to these logs and only for archival and storage management purposes.

Section 3.0 Retention

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

The operational and audit data is retained via standard backups of the systems which comprise the ESB. This data is available online for a period of 180 days. Off site retention of this data is for seven (7) years. This requirement is per *Section* 5.3 - *Audit Logs Maintained* of the DHS - 4300A which states "Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information.

Audit trails should be preserved for a period of seven years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease".

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

No. This is the standard retention period specified by DHS Certification and Accreditation (C&A) policy for system audit data. This requirement is per *Section* 5.3 - *Audit Logs Maintained* of the DHS - 4300A which states "Audit trail records must be maintained online for at least 90 days, thereby allowing rapid access to recent information. Audit trails should be preserved for a period of seven years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease".

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

The data is retained solely for the purpose of reconstructing events in the case that unauthorized access is suspected and is not used for any other purpose. The ability to manually review user access patterns after the fact if unauthorized activity is suspected greatly mitigates the possibility of misuse of the ESB. This would be done by querying all activities conducted by the suspected user. This data is stored in the ESB audit tables within the ESB Oracle database which is only accessible by ESB administrators with the appropriate role to read the audit database tables.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The information collected and maintained by the ESB (data used to authenticate and authorize user access to data and services, and audit data) is currently not shared with anyone other than with DHS and USCIS IT Security for evaluation of suspected security incidents. Since the ESB only maintains login ids/passwords and audit records, there is no reason to share this information with anyone other than for the purpose of evaluation of suspected security breaches. The privacy impacts associated with any service that generate or collect data and is not part of the core ESB service is not included in this PIA. All privacy impacts associated with such data transport, system connection, or information access for a particular ESB hosted service shall be provided in a separate PIA associated with the program or application requiring such a service to be deployed and hosted by the ESB.

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

The information collected and maintained by the ESB (data used to authenticate and authorize user access to data and services, and audit data) is not shared with anyone other than with DHS IT Security and

USCIS IT Security for evaluation of potential security incidents. The audit logs will only be accessible to IT Security upon request, otherwise only ESB administrators will have access to these logs and only for archival and storage management purposes.

4.3 How is the information transmitted or disclosed?

The ESB information (data used to authenticate and authorize user access to data and services, and audit data) is not transmitted but may be accessed by an ESB administrator with ESB administration privileges. The information is disclosed by executing query commands to the database and via the Windows 2003 Active Directory management console for user data stored in the Active Directory.

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

All access to ESB services 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 ESB system using PICS. All maintenance of authentication and authorization data is audited. All ESB auditing data stored in a database requires a user id and password with the appropriate privileges to access this data. All ESB user credentialing data stored in the Active Directory requires a user id and password with the appropriate privileges to access this data. Passwords are stored in non-reversible encryption within Active Directory. By design, there is no mechanism for retrieving passwords from Active Directory.

Active Directory is the piece of software that's bundled with the Windows Server Operating system which performs the authentication of end users for the ESB. This is the same technology that is used to authenticate windows users when logging on to a windows work station.

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

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

The information collected and maintained by the ESB (data used to authenticate and authorize user access to data and services, and audit data) is currently not shared with anyone external to DHS. This PIA will be updated when USCIS initiates this process.

Any user or system wishing to access an ESB hosted service must submit a PICS account request form (DHS Form G-872c) requesting granting of access to an ESB service(s). This DHS Form is then processed by the HQ PICS Security Officers following standard operating procedures for PICS account creation. This is the existing USCIS standard operating procedure for granting user credentials.

5.2 What information is shared and for what purpose?

The information collected and maintained by the ESB (data used to authenticate and authorize user access to data and services, and audit data) is currently not shared with anyone external to DHS.

5.3 How is the information transmitted or disclosed?

The information collected and maintained by the ESB (data used to authenticate and authorize user access to data and services, and audit data) is currently not shared with anyone external to DHS.

To the extent possible, all connections within the ESB and between the system and external suppliers or consumers of data are via DHS approved secure transmission mechanisms. This means that all interconnected systems, to the extent possible, are connected using FIPS 140-2 compliant mechanisms.

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?

Although there are a number of ESB hosted services that will have associated Memoranda of Understanding (MOU) and information sharing agreements, these ESB services are outside the scope of this PIA. All privacy impacts associated with a particular ESB service shall be provided in a separate PIA associated with the program or application requiring such a service to be deployed.

Since the ESB may be used to service users from operating entities outside of DHS, there are a number of controls within the ESB program to ensure that the ESB is used appropriately and that proper end users have proper access to data and/or services controlled by the ESB.

The first process control is that USCIS OIT Division Chiefs and each IT application steward must agree to and sign an Application Connection and Information Sharing Agreement with the ESB system owner. This document instantiates a formal process for the USCIS/OIT ESB system owner to request application connections to an USCIS/OIT managed system in production. The purpose of this document is to have a process in which the ESB can solicit approval of connectivity by the USCIS/OIT system owners. This agreement allows a USCIS/OIT system owner to agree to terms of how their system will be connected to the ESB and more importantly who will be using the information provided by the connected applications on the ESB, and how the information will be used.

Whereas an Interconnection Security Agreement (ISA) focuses on the security aspect of a connection, this agreement focuses on how the data will be used and by whom. The Application Connection and Information Sharing Agreement may be in lieu of, or in addition to an ISA and/or MOU. For example, the information owner may agree to give one organization access to their data because the organization has a need to know the information and the sharing is compatible with the original collected use of that data. Not all organizations will have the same need to know for the same information and thus the ESB can provide appropriate access controls to the information through automated means. The ESB will honor these constraints by a combination of service design as well as enforcement of RBAC.

To protect sensitive information and limit the damage that can result from accident, error, or unauthorized use, the principle of least privilege is applied. The principle of least privilege requires that users be granted the most restrictive set of privileges (or lowest clearance) needed for performance of authorized tasks (i.e., users should be able to access only the system resources needed to fulfill their job responsibilities). Application of this principle ensures that access to sensitive information is granted only to those users with a valid need to know. The roles base access enables the "principle of least privilege."

In addition to the above service design and RBAC, users connecting to the ESB must be vetted and approved to access the data and services via the ESB using the same procedures that are currently in place to provide user ids to USCIS systems. Currently the USCIS/ICE process for user credentialing includes vetting USCIS and ICE end users, non USCIS/ICE DHS users, as well as non DHS users (e.g. Department of State). All these users will go through the same user id vetting and user id credentialing process for the ESB as they currently do for the USCIS stove pipe applications.

In addition to the above, all users, within USCIS, within other DHS agencies, or within other Government Organizations wishing to access an ESB hosted service must submit a PICS account request form (DHS Form G-872c) requesting granting of access to ESB service(s). This DHS Form is then processed by the HQ PICS Security Officers following standard operating procedures for PICS account creation. This is the existing USCIS standard operating procedure for granting user credentials.

5.5 How is the shared information secured by the recipient?

The information collected and maintained by the ESB (data used to authenticate and authorize user access to data and services, and audit data) is currently not shared with anyone external to DHS.

ESB services may share information with external users. When these services are made available through the ESB, a separate privacy review will be conducted to address the arrangements between the sharing systems and/or users. Generally, these arrangements require that the users of the shared data must conform to the Rules of Behavior for the systems they access. These arrangements also entail that system and data owners approve of the use of the data by all users accessing the system, including new users accessing via new system/services through the ESB.

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

The information collected and maintained by the ESB (data used to authenticate and authorize user access to data and services, and audit data) is currently not shared with anyone external to DHS. Individual ESB services may share information available to those services with external users. Each sharing arrangement will include a training requirement to ensure that all users properly understand the appropriate use of all systems, services, and data made available to them through the ESB.

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

The ESB only stores user id, non-reversible encrypted password, site code, first name, last name, organization code, and service access control list. The ESB is simply a conduit for the delivery of data stored in various legacy systems. All data gathered by the ESB from the underlying systems or services is encrypted in route from the ESB source system to the resulting consuming system. The data is fully discarded from computer memory when the service request completes. Only audit data consisting of the service invocation parameters for any given service is stored. External users of ESB services must adhere to the Rules of Behavior for the underlying systems that are sources of data to the service they use. Further, the system owners of the source systems from which the USCIS gathers data for use in a service must agree to the use of their data by the users of the service. The scope of which users may have access to which data sources is fully controlled by the assignment of roles to each user for each service they access via the ESB.

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?

A Privacy Act Statement is provided on the G-872c Form itself for collection of user information used to request an ESB user account. This notice is provided at the point of collection, the G-872c Form, and no additional data is collected through the ESB and therefore all issues are addressed by the underlying processes/systems. This is the standard procedure required by PICS and used by all USCIS systems. Proper notice is provided for the use of the system and the data delivered as per DHS policy and regulations that cover the use of USCIS systems.

PICS is covered by the DHS System of Records Notice (SORN) General Information Technology Access Account Records (GITAAR), published in the Federal Register on December 29, 2006 (71 FR 78446).

In addition, at the time any end user logs into the ESB or any application that connects to the ESB, a warning banner is displayed stating that individuals using the computer system are subject to having all of their activities on the system monitored and recorded by system personnel. It also states that anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials. The ESB audit logs is the implementation of the "monitoring" as disclosed in the login warning banner.

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

The only personally identifiable information collected by the ESB is the information from the G-872c Form required by PICS. This collected information includes first name, last name, organization code, site code, and service access control list. No mechanism is in place for the opportunity and/or right to decline information related to the ESB. There may be rights to refuse to provide data by refusing to complete the G-872c Form. If the user refuses to complete the G-872c the end user may be refused access to data and/or services provided by the ESB.

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 only personally identifiable information collected by the ESB is the information from the G-872c Form required by PICS. No mechanism is in place for the right to consent to particular uses of the information related to the ESB. There may be rights to refuse to provide data by refusing to complete the G-872c Form. If the user refuses to complete the G-872c the end user may be refused access to data and/or services provided by the ESB.

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

The collection of ESB activity data via audits is required by DHS and National Institute of Standards (NIST) security controls. The privacy risk is that an individual may not be fully aware that their system interaction will be audited and logged. In order to mitigate this risk, the ESB provides the login banner disclosure as well as a PIA on the ESB.

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 ESB does not maintain any mechanism other than ESB administration consoles to display information. ESB users will not be able to view their activity logs or their user data in the Active Directory. The system was not designed to support this feature. Therefore no procedures are in place for individuals to access this information on their own. The audit logs will only be accessible to IT Security upon request, otherwise only ESB administrators will have access to these logs and only for archival and storage management purposes. The ESB administrator can query the audit logs, upon request, by login id and time. Manual correlation will be required to correlate the login id in the audit with the user's first name and last name stored in the Active Directory.

Users may seek access to their information in PICS by speaking to the ICE PICS Helpdesk. The only information they will receive is the information submitted by the individual. The password can be reset as necessary.

7.2 What are the procedures for correcting erroneous information?

Users who are unable to access services that they should have privileges to access should follow the standard PICS procedures for correcting this information. This includes calling the ICE PICS Helpdesk. This procedure is the same for any USCIS system which is integrated with PICS for user id and password issuance.

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

When users request a user id for the ESB they will be instructed to call the ICE PICS Helpdesk with any login issues.

7.4 If no redress is provided, are alternatives available?

The only erroneous data that the ESB may have is a user's roles. These may not have been entered correctly from the PICS user id request form. If this happens, users are instructed to call the ICE PICS Helpdesk for resolution.

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 in the ESB since it is not responsible for the data in the underlying systems and does not have any update capabilities. All issues related to privileges to the ESB are addressed through the underlying system through the ICE PICS Helpdesk. This procedure is the same for any USCIS system which is integrated with PICS for user id and password issuance.

Section 8.0 Technical Access and Security

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

Only ESB administrators have access to the data (user credentials, audit logs) maintained by the USCIS ESB.

8.2 Will contractors to DHS have access to the system?

Operations and Maintenance (e.g. the operators) contractors working on supporting the ESB infrastructure may have access to the system. All access to the ESB follows the logical access controls set up for access to USCIS computer systems. Access controls are applied to contractors and to federal employees equally.

All contractors are required to undergo background checks and obtain favorable results. All IT contracts must contain Privacy Act compliance language before the award according to DHS contracting guidelines based on the Federal Acquisition Regulation and other Executive Orders, public law, and national policy.

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 and services accessible through the ESB. Users are granted these roles individually. Users may only access data and/or services from an underlying service to which they have been granted the appropriate role.

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

Both contractors and government personnel may have access to the ESB. Security procedures are in place in accordance with the system security plan and the USCIS systems lifecycle methodology (SLM). This plan is the primary reference that documents system security responsibilities, policies, controls, and procedures. Access to the ESB is controlled via the Active Directory to authenticate users. The ESB uses Active Directory to authenticate the login id and password. Once authenticated, the ESB retrieves the roles for the connection to enforce appropriate service access. System Administrators assign roles pre-approved by their supervisors so that users have appropriate access to perform their particular job functions.

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 basis and applied using the PICS procedures embodied in PICS. The procedure for using the PICS system is standardized and documented in the appropriate USCIS policies and procedures manuals. The system may only grant roles that have been predetermined by the implementation of the ESB system. There exists one role for each of the underlying legacy systems and services. Auditing for user management tasks (e.g. add user, delete user, grant role, revoke role) is performed by the ESB system 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?

Full auditing capabilities have been implemented in the ESB 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 authentication and authorization data and the auditing of specific details for each query requested of the system and response provided by the system. The ESB maintains this audit data on the servers in use by the system and these servers have been hardened 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?

Prior to use of the ESB users must have undergone 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 & Accreditation and received its Authority to Operate (ATO) on May 4, 2007.

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

The ESB 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 ESB 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 ESB system was implemented using 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.

System designers and operational users of the system are working closely with the Privacy Office to ensure compliance with the Privacy Act and the requirements of FISMA. USCIS is working with a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. In addition, USCIS follows the USCIS SLM process, which is supplemented with information from DHS and USCIS security policies and procedures as well as the NIST Special Procedures related to computer security and FISMA compliance.

9.3 What design choices were made to enhance privacy?

All connections for data passing between systems via the ESB has been designed and implementing using secure communications mechanisms as provided for in the DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook.

Conclusion

The ESB collects and maintains a very limited set of data (e.g. user id, password (non-reversible encrypted), site code, first name, last name, organization code and service access control list to be exact) that is required to ensure appropriate authentication and authorization. It also maintains a full set of audit data sufficient to reconstruct events. This data is secured according to DHS policy and procedures as identified in the DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook and is only accessible by appropriate personnel as noted in those policies and procedures. Further, the ESB fully implements all required procedures and mechanisms relating to 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.

Data that is transported by the ESB by any of the hosted service may 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.

Responsible Officials

Harry Hopkins
Office of Information Technology (OIT)
United States Citizenship and Immigration Services (USCIS)
Department of Homeland Security

Approval Signature Page

Original signed and on file with DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security