Privacy Impact Assessment
for the

Office of the Citizenship & Immigration Services Ombudsman (CISOMB)

Virtual Ombudsman System

March 19, 2010

Contact Point
January Contreras
Citizenship and Immigration Services Ombudsman
Department of Homeland Security
202-357-8100

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

Abstract

The Office of the Citizenship & Immigration Services Ombudsman (CISOMB or Ombudsman) at the Department of Homeland Security (DHS), as mandated by the Homeland Security Act of 2002 § 452, is an independent office that reports directly to the Deputy Secretary of Homeland Security. The CISOMB: (1) assists individuals and employers with resolving problems with USCIS; (2) identifies areas in which individuals and employers have problems in dealing with USCIS; and (3) proposes changes to mitigate those problems. CISOMB has developed the Virtual Ombudsman System (VOS) to ensure the efficient and secure processing of information to aid the Ombudsman in assisting individuals and employers and making systemic recommendations to USCIS. CISOMB is conducting this privacy impact assessment (PIA) because these transactions require collection of personally identifiable information (PII).

Introduction

CISOMB receives cases through: (1) CISOMB's paper form 7001, Case Problem Submission Worksheet and Supporting Statement Case Problem Submission Form, which is posted on the DHS CISOMB Internet website at www.dhs.gov as a fillable PDF form; or (2) CISOMB's online form 7001 (same title) that is transmitted electronically with any relevant documentation to CISOMB for further processing. CISOMB reviews all information for completeness and scans all documentation into the CISOMB account within the Internet Quorum/Enterprise Correspondence Tracking (IQ/ECT) system as a case record and forwards electronically, as appropriate, along with any attachments, to USCIS for further action. Currently, CISOMB converts every case problem submission to Adobe (pdf) format for resolution.

CISOMB has developed the VOS to ensure the efficient and secure processing of information and to aid the Ombudsman in assisting individuals and employers and to make systemic recommendations to USCIS. The core of the VOS is CISOMB's web form 7001 which is a user interface web-based form which will automatically convert information submitted by an individual or employer into a case within CISOMB's account within IQ/ECT. This is a change from the previous process where information was manually entered into IQ/ECT from paper form 7001 or web form 7001. For individuals and employers who do not have Internet access, CISOMB will manually input data and case documentation from paper form 7001. IQ/ECT is the Department's enterprise-wide correspondence and case management tracking system. This system allows the Department's headquarters and components to manage cases and resolve issues in a coordinated and timely manner. For more information on IQ/ECT, please view the Enterprise Correspondence Tracking System

PIA at www.dhs.gov/privacy. The system also enables CISOMB to segregate data into several categories to generate internal reports, provide customized feedback to individuals and employers, and supply real-time aggregated statistical information for the CISOMB to assist individuals and employers with their problems with USCIS.

When an individual, employer, or their designated representative contacts CISOMB, CISOMB identifies the correspondence as: (1) a request for information about a case that was filed with USCIS (case problem); or (2) a problem, recommendation, or information request that may or may not pertain to a case which the individual, employer, or designated representative is seeking to bring to the attention of CISOMB (trend).

CISOMB further analyzes the case request and assigns it to one of six categories: (1) USCIS Referral; (2) No Jurisdiction; (3) Decision Issued; (4) Instructions; (5) Repeat Sender; and (6) 45 Days Follow Up. CISOMB acknowledges receipt of the case with a hard copy response letter to the individual or employer. These categories pertain to specific actions that will be taken by CISOMB in responding to the case problems received. Once the case problem has been assigned an appropriate category, CISOMB issues a response letter if the case problem is a "No Jurisdiction," "Decision Issued," "Instructions," "Repeat Sender," or "45 Days Follow Up." If the case problem is a "USCIS Referral," CISOMB refers it to USCIS for further research and review. CISOMB acknowledges receipt of the case with a hard copy response letter to the individual or employer. Once USCIS completes research and review of the case problem referred by the CISOMB, a letter is mailed to the respondent by USCIS. A copy of the letter issued to the respondent is transmitted to CISOMB through the IQ/ECT System for review.[1] Once USCIS mails the letter to the respondent and a copy is provided to CISOMB, CISOMB categorizes the case problem as "completed" and work on the case problem is finished. If the USCIS response is not satisfactory to the individual or employer and they contact CISOMB, then the case remains open.

The use of the CISOMB VOS will aid CISOMB in accomplishing the office's statutory mandate. It will also reduce the government burden and improve accuracy because information obtained via received correspondence will not need to be entered into IQ/ECT. An individual or employer will have the option to properly submit the information electronically feeding it directly to the CISOMB account within IQ/ECT, which currently does not exist. This will reduce the amount of time dedicated to data entry and collection. CISOMB will continue to process paper format information for case problems through paper form 7001 for those individuals and employers without Internet access. The CISOMB VOS eliminates the

[1] IQ/ECT was acquired by the Department of Homeland Security during fiscal year 2004 as a replacement correspondence management system. It is owned and operated by the Executive Secretariat for DHS.

need to convert every case problem to the Adobe (pdf) format for every submission. This will reduce manual work and increase the ability to devote more time to individual or employer resolution and statistical analyses.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

CISOMB collects the following information on the subject of the case:

- Subject's full legal name (first, middle, and last name) including alias and all other legal names;
- Subject's date of birth;
- Subject's country of birth;
- Subject's country of citizenship;
- Subject's alien ("A") Number;
- Type of case problem whether subject case problem or an employer case problem;
- First and last name of person preparing form if other than the subject named in the case;
- Subject's attorney or representative name and contact information;
- Subject's applications and petitions filed;
- Receipt number located on the top left hand corner of the Notice of Action (Form I-797) received from USCIS in response to the application/petition filed by/on behalf of the subject;
- Immigration status or interim benefit applied or petitioned for by/on behalf of the subject;
- Source of case problem related to the type of problem such as immediate adverse action; emergengy; significant hardship; processing delay; financial impact; or non-response from USCIS;
- Description of the case problem such as visa expiration, green card denial, or processing error;
- Prior actions taken to remedy the problem including: contacting an attorney; visiting USCIS Case Status Online; contacting USCIS National Customer Service Center or other government department or agency; and/or contacted a Congressional representative;
- Consent of the subject petitioner for USCIS to disclose all information in the file;

- Verification statement signed and dated by the subject of the inquiry or the authorized representative; and
- Declaration by the subject or the attorney or representative submitting the case problem.

1.2 From whom is information collected?

CISOMB collects information from all members of the general public who seek assistance from the Ombudsman in resolving problems with USCIS.

1.3 Why is the information being collected?

CISOMB collects information to carry out its mandate as provided by Section 452 of the Homeland Security Act of 2002. CISOMB uses this information to assist an individual or employer in resolving problems with USCIS; to identify areas in which an individual or employer has problems in dealing with USCIS; and to propose changes in the administrative practices of USCIS so that problems can be identified and mitigated.

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

The specific legal authorities that define this collection of information are articulated in the Homeland Security Act of 2002, Pub. Law (2002), 6 U.S.C. § 452 et seq.; Privacy Act of 1974, 5 U.S.C. 552a; Title VI of the Civil Rights Act of 1964; and Section 504 of the Rehabilitation Act of 1973.

The OMB approval for the collection of this information is provided on web form 7001 and paper form 7001, Case Problem Submission Worksheet and Supporting Statement Case Problem Submission, OMB Control Number 1601-0004, Expiration Date 01/01/2013, which is used to collect the information described in Section 1.1.

Records are also collected, maintained, and retrieved in accordance with DHS/CISOMB – 001 Virtual Ombudsman System of Records Notice that is being prepared in conjunction with this PIA.

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

Privacy Risk:

There are risks that the individual or employer will provide inaccurate data and that the individual or employer will provide more information than is necessary to resolve the case.

Mitigation:

The same CISOMB personnel that enter data from paper form 7001 will also manage inconsistencies in the VOS. CISOMB personnel contact the preparer of the form to clear up inconsistencies or typing errors. CISOMB protocols are in place to verify the subject of the case or their representative is the same person who is on file with USCIS and CISOMB. The "A" Number is treated the same as a Social Security Number (SSN) for privacy purposes.

When the individual's browser is closed, all data from the browser session is deleted from the individual's computer. There is no way to control what the individual or employer does with screen shots or printouts of their data. CISOMB recommends that the individual or employer exercise reasonable caution when using a computer or printer to avoid the unintentional release of PII. The individual or employer should make sure they can account for all original documents, scanned images, and printouts when they are finished entering data. CISOMB recommends the individual or employer delete unneeded files and properly dispose of paper files to prevent easy retrieval of PII.

The scope of the information collected is tailored to meet the needs of an individual or employer in resolving problems with the USCIS. When more information is provided than is necessary, the information is returned to the individual or employer or deleted with an explanation of why the information is not needed. These procedures ensure that any risk associated with additional and unnecessary information is mitigated.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

The CISOMB VOS is the user interface to the CISOMB account within IQ/ECT. It is used to generate workflows in IQ/ECT, reducing the need for CISOMB personnel to manually enter data from paper form 7001.

CISOMB uses the information, after it has been processed within IQ/ECT: to assist an individual or employer in resolving problems with USCIS; to identify areas in which an individual or employer has problems in dealing with USCIS; and to the extent possible, to propose changes to mitigate problems identified to USCIS. The role of CISOMB is to assist in resolving the case problem by analyzing the case and making a recommendation for resolution to USCIS.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?

Web form 7001 edits are performed by the CISOMB VOS. Analysis is not performed.

Web form 7001 provides a one-way push of data to the CISOMB account within IQ/ECT. The IQ/ECT system, already in place, analyzes data to assess needs, issues, trends, and requirements. It establishes a means by which the Ombudsman can identify and assist an individual or employer in resolving problems with USCIS. Additionally, aggregated data are used for reporting to Congress.

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

As web form 7001 is populated, the system will perform edits. Required fields must be completed before the web form can be submitted electronically to the CISOMB account within IQ/ECT.

Within IQ/ECT, information will be checked for accuracy against data previously submitted and verified by DHS, USCIS, and CISOMB for case problem resolution. For example, if an individual or employer submits a request for assistance to CISOMB and the information the person submits does not match the information currently held by USCIS, CISOMB will contact the individual or employer requesting clarification. CISOMB personnel contact the individual or employer of the form (or their representative) to remedy inconsistencies or typing errors.

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.

Privacy Risk:

There is a risk that information in the CISOMB VOS and IQ/ECT will be accessed by individuals without the proper clearances and without a need to know. Information captured on web form 7001 and paper form 7001 is provided directly by the individual or employer.

Mitigation:

CISOMB staff receives annual privacy training and introductory training on IQ/ECT before they are given an account name and password, and specialized CISOMB access and security control training as a prerequisite for authorization to use the CISOMB account within IQ/ECT. The system does not analyze data and

information captured on web form 7001 and paper form 7001 is provided directly by the individual or employer. CISOMB does not make assumptions on accuracy of information provided. If inaccurate information is found, it is resolved as quickly as possible through checking existing USCIS systems and working directly with the individual or employer. This ensures inaccurate information is kept to a minimum and ensures that the individual or employer is directly participating in any information correction and clarification. Actions taken and recommendations made to USCIS are based on information provided directly from an individual or employer.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

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

The CISOMB VOS moves data electronically approximately every hour to the CISOMB account within IQ/ECT. Retention time on the CISOMB VOS is minimal since it is a data entry web form and the web form data is not needed once the data has been moved to IQ/ECT.

Within IQ/ECT, all electronic records responding to correspondence and cases are deleted or destroyed after five years as established by DHS. Paper records containing copies of incoming and outgoing letters are destroyed no later than 18 months after scanning and verification. All issues are resolved within 60 days. There are no issues that remain unresolved through the five year retention period.

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

CISOMB VOS records do not have a NARA approved retention and disposal policy since records only transit and are not maintained on the CISOMB VOS server. Records are then electronically transferred to the CISOMB account within IQ/ECT, normally within an hour of their submission. The records are retained in IQ/ECT, not on the CISOMB VOS. The NARA approved retention and disposal policy for CISOMB records within ECT is N1-563-08.

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

Privacy Risk:

There is limited privacy risk since data is not retained on the CISOMB VOS server. The CISOMB VOS is designed to reduce the need for paper form 7001 and enable an individual or employer to use web form 7001 so that data can be electronically transferred to the CISOMB account within ECT.

Mitigation:

Data in the CISOMB VOS, once electronically transferred to the CISOMB account within IQ/ECT, is no longer needed on the CISOMB VOS server and is deleted within one hour. Data is not retained on the CISOMB server. Information is retained in the CISOMB account within IQ/ECT. In accordance with the NARA approved retention and disposal policy N1-563-08, IQ/ECT records are retained for five years and then destroyed.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organizations is the information shared?

CISOMB may refer information to USCIS which is limited to information they have on file, per the original application for benefit or service filed by the applicant, necessary to identify the individual or employer to USCIS in order to verify the nature of the issue and to resolve the problem. This information is only shared with USCIS as established by 6 U.S.C. § 452(d)(4). Information is shared with Congress in the form of data tables comprised of aggregated data within the Ombudsman's Annual Report to Congress as called for under Section 452 of the Homeland Security Act of 2002.

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

Information is shared with USCIS as necessary to assist an individual or employer in resolving problems with USCIS. Information shared are data elements described in Section 1.1. Any or all information included in Section 1.1 may be necessary to assist in resolving the case problem.

4.3 How is the information transmitted or disclosed?

CISOMB VOS data is encrypted and transmitted only to the CISOMB account within IQ/ECT. There is no disclosure of data on the CISOMB VOS server. Data received by IQ/ECT is covered under the approved Enterprise Correspondence Tracking System PIA and by the DHS/ALL-016 - Department of Homeland Security

Correspondence Records System of records, November 10, 2008, 73 FR 66657. Both can be found at www.dhs.gov/privacy.

IQ/ECT information is transmitted with a statement identifying the information as "For Official Use Only" by:

1. Hardcopy: first class mail through the U.S. Postal Service or other federally contracted delivery providers. It may also be hand-carried, by authorized staff only, and given only to the outside agency staff with an authorized need-to-know.

2. Electronic copy: through government secured fax and email lines, as authorized and appropriate with a statement identifying the information as "For Official Use Only." Information is transmitted only for the specific purpose intended. CISOMB will provide electronic data to USCIS via secure means of electronic transmission through IQ/ECT. The electronic data will be a scanned copy of information specifically authorized to be released.

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

Privacy Risk:

CISOMB VOS moves data from web form 7001 to the CISOMB account within IQ/ECT. Once moved to IQ/ECT, data is treated the same as records keyed directly from paper form 7001. Once the data is compiled and the case is established, portions of the case may be shared with USCIS for problem resolution. That is done by IQ/ECT, encrypted email, phone, or fax. Information is not transmitted to USCIS via the CISOMB VOS.

Mitigation:

Case data is shared by CISOMB to USCIS via IQ/ECT, encrypted email, phone, or fax. Sharing is done between individuals with proper clearances on a "need to know" basis to process a case. Additional report parameters have been added within the CISOMB account within IQ/ECT to allow: (1) selection of all CISOMB data; (2) selection of non-CISOMB VOS data; and (3) selection of only CISOMB VOS data. All CISOMB VOS records contain a protected "submission number" field, identifying the record as originating from the CISOMB VOS.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organizations is the information shared?

Information may be shared outside of DHS on a need to know basis in accordance with the routine uses outlined in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA.

5.2 What information is shared and for what purpose?

The CISOMB VOS information is collected and moved to the CISOMB account within IQ/ECT. There is no sharing of data, directly, from the CISOMB VOS.

However, CISOMB will share information outside of the Department to those external entities in accordance with the routine uses outlined in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA and in the DHS/USCIS – 001 Alien File (A-File) and Central Index System of Records (CIS), January 16, 2007, 72 FR 1755. This system of records is used by USCIS to identify the alien by A Number and by CISOMB, in turn, to link to cases and verify the applicant name and the USCIS immigration forms filed.

5.3 How is the information transmitted or disclosed?

The CISOMB VOS does not transmit or disclose information it processes, since the data moves electronically to the CISOMB account within IQ/ECT.

Additional report parameters have been added to the CISOMB account within IQ/ECT to allow:

1. Selection of all CISOMB data;

2. Selection of non-CISOMB VOS data; or

3. Selection of only CISOMB VOS data.

All CISOMB VOS records contain a protected field called “Submission Number,” identifying the record as originating in the CISOMB VOS.

Should CISOMB need to share information external to the Department, the following transmission means would be used:

Hardcopy

CISOMB will share information outside of the Department to those external entities in accordance with the routine uses outlined in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA and in the DHS/USCIS – 001 Alien File (A-File) and Central Index System of Records (CIS), January 16, 2007, 72 FR 1755. This system of records is used by USCIS to identify the alien by A Number and by CISOMB, in turn, to link to cases and verify the applicant name and the USCIS immigration forms filed.

Once CISOMB verifies that an external agency is authorized to receive the information under either system of records, the information is transmitted through government secured fax and email lines, with a statement identifying the information as FOUO. The information is transmitted only for the specific purpose intended, as outlined in the DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA. Information may be mailed using first class mail through the U.S. Postal Service or other federally contracted courier services. Information may also be hand carried, by authorized CISOMB staff, and given to the outside agency staff with an authorized need-to-know.

Electronic Copy

CISOMB will provide electronic data to authorized external agencies via secure means of electronic transmission in accordance with the routine uses outlined in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA. The electronic data will be a scanned copy of information specifically authorized for release.

Inter-Agency Agreements (IAAs)

IAAs will be established as necessary by CISOMB to share information with external entities, ensure that information is shared only in accordance with the routine uses outlined in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA. The correspondence containing the requested information from this system of records to any other entity will contain a statement saying that the information is provided only for the purpose specified, and any unauthorized use, disclosure, or retention of the information could expose the recipient to criminal penalties.

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?

Yes, there is a Memorandum of Understanding between the CISOMB and USCIS. However, no information is shared directly from the CISOMB VOS. Information is transferred electronically from the CISOMB VOS server to the CISOMB account within IQ/ECT.

5.5 How is the shared information secured by the recipient?

No information is shared directly from the CISOMB VOS. Information is transferred electronically from the CISOMB VOS server to the CISOMB account within IQ/ECT. If sharing does occur in accordance with the routine uses,

information is protected as outlined in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA.

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

All federal agencies are required to complete annual privacy training. This training is sufficient for information shared under the CISOMB VOS.

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

Privacy Risk:

There is no external sharing of data directly from the CISOMB VOS server or from IQ/ECT. CISOMB will share information outside of the Department to those external entities in accordance with the routine uses outlined in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA and in the DHS/USCIS – 001 Alien File (A-File) and Central Index System of Records (CIS), January 16, 2007, 72 FR 1755.

Mitigation:

Information is shared by IQ/ECT, encrypted email, phone, or fax. Information is not transmitted via the CISOMB VOS. Sharing is done between individuals with proper clearances on a "need to know" basis to process a case and in accordance with the routine uses outlined in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA and in the DHS/USCIS – 001 Alien File (A-File) and Central Index System of Records (CIS), January 16, 2007, 72 FR 1755.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

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 available to the individual or employer at the point of collection on both the web form 7001 and paper form 7001. The Privacy Act Statement covers the authority, purpose, routine uses and effects on the individual or employer as it relates to the collection.

Notice is also provided though this PIA and DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA and in the DHS/USCIS – 001 Alien File (A-File) and Central Index System of Records (CIS), January 16, 2007, 72 FR 1755. Both can be found at www.dhs.gov/privacy.

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

Yes. CISOMB web form 7001 and paper form 7001 clearly states, "You do not have to use this form to submit your case problem to the CIS Ombudsman. However, by submitting a properly completed form, the CIS Ombudsman will receive the necessary information to process your case problem. If you do not use the form and do not provide us with the necessary information, you may experience a delay in the processing of your case problem."

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?

Yes, the individual or employer may exercise control over the uses of information by choosing to not submit information to CISOMB. CISOMB web form 7001 and paper form 7001 clearly states that the purpose for the collection is to resolve issues with USCIS. Information is shared in accordance with the routine uses published in DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA and in the DHS/USCIS – 001 Alien File (A-File) and Central Index System of Records (CIS), January 16, 2007, 72 FR 1755. Both can be found at www.dhs.gov/privacy.

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

Privacy Risk:

The privacy risks identified with notice are that the individual or employer is not aware of how their information is going to be collected, shared, and maintained.

Mitigation:

The privacy risks are mitigated by providing an individual or employer with a Privacy Act Statement at the point of collection on CISOMB web form 7001 and paper form 7001. Notice is also provided through this PIA and through DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA and in the DHS/USCIS – 001 Alien File (A-File) and Central Index System of Records (CIS), January 16, 2007, 72 FR 1755. Both can be found at www.dhs.gov/privacy.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

No data is retained on the CISOMB VOS server once it has been moved electronically to the CISOMB account within IQ/ECT. Data is not sent back to the CISOMB VOS server, nor is data editing allowed after it has been submitted. All post-submission corrections would need to be made within IQ/ECT. This is a one-way push of data.

An individual or employer can gain access to information by submitting a Privacy Act request in writing, and clearly marked as a "Privacy Act Request" on the envelope and letter. Inquiries should be addressed to: Office of the CIS Ombudsman, Privacy Act/FOIA, Department of Homeland Security, Mail Stop 1225, Washington, D.C. 20528-1225. For additional directions, please see the notification procedures section of the DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA.

7.2 What are the procedures for correcting erroneous information?

See Section 7.1.

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

Procedures for correcting information are provided in the notification procedures section of DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA. The system of records notice will be published in the Federal Register and at www.dhs.gov/privacy.

7.4 If no redress is provided, are alternatives available?

Redress procedures are provided in the notification procedures section of DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA. The system of records notice will be published in the Federal Register and at www.dhs.gov/privacy.

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.

Privacy Risk:

The privacy risk is that the individual or employer will not know how to gain access to their information, how to correct it, and where redress is provided.

Mitigation:

The privacy risks are mitigated by notifying the individual or employer through the Privacy Act Statement at the point of collection on CISOMB web form 7001 and paper form 7001, through this PIA, and by following the notification procedures section of DHS/CISOMB – 001 Virtual Ombudsman System of Records that is being prepared in conjunction with this PIA. The system of records notice will be published in the Federal Register and at www.dhs.gov/privacy.

Section 8.0 Technical Access and Security

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

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

Current CISOMB operations do not involve an IT system other than IQ/ECT. Access to the CISOMB VOS system will be restricted to CISOMB staff, contractors, and other authorized DHS personnel with a need to know.

8.2 Will contractors to DHS have access to the system?

Yes. The CISOMB VOS software is developed and supported by Lockheed Martin Desktop Solutions, Inc. (LMDSI). Hardware at the Stennis Data Center (DC-1) is supported by Computer Sciences Corporation (CSC). Help Desk support is provided by CSC, for hardware, and LMDSI, for application and software support.

Contractors are properly vetted, possess valid security credentials, and will be trained by the DHS Office of Security before handling information that same as required for DHS personnel.

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

Because CISOMB VOS is a user interface to IC/ECT, roles are not necessary or available. Roles are, however, in place for IQ/ECT. CISOMB employs Immigration Law Analysts to review and analyze case problems and trends filed by an individual or employer. The Ombudsman's Information Management System Team Supervisor is an Immigration Law Analyst assigned to administer and provide oversight for the activities of the case problem and trend resolution process.

The CISOMB Receptionist is assigned to answer the main telephone line on behalf of the CISOMB. The Receptionist is charged with receiving solicited and unsolicited incoming telephone calls that may pertain to case problems or trends which the caller is attempting to bring to the attention of CISOMB. Other roles and privileges are those established by the IQ/ECT operating procedures as authorized by DHS HQ.

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

LMDSI will control system level access to web form 7001, using LMDSI internal procedures that have been approved by CISOMB.

During pre-release testing, passwords will be required to access web form 7001. Tester instructions are under development.

User guidance for web form 7001 is being prepared, paralleling the instructions for paper form 7001, and will be available upon completion of testing.

The public will be allowed to view or download user instructions and use web form 7001 once the CISOMB web page is modified and password protection is removed from web form 7001.

CISOMB VOS web form 7001 is not a full-blown system requiring detailed procedures. It is a front-end form that sends e-mail to the CISOMB account within

IQ/ECT, and then deletes the data from the CISOMB VOS server. Procedures are in place within the CISOMB account within IQ/ECT to handle paper form 7001 data.

Within IQ/ECT, CISOMB Analysis Standard Operating Procedures are documented and are in place.

Current CISOMB IQ/ECT procedures documented include:

1. Receipt of Correspondence;
2. Processing of Correspondence;
3. Analysis of Correspondence;
4. Referral of Correspondence;
5. Quality Assurance;
6. Mailing of Correspondence to an individual or employer;
7. Reports; and
8. Technical Support.

These procedures will be updated to include handling of workflows and reports submitted through web form 7001 electronically to the CISOMB account within IQ/ECT.

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

CISOMB VOS rules are maintained within LMDSI development documentation. There are only two VOS server roles: (1) Developer/Engineer; and (2) User. Web form 7001 is controlled by LMDSI, with oversight from CISOMB. LMDSI follows their CISOMB approved internal security and auditing procedure. LMDSI is responsible for enforcing developer security. Access during testing will be by password. Web form 7001 a public facing web form and will not be restricted during initial launch. The system is being tested before launch and subsequent updates will also be tested. There are no auditing procedures in place for web form 7001.

Within IQ/ECT, the actual assignment of roles and responsibilities are verified per Section 5 of the CISOMB Analysis Standard Operating Procedures which contains security and auditing procedures. The user roles consist of:

1. Intake;
2. Immigration Law Analyst; and
3. Manager.

All roles receive training in IQ/ECT and specific training and accreditation in the use of the CISOMB account within IQ/ECT. All roles will be trained to enter data

using the web form 7001 and to enter and edit data directly in the equivalent fields within IQ/ECT.

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

During testing, the contents submitted through web form 7001 will be compared with the data received by the CISOMB account within IQ/ECT. Web form 7001 data is encrypted before transmission to the CISOMB account within IQ/ECT.

IQ/ECT allows for the auditing and tracking of any user action taken within the system. Additionally, any actions taken regarding an individual's or employer's case or workflow are tracked and logged for security control and continuity of operations. Any correspondence back to an individual or employer is tracked and logged.

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

Instructions are provided to users on screen and in writing. They are encouraged to read the instructions for web form 7001 before they begin data entry.

Within IQ/ECT, annual privacy training and CISOMB internal training will be conducted specifically focusing on the use of the system providing necessary awareness for the functionality of the system as it pertains to the secure processing, storage, and retrieval of information.

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

C&A Testing is in progress for the CISOMB VOS.

IQ/ECT received an authority to operate on August 31, 2006. Additional C&A will be conducted and system FISMA clearance will be handled by DHS CIO.

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

Privacy Risk:

There is a risk that information in the CISOMB VOS and IQ ECT will be accessed by individuals without the proper clearances and without a need to know.

Mitigation:

CISOMB staff receives annual privacy training, introductory training on IQ/ECT before they are given an account name and password, and specialized CISOMB access and security control training as a prerequisite for authorization to use the CISOMB account within IQ/ECT. All roles are scheduled for CISOMB VOS web 7001 training and additional CISOMB account IQ/ECT training prior to launch of web form 7001.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

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

CISOMB purchased this custom system to be used in an effort to collect information to receive and process correspondence received from an individual, employer, or their designated representative to: (1) assist an individual or employer in resolving problems with USICS; (2) identify areas in which an individual or employer has problems in dealing with USCIS; and (3) and to the extent possible, propose changes to mitigate problems as mandated by the Homeland Security Act of 2002, Section 452.

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

The CISOMB VOS will be constructed in compliance with all applicable DHS Privacy Office, DHS CIO, DHS Records Management, and OMB regulations regarding data collection, use, storage, and retrieval. The proposed public use data collection system is therefore intended to be distributed for public use primarily by electronic means with limited paper distribution and processing of paper forms.

9.3 What design choices were made to enhance privacy?

The CISOMB VOS has been constructed on the advice of the DHS Privacy Office, DHS CIO, DHS Records Management, and OMB regulations regarding data collection, use, sharing, storage, and retrieval of information.

Responsible Officials

Raymond G. Mills
Privacy Point of Contact
Office of the Citizenship and Immigration Services Ombudsman
Department of Homeland Security

Approval Signature Page

APPROVAL SIGNATURE

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security