



Privacy Impact Assessment  
for the

USCIS Customer Relationship Interface System  
(CRIS)

December 4, 2008

**Contact Point**

**Donald Hawkins**  
**USCIS Privacy Officer**  
**United States Citizenship and Immigration Services**  
**202-272-8000**

**Reviewing Official**

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



## Abstract

The United States Citizenship and Immigration Services (USCIS) has developed the Customer Relationship Interface System (CRIS) to provide USCIS customers with the status of pending applications and petitions for benefits and processing time information. This PIA is required because the CRIS database contains personally identifiable information (PII) such as Alien Registration Number (A-Number), full name, date of birth, and address.

## Overview

The USCIS Information and Customer Service Division owns and operates the Customer Relationship Interface System (CRIS). CRIS is a web based system, accessible through the USCIS website, that provides:

1. Customers with pending immigration benefit application case status information and estimated processing times;
2. A web-based method for customers to report a change of address;
3. A service request tool for the National Customer Service Center (NCSC) toll-free call center representatives to record reported issues with pending cases such as typographical errors or non receipt of a document; and
4. A process for USCIS personnel to record the issue resolution, such as a response letter, email or telephone conversation to the customer who reported the issue.

Users of CRIS are USCIS customers, i.e., applicants and or petitioners, their legal representatives, and USCIS personnel.

USCIS Customers and their legal representatives consist of:

- applicants and petitioners for immigration benefits,
- employers who have filed for benefits on behalf of non-US citizen employees,
- attorneys representing applicants or petitioners,
- community based organizations (CBO) representing applicants or petitioners, and
- translators and care givers of applicants or petitioners.

USCIS personnel who use CRIS include:

- Tier 1 Customer Service Representatives (CSR): USCIS contract staff who are the first level of customer service support for the NCSC call center. Tier 1 customer service representatives record reported issues from USCIS customers and their legal representatives.
- Tier 2 personnel: USCIS employees providing additional expertise for customer service;
- Immigration Information Officers (IIO): USCIS employees who are trained to provide immigration information on pending cases.
- Supervisory Immigration Information Officers (SIIO): USCIS employees with additional expertise and provide oversight of the IIO staff within their office; and,
- USCIS headquarters personnel.

Customers can access the system via the Internet to check the applicant's or petitioner's case status, estimated processing time, or to notify USCIS of a change of address. USCIS personnel access the system via the DHS intranet.

Customer PII collected by CRIS includes:



- Customer biographic information, such as name, current and previous address, date of birth, country of birth, country of citizenship, Alien Number (A-Number), name of school or employer the customer attends or works for, port of entry into the United States, date of entry, and length of stay;
- Receipt number, which is a number assigned by USCIS upon receipt of each application according to when and where the application was received;
- Contact information, such as home and work phone numbers and email addresses; and
- System access information, such as login identification (ID), password, and security questions and answers.

### **CRIS System Components**

Users may interface with CRIS in two ways: via the Internet at [www.USCIS.gov](http://www.USCIS.gov), or via the phone by calling the NCSC at (800) 375-5283 or 1-800-767-1833 (TTY). There are four components to CRIS: Case Status Service Online (CSSO) and Change of Address Online (CoA), which the customer interfaces with directly via the Internet, and Customer Service Gateway and Service Request Management Tool (SRMT), which are only accessible to USCIS personnel who interface with the customer primarily over the phone.

### **Customer Interfaces**

#### **Case Status Service Online (CSSO)**

CSSO provides status updates on pending immigration benefits applications and petitions to USCIS customers and their representatives. Individual customers and their representatives can access CSSO via the Internet and enter their receipt number which they received when they filed the application or petition. The receipt number is a unique confirmation number that USCIS provides the customer upon receipt of an application or petition for immigration benefits. After the user submits the receipt number, CSSO will display the current status of the case. In addition, users may create an online portfolio to receive updates of the status of multiple cases by providing user information and the receipt number for each case status to be tracked. They use these portfolios to monitor case status information and receive updates via email. USCIS personnel may access the system, usually to verify the pending status and the processing timeframes prior to creating a service request initiated by the user.

#### **Change of Address Online (CoA)**

CoA allows a customer to readily meet the federally mandated requirement that non-US citizens notify USCIS of any change of address. Customers may electronically submit their Form AR-11, Alien's Change of Address Card, and print their completed Form AR-11 for their records. If they have pending applications or petitions with USCIS, the customer may additionally opt for CoA Online to create a service request for USCIS to update those applications or petitions with their new address.

### **USCIS Personnel Interfaces**

#### **Customer Service Gateway**

The CRIS Customer Service Gateway displays the appropriate scripts for answering a customer's question on the customer service representative's screen. These scripts are tailored for Tier 1 customer service representatives to explain laws, regulations, and USCIS forms information in response to customer questions. No PII is collected in this component of CRIS.



## Service Request Management Tool (SRMT)

SRMT provides USCIS customer service staff the ability to document a customer's issue with a pending case in a Service Request (SRs). SRs are then accessible by SIOs and IIOs at USCIS offices and service centers where the customer's application or petition is pending a decision and allows the SIOs and IIOs to document what was done to address the issue and then allows for the creation of a response letter or email to inform the customer of how the issue they reported to USCIS was resolved. Typical issues include typographical errors, the non-receipt of information, change of beneficiary information, and cases not processed within USCIS stated processing times.

SRMT provides USCIS the ability to send the service request to the appropriate USCIS location for resolution and then to record the resolution of the issue by response letter, email or telephone correspondence to the customer who reported the issue.

## Section 1.0 Characterization of the Information

### 1.1 What information is collected, used, disseminated, or maintained in the system?

CRIS collects the minimum amount of information necessary to provide customer service.

#### CSSO Data Elements

Individual customers and their representatives can access CSSO at any time to check the status of one application, or may opt to create an account to check the status of multiple applications at once and/or receive notification when status changes.

To do a one-time check of the status of one application, CSSO only requires that the individual input the application receipt number on the USCIS website and click the "go" button to retrieve the case status. The receipt number is a number assigned by USCIS upon receipt of each application and mailed to the applicant to confirm that the application was received. The number is comprised of: a numeric code for which USCIS Service Center received the application; a case number assigned chronologically by the application's appropriate case management system; and, except in applications for naturalization, on which fiscal year and day the application was received.

If the individual opts to create an account to track multiple applications and receive email updates when status changes, CSSO collects the minimum amount of PII necessary to allow the individual to track a portfolio of receipt numbers. All case status information provided online is non-attributable information and therefore, no sensitive information is required to be collected. The following information is collected from the USCIS customer for CSSO and most of the fields are optional. The fields marked with an asterisk (\*) below are mandatory:

- Salutation
- First Name
- Last Name
- City
- State
- Country
- Postal Code
- Email address\*
- User ID\*
- Password\*
- Security Question\*
- Security Answer\*
- Application/Petition Receipt Number\*

CSSO receives case status updates from the USCIS Computer Linked Account Information System (CLAIMS) 3 (which contains case status information on all benefits except refugees, asylees, and naturalization petitions) and CLAIMS 4 (which contains case status information on



naturalization petitions) systems.<sup>1</sup> Information is sent electronically on a daily basis to the CRIS database with a case Receipt Number and the new updated status of that case in the form of a case status code. CSSO uses that code to return customer a detailed explanation of the case status for each receipt number provided. A case status code is an abbreviation of the specific status of an application, and does not contain PII. CSSO uses the case status code to display an explanation of the case's status, such as:

- Your case is currently undergoing a required review by an immigration officer. We will notify you by mail as soon as the review is completed and a decision is made. If you move while this case is pending, please use our Change of Address online tool or call 1-800-375-5283 to update your address. You can use our processing dates to estimate when your case may be processed by following the link below. You can also receive automatic e-mail updates as we process your case by registering in the link below.
- Your permanent resident card is now under production and should be mailed to you within 30 days. If you move while your card is being created, please contact customer service at 1-800-375-5283 to update your mailing address. You can also receive automatic e-mail updates as we process your case by registering in the link below.
- On <DATE>, we determined that this <APPLICATION/PETITION> was not properly filed because the application or petition was not signed. Therefore, we have rejected your case and returned it to you with all supporting materials. Please follow the instructions on the notice to sign the application or petition and submit the case.

## CoA Data Elements

When a non-US citizen moves he or she must notify USCIS of their new address. The information collected by Change of Address Online is the following:

- First Name
- Middle Name
- Last Name
- Status in the United States
- Country of Citizenship
- Date of Birth
- Alien Number
- Country of Birth
- Phone number
- Alternate phone #
- Email address
- New Street Address (city, state, zip code)
- Length of Stay if Temporary Address
- Last Street Address (city, state, zip code)
- Employer/School name
- Employer/School Street address (city, state, zip code)
- Length of Stay in the United States
- Port of Entry into the United States
- Date of Entry into the United States
- Representative First Name
- Representative Last Name
- Representative Firm Name
- Beneficiary Type
- Beneficiary First Name
- Beneficiary last name
- Beneficiary Date of Birth
- Beneficiary Country of Birth

## Customer Service Gateway Data Elements

USCIS does not collect personally identifiable information from individuals via the Customer Service Gateway. The Customer Service Gateway consists of scripts for USCIS customer service staff to read in response to customers who call the customer service center according to the information the customer is seeking. If the customer has a question or issue that requires the collection of the customer's information, that information is collected in the SRMT component of CRIS.

---

<sup>1</sup> PIAs for these systems are available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).



## SRMT Data Elements

When a customer calls the NCSC call center and a USCIS customer service representative determines that they have a legitimate issue which needs to be addressed on a pending application or petition, the USCIS customer service representative collects information from the customer. The specific information collected is determined by the type of application or petition filed along with the type of issue the customer is reporting. The complete list of PII that may be collected and stored within SRMT is as follows:

- Filing Date
- Form Type
- Service Request Type
- Caller Type
- Applicant First Name
- Applicant Last Name
- Beneficiary First Name
- Beneficiary Last Name
- Representative Firm Name
- Street Address (city, state, zip code)
- Email address
- Phone number
- Alternate Phone number
- Alien Number
- Receipt Number
- Status in the United States
- Date of Birth
- Beneficiary Type
- Beneficiary Date of Birth
- Country of Birth
- Firm or School Name
- Length of Stay in the United States
- Port of Entry into the United States
- Customer Comment
- User ID
- Password
- Security Question
- Security Answer

USCIS employees use SRMT to process service requests, record their actions taken for each issue reported and they can generate correspondence in the form of letters and emails addressed to the individual(s) who contacted USCIS notifying them of the actions taken on their pending case.

## 1.2 What are the sources of the information in the system?

Immigration case status is collected from USCIS's Computer Linked Application Information Management System (CLAIMS) 3 and CLAIMS 4 and fed into the CRIS system. CLAIMS 3 is the case management system for all applications except naturalization, asylum, and refugee status, and CLAIMS 4 processes naturalization applications. This information is used in CSSO and SRMT. The customer provides the remainder of the information for SRMT, CSSO, and CoA. USCIS Content Management Office (CMO) provides the scripts used in the Gateway.

## 1.3 Why is the information being collected, used, disseminated, or maintained?

The CSSO information is maintained and disseminated to enable USCIS customers to create online accounts which enable them to quickly access their case status information and receive email updates. The CoA information is collected as required by Section 265 of the INA (8 U.S.C. 1305) which requires all aliens to report a change of address to USCIS within ten days of the move. The



SRMT data that is collected enables USCIS to document and record the resolution to customer reported issues with their pending applications or petitions.

## 1.4 How is the information collected?

The CLAIMS 3/CLAIMS 4 data is electronically fed to CRIS as applications are processed by USCIS. The status information that CRIS receives is only a status code for a particular receipt number which CSSO uses to display the current status of the application or petition (e.g. received, reviewing, relocated, card mailed, fee received, denied, approved, etc.) Customers provide information over the Internet within CSSO to create an online account and track status information by receipt number. Customers can also update their addresses over the Internet by providing change of address information, old residence and mailing address, new residence and mailing address to CoA Online.

USCIS customer service representatives access SRMT to enter information provided by the customer over the phone, which creates the SR. USCIS personnel who process SRs then access SRMT to see reported issues and to record the letter, email, fax or telephone correspondence they have with the customer to respond to the issue reported. Depending on the complexity of the SR, USCIS personnel may access any of the internal case status tracking systems at their disposal (usually CLAIMS 3 or CLAIMS 4) to resolve the issue.

## 1.5 How will the information be checked for accuracy?

The information collected by CRIS is viewed by USCIS personnel and is used to lookup the customer's records within the official case management systems. Self-verification by the customer entering account setup information for CSSO on the Internet and visual inspection of SRMT collected information by USCIS personnel is used to verify the accuracy of the data. The status codes within CLAIMS 3/CLAIMS 4 are provided to CSSO by an electronic data feed. The data feeds to CSSO are automatic without human intervention to prevent error and to ensure the accurate mapping of case status updates to receipt numbers within CSSO. For the Customer Service Gateway, USCIS personnel provide the scripts and no PII is involved.

## 1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

8 U.S.C. 1101 et seq. of the United States Immigration and Nationality Act, provides authority for development and maintenance of CRIS.

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

**Privacy Risk:** Unauthorized access to a customer's information

**Mitigation:** CRIS does not provide any personally identifiable information to requestors online. The only information that is provided is the application status, and this information is generic and cannot be used to deduce an individual's identity. Additionally, a case status response requires that an individual submit a valid receipt number. The receipt number does not indicate or



correspond to any personally identifiable information about the customer, but rather the location and date the application was received.

**Privacy Risk:** Changes or updates to application data via requests from unauthorized individuals.

**Mitigation:** CRIS does not validate the entries made by the customers and data collected by the customer service representatives. This risk is mitigated by CRIS not providing any automated updates to USCIS case management systems. The PII which is collected by CRIS is manually reviewed by USCIS personnel prior to any updates being made within the CLAIMS 3/CLAIMS 4 systems. USCIS personnel independently verify that an update or change is necessary for the application information, such as identifying a typographical error or correcting a transposed first name and last name. If a change is made, a notice is sent to the mailing address on file for that application to ensure that the notification goes to the original source of the application.

**Privacy Risk:** Collection of more information than necessary to fulfill system function.

**Mitigation:** Only the minimum amount of PII necessary is collected by each CRIS module for the particular task requested and only enough information to uniquely identify the pending application or petition.

## Section 2.0 Uses of the Information

### 2.1 Describe all the uses of information.

CRIS only collects information to assist USCIS in matching accounts within CSSO and service requests within SRMT to the correct application or petition. The PII collected is used by USCIS personnel for researching reported issues and for sending current case status information on pending applications or petitions.

- CSSO: PII elements consisting of the email address and application/petition receipt number are required to obtain current case status information and send that information to the customer. User ID, password, security question and answer are used to setup an online secure account and the country and zip code are used to gather demographics of user accounts
- SRMT: PII elements noted in Section 1.1 allow the USCIS representative to collect the necessary and minimum amount of information required for USCIS personnel who will research the reported issue to validate that the person calling with the issue has pending application/petition and that the reported issue is valid, such as a typographical error reported on a pending application, or a change in beneficiary on a petition. The address information collected within the service request is used to form a response letter to be mailed to the customer and their representative explaining how USCIS addressed the service request.
- CoA: PII elements collected are those necessary to submit an electronic Form AR-11 (Change of Address form) rather than mailing a paper-based AR-11 for non-US citizens to notify USCIS of any address change as required by law.





## 2.2 What types of tools are used to analyze data and what type of data may be produced?

The CRIS components do not conduct any electronic analysis of PII. All data is collected for reference purposes only by USCIS personnel and CRIS does not update any other application/petition processing systems used for the adjudication of pending applications or petitions.

## 2.3 If the system uses commercial or publicly available data please explain why and how it is used.

CRIS does not use commercial or publicly available data.

## 2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

**Privacy Risk:** Information may be outdated, inaccurate, irrelevant, or incomplete.

**Mitigation:** Customer provides PII directly to CRIS either online or to a USCIS customer service representative, therefore self-verifying the timeliness, accuracy and completeness of the information. Additionally, the function of SRMT allows customers to file a Service Request in order to update or correct application information, and those corrections are made by trained USCIS personnel who verify the need for a correction or change, independent of the service request, such as correcting a typographical error or a transposed first and last name.

**Privacy Risk:** Information may be compromised or accessed by unauthorized individuals.

**Mitigation:** The CSSO customer created accounts are protected by use of secure Internet protocols, strong password and login authentication, and database encryption algorithms. USCIS personnel trained in the appropriate use of PII manually collect the PII for SRMT from the customer who has initiated the contact to request a service request. Further, the data is stored within a secure Federal data center and protected by data security policies controlling the operations of DHS databases.

## Section 3.0 Retention

### 3.1 How long is information retained?

CSSO: Case status data will be maintained for one year within CRIS after a final decision, such as Approval or Denial of the application or petition, has been made. Case Status information is then transferred to tape for five years. After that time, data will be deleted/destroyed. Case status data in CRIS comes from the CLAIMS 3 and CLAIMS 4 systems, where that information is separately maintained electronically and destroyed 15 years after the last action pertaining to the application according to the Benefits Information System Privacy Act system of records notice, DHS-USCIS-007, September 29, 2008 73 FR 56596.

CoA: The CoA information is transferred daily to the USCIS AR-11 electronic storage and retrieval system via an automatic data transfer and stored within the AR-11 system. Information



located in the AR-11 system is maintained and disposed of in accordance with its NARA Data Retention Schedule, which states that the last Form AR-11 received from a registrant is destroyed 5 years after the date of receipt unless destroyed upon naturalization, departure, or the registrant's death. The CRIS CoA data collected is handled as a sub-system to SRMT and is retained according to the SRMT data retention schedule.

SRMT: SRMT data is maintained within CRIS for access by USCIS personnel for 90-days after the Service Request has been closed. After that time, the data is moved into Archive Tables, which are inaccessible by users, and are then moved to tape and taken out of the system after one year and transferred to tape for 5 years. After that time, data is destroyed. A record of the Service Request and action taken to close the request may also be printed and filed into the applicant's A-File, where it is stored for retained for 75 years from the date the file is retired to the Federal Records Center or date of last action (whichever is earlier) and then destroyed.

### **3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?**

USCIS has approved the retention schedule and has proposed it to the National Archives and Records Administration (NARA).

### **3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.**

**Privacy Risk:** Data collected in CRIS may be maintained for longer than necessary to fulfill the operations of the system.

**Mitigation:** CRIS determined that the minimum period necessary to hold the data is one year on-line and five years archived in backup tapes because data within the CRIS system is of the same nature as written correspondence and should therefore be retained according to the same policies as written correspondence received and generated by USCIS for auditing and accountability purposes.

**Privacy Risk:** Data retained by CRIS may be accessed by unauthorized users.

**Mitigation:** The CRIS system and its database undergo an annual security assessment and every three years a re-certification for accreditation. The CRIS security controls and annual security reviews provide an assessment of the risks to loss of CRIS data for the organization. CRIS security controls are continually monitored to ensure that all risks are mitigated by following proper security measures. Roles based access to information is controlled and monitored within CRIS so that limited information is provided on a restricted basis and data access is audited to ensure proper access restrictions are in place.

**Privacy Risk:** PII may be accessible in CRIS for longer than is necessary.

**Mitigation:** Internet access to information is limited to non-personally identifiable case status information. Intranet access by USCIS personnel to customer data is only available while the service request is being processed and up to 90-days after the service request is closed. After that time, the customer information in the service request is moved to archive tables which are inaccessible to users. This further limits the amount of accessible information within CRIS to authorized users until such time as the data can be taken offline to tape storage and subsequently destroyed.



## Section 4.0 Internal Sharing and Disclosure

### 4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The only system that CRIS regularly sends information to is the AR-11 Change of Address system within USCIS. CRIS provides all data from the electronic AR-11 form daily via a daily electronic batch data feed to the USCIS AR-11 CoA system. Service Requests collected via SRMT are shared with USCIS personnel who review the requests and make necessary changes to the appropriate case management system, such as CLAIMS 3 or CLAIMS 4. Depending on local office or service center policies, USCIS staff may also file a copy of the action in the applicant's A-File.

DHS has other systems, covered by separate PIAs available on [www.dhs.gov/privacy](http://www.dhs.gov/privacy), which may use CRIS data to conduct analysis, such as the USCIS Fraud Detection and National Security (FDNS) system and the Immigration and Customs Enforcement (ICE) Pattern Analysis and Information Collection (ICEPIC). Additionally, data collected in CRIS may be shared with DHS Information and Analysis (I&A) analysts for national security purposes in accordance with DHS's information sharing responsibilities.

### 4.2 How is the information transmitted or disclosed?

The AR-11 change of address data is electronically transferred over the secure USCIS intranet to the USCIS AR-11 system. Information within SRMT is accessed electronically by SIOs and IIOs, who manually make corrections to data within the CLAIMS 3 or CLAIMS 4 systems. Information shared for fraud detection or national security purposes is provided by referrals from USCIS personnel and transferred directly between appropriate analysts.

### 4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

**Privacy Risk:** Information shared outside of CRIS may be used for purposes beyond the reason for the initial collection.

**Mitigation:** All information collected via CRIS (in CoA and SRMT) is shared with the internal USCIS system directly associated with the corresponding application information, such as CLAIMS 3, CLAIMS 4, AR-11, and the A-File. This sharing is done to comply with the customer request that application information be updated. Additional data sharing is associated with fraud detection and national security purposes, which supports the integrity of the immigration benefit system process and USCIS's information sharing function as a component of DHS.

**Privacy Risk:** Unauthorized access to information shared outside the system.

**Mitigation:** Change of Address information is the only CRIS-related data that is shared internally on a regular basis. The data comes directly from the customer and is securely submitted electronically (as noted in Sections 8 & 9 of this document) to CRIS and then to the AR-11 system, thus greatly reducing the risks associated with unauthorized access or data entry errors when transferring data. Information collected within SRMT and CSSO is accessible by online secure accounts by internal USCIS personnel only. The information remains within USCIS and only USCIS personnel have accounts to access CRIS data. Information collected is not shared with other systems



electronically. Information within SRMT is viewed by SIOs and IOs to manually make corrections to data within the CLAIMS 3/CLAIMS 4 systems.

## 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 organization(s) is the information shared, what information is shared, and for what purpose?**

CRIS does not share any PII with organizations outside of DHS. Information submitted to CRIS to update the applicant's file is passed to another USCIS system such as AR-11, CLAIMS 3, CLAIMS 4, or the A-File, and information may be shared from those systems. The information CRIS provides to customers is limited to case status information, which is not personally identifiable. Case status information is shared online to anyone who inputs a valid receipt number in CSSO.

### **5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.**

CRIS does not share any PII with organizations outside of DHS. USCIS does share information from other systems outside of DHS, and some of the information in those systems may originate from data collected in CRIS. That sharing is compatible with the collection of the information and covered by the routine uses in the following system of records notices: Benefits Information System DHS-USCIS-007, September 29, 2008 73 FR 56596, Fraud Detection and National Security Data System (FDNS DS) DHS-USCIS-006, August 18, 2008, 73 FR 48231, and/or Alien File (A-File) and Central Index System (CIS) DHS-USCIS-001, January 16, 2007, 72 FR 1755.

Case status information, which is provided in generic, non-personally identifiable format, is shared as part of the purpose of the system, to determine the status of pending applications and/or petitions for benefits.

### **5.3 How is the information shared outside the Department and what security measures safeguard its transmission?**

CRIS displays case status information online or sends it via email to addresses associated with CSSO accounts to any individual who is able to provide a valid receipt number. CRIS maintains an audit trail of all user successful log-on and log-off activity and password change actions. Additionally, automated case status information sent to a customer via email has an audit trail available for review.



CRIS does not share personally identifiable information directly outside the Department, but does share with systems that share outside of DHS as described by the system of records notices identified in 5.2, above.

## 5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

**Privacy Risk:** Unauthorized individuals may use CSSO to obtain information that does not pertain to them.

**Mitigation:** CRIS does not provide any personally identifiable information to requestors online because it does not authenticate that the requestor is actually the customer or his representative. The only information that is provided is the application status, and this information is generic and cannot be used to deduce an individual's identity. Additionally, a case status response requires that an individual submit a valid receipt number. The receipt number does not indicate or correspond to any personally identifiable information about the customer, but rather the location and date the application was received. USCIS provides customers their application receipt numbers on receipt notices mailed to the address provided on the application, and cannot be obtained online or via phone to prevent unauthorized access.

Additionally, CRIS does not provide any automated updates to USCIS case management systems. The PII which is collected by CRIS is manually reviewed by USCIS personnel prior to any updates being made within the CLAIMS 3/CLAIMS 4 systems. USCIS personnel independently verify that an update or change is necessary for the application information, such as identifying a typographical error or correcting a transposed first name and last name. If a change is made, a notice is sent to the mailing address on file for that application to ensure that the notification goes to the original source of the application.

## Section 6.0 Notice

### 6.1 Was notice provided to the individual prior to collection of information?

Collection of data within CRIS is covered by the Benefits Information System system of records notice, DHS-USCIS-007, September 29, 2008 73 FR 56596. Prior to establishing an online account or entering change of address information online, customers are presented with a Privacy Act Statement as required by Section (e)(3) of the Privacy Act.

The Privacy Act Statement details the authority to collect the information requested and uses to which USCIS will put information the customer provides on immigration forms and in support of an application. The forms also contain a provision by which a customer authorizes USCIS to release any information received from the customer as needed to determine eligibility for benefits.

As Case Status Online and Change of Address Online are the only systems that are directly accessible to the public, both of these systems prominently display a Privacy Statement required by



Section (e)(3) of the Privacy Act and also provide a link to the DHS web-privacy policy. The Privacy Statements for Case Status Online and Change of Address online are available in Appendix A of this PIA.

Before a Tier 1 customer service representative collects information from the public and enters that information into SRMT, the customer is asked a series of questions and notified that information will be collected to assist with the recording of the Service Request to assist in a timely response and follow-up by USCIS

## **6.2 Do individuals have the opportunity and/or right to decline to provide information?**

Case Status Online does not require the input of PII unless the individual wants to create a Case Status account. Because this service is optional, individuals have the opportunity to decline to provide information. If they choose not to provide the information, they will not have the ability to create an account and receive automatic case status updates.

When Change of Address information is provided online, the customer has the right to decline to provide PII; however, the customer is informed at the point of collection that a change of address cannot be completed without providing this information. This is also true for updating the address for an application or petition. According to 8 U.S.C. 1305, all aliens are required by law to provide a change of address within ten days of the date of that change. Failure to provide the change of address may result in penalties, including fines not to exceed \$200 and/or imprisonment of no more than 30 days. 8 U.S.C. 1306 (b).

SRMT also collects PII in order to complete a Service Request. It remains within the rights of the customer or their representative to decline to provide the required information for the Service Request; however, this will result in the inability to complete the 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 customer must register and use a User ID and Password for authentication before the use of CSSO or CoA online. Customers must accept the terms and conditions for how information will be collected and used as well as how the unauthorized use of the system is prohibited. If they do not agree to these terms, they may still obtain case status information online, but they will not be able to register for automatic emails on case status updates.. In addition, the privacy policy link describes all potential uses for the collected information.



## 6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

**Privacy Risk:** Individuals may be unaware that their information is being collected and used by USCIS.

**Mitigation:** Notice is provided when customers speak with USCIS personnel and via the Internet, as outlined above. Individuals are not unaware that information is being collected as they are prompted with online forms for data entry and if they are calling USCIS with an issue, the customer service representative informs the customer that they require the collection of information in order to properly record the customer's service request.

## Section 7.0 Access, Redress and Correction

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

Users who create online CSSO accounts must authenticate via a secure login using the username, password, and security questions used to create the account. Once authenticated, individuals may access the information they used to create their profiles, such as name and location information as well as their password reset and security question and answer on file. The customers also have access to their case status portfolio of receipt numbers to add and delete cases for which they desire updated case status information.

Change of Address information collected by the customer online is not accessible by the customer after the submission of the information to USCIS. No further edits or review of the data are available once the information has been submitted. If the information is incorrect, the customer must re-submit with corrected information.

For SRMT, data which is collected from the customer by the customer service representative cannot be accessed by the customer. Once collected, the customer must wait for USCIS to respond to their service request. If 30 days goes by and the customer is not contacted customer service and without a response, the customer may contact customer service again with the same issue to create a secondary service request for the same issue.

If a FOIA or Privacy Act (PA) concern arises, CRIS customers can file a FOIA request to gain access to their USCIS records. USCIS has final discretion on the application of statutorily based withholding or releasing the requested information. If an individual would like to file a FOIA/PA request to view their USCIS record, the request can be mailed 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 inaccurate or erroneous information?

Customers can make changes in their CSSO account by logging in and making the correction to information they provided. If Case Status information appears to be inaccurate, the customer can contact USCIS customer service. For Change of Address, if the customer has made a mistake with their address and they have submitted their information to USCIS, they may repeat the original process and submit a correct address or they may contact USCIS customer service at 1-800-375-5283 and speak with a customer service representative.

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

The USCIS website contains links for the CSSO and CoA components and lists the toll free phone number for customer assistance.

## 7.4 If no formal redress is provided, what alternatives are available to the individual?

If the USCIS customer service representative is unable to address the customer's issue, a service request is taken with SRMT and forwarded to the appropriate office or service center with USCIS or the phone call is transferred to a Tier2 Immigration Information Officer to provide further information to the customer.

## 7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

**Privacy Risk:** Individuals may not be able to access or correct their information in CRIS.

**Mitigation:** Because redress is inherently the same process as the original submission of information, CRIS allows for access and redress. Users may contact USCIS via the toll free phone number and report issues for as long as their cases are pending with USCIS. They may also access case status information online as long as they have valid receipt numbers for their pending cases. Privacy is protected on updates and new reported issues as with the original submission of data.

## Section 8.0 Technical Access and Security

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





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

CSSO users are identified online as those customers and their legal representatives who have a pending application or petition with USCIS. This information is provided on the Internet on the CSSO website to clearly identify who may establish an account online for CSSO status updates. Any person interested in receiving case status information for a pending USCIS application or petition may create an online account.

SRMT users are identified and authorized by the USCIS Information and Customer Service Division, Service Center Operations, Field Operations and Asylum offices. Access to SRMT is restricted by USCIS management and limited to USCIS personnel and approved contractor staff:

- Tier 1 customer service representatives – USCIS contractors, the first level of customer service support on the toll free customer service number, who record reported issues from customers and their representatives
- Tier 2 personnel – USCIS employees providing additional expertise for customer service
- Immigration Information Officers (IIO) – USCIS employees trained to provide immigration information on pending cases.
- Supervisory Immigration Information Officers (SIIO) – USCIS employees with additional expertise and functions, and providing oversight of the IIO.
- USCIS Headquarters personnel

## **8.2 Will Department contractors have access to the system?**

Yes, contractors have access to CRIS. USCIS establishes personnel security requirements for contractors (additional claims processing staff and Tier1 customer service organizations) . USCIS requires an approved Interconnectivity Security Agreement (ISA) be established prior to contractor staff being granted access to the CRIS Intranet modules. All contractor staff are required to undergo a security clearance prior to being granted an account online with SRMT. Once granted a clearance, contractor staff are further restricted within CRIS by role-based security to restrict data access for collection only.

## **8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?**

The USCIS personnel are required to receive annual security awareness training. The security awareness training covers how to handle personally identifiable information. Refresher training is required every year.

## **8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?**

CRIS received ATO on July 28, 2008 which is valid until July 28, 2011.



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

CRIS maintains an audit trail of all user successful log-on and log-off activity and password change actions. Additionally, automated case status information sent to a customer via email has an audit trail available for review. For SRMT, all activity performed on a customer's Service Request, such as assigning the request to be fulfilled, relocating it to another office, placing the request into a pending status for further research, etc., is logged, noting who performed the action and when it was performed. For further traceability of actions performed on CRIS data, all updates to CRIS tables contain audit information with who made the edit or update and when each update occurred. The auditable information within CRIS cannot be deleted by any of the roles within the system and are only accessible by system administration personnel. Further safeguards to CRIS modules include 20-minute inactivity user session timeouts and the restrictions to have only one active session per user.

## 8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

**Privacy Risk:** Unauthorized users may gain access to data stored in CRIS.

**Mitigation:** Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized users; namely, misuse and inappropriate dissemination of data. CRIS utilizes a role-based approach to user access. Each role has specific rights assigned to it. Audit trails will be kept in order to track and identify any unauthorized use of system information. Data encryption using Internet Secure Socket Layer data encryption is employed on all CRIS applications and user passwords are stored in the database using a 3-DES encryption algorithm. These multi-layer encryption technologies are employed to ensure that only those authorized to view the data may do so and that the data has not been compromised while in transit. Further, CRIS complies with DHS security guidelines, which provide restrictions on the hardware and operating systems which the CRIS system can be hosted and where they can be located. All of these security restrictions control the safeguarding of CRIS data against unauthorized access to customer data and prevent undisclosed information dissemination.

## Section 9.0 Technology

### 9.1 What type of project is the program or system?

CRIS is an operational customer service system.

### 9.2 What stage of development is the system in and what project development lifecycle was used?

CRIS is currently in Operations and Maintenance stage of the system lifecycle.



CRIS follows Information Technology Lifecycle Management 1.0 (ITLM), which incorporates data integrity, privacy and security within each ITLM phase as defined by the DHS Chief Information Officer (CIO).

### 9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

CRIS is a web-based application and as such is susceptible to privacy concerns. CRIS is operating in accordance with Office of Management and Budget (OMB) M-04-04, E-Authentication Guidance for Federal Agencies. CRIS has an E-Authentication Assurance level of 1.

System security and information privacy for CRIS is achieved through several mechanisms including:

**Socket level encryption and authentication:** All Internet data transmissions associated with CRIS is encrypted via Secure Sockets Library (SSL), which uses public key technology to negotiate a session key and cryptographic algorithms (based on the Data Encryption Standard (DES), triple-DES, International Data Encryption Algorithm (IDEA), Rivest Code (RC) 4, RC2, and Message Digest (MD) 5 hashes) between all CRIS clients and the CRIS web server. The public key will be stored in a X.509 certificate that bears a digital signature from the USCIS' certificate authority.

**Infrastructure network perimeter/border security:** CRIS is deployed within the Department of Justice Data Center (JDC-W) and leverages infrastructure and network services it provides, such as Protocol Filtering, Internet Protocol (IP) Address Filtering, Transmission Control Protocol/User Datagram Protocol (TCP/UDP) Port Filtering, Stateful Inspection, Packet Filtering, Network Address Translation (NAT), Reverse Proxy, Encrypted and Secure Authentication.

Physical security:

**Application-based user authentication and access Control:** CRIS uses user IDs and passwords to identify users and provide access control to application services. All application services and database privileges are based on user roles. Passwords associated with the user accounts and roles are stored within the application database in encrypted form. Password encryption is implemented via a CRIS system Java utility class, which provides for just-in-time encryption and decryption of passwords.

**Access Control Lists:** Access control lists that are checked against user identification information stored within the session before any web page within the application is displayed restrict direct URL access. This prevents users from bypassing the application menus and assigned privileges by using the browser to directly navigate to web pages that have restricted access. CRIS access control lists are maintained and used via database tables and Java classes that are called before each page is loaded. The system does not have the technology or the ability to monitor the activities of individuals or groups beyond that required to accept address changes.



## Conclusion

CRIS is a web enabled system that offers customers of USCIS access to pending case status information and estimated processing times; the ability to notify USCIS electronically of a change of address; to record a service request by customer service representatives from applicants on issues they have with their pending cases; and for USCIS personnel to document the resolution of the reported pending case issue. CRIS enhances USCIS's customer service capabilities and provides timely case status information to customers on their pending applications and petitions.

## Approval Signature

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III  
Chief Privacy Officer  
Department of Homeland Security



## APPENDIX A – Privacy Act Notice

### CRIS-Case Status Online

**Authority:** In accordance with the Paperwork Reduction Act of 1995, Public Law 104-13 and the Privacy Act of 1974 as amended, Public Law 93-589 USCIS provides Case Status and Change of Address to individuals and their representatives via a web-based application.

**Purpose:** The purpose of the collection of the information to setup an online Case Status account is to enable U.S. Citizenship and Immigration Services to provide status updates on pending applications and petitions to those individuals who have filed for benefits and wish to receive status updates electronically via the Case Status Online system.

**Routine Uses:** The information will be used by and disclosed to DHS personnel and contractors or other agents who need the information to assist in activities related to providing status information on pending applications and petitions. Additionally, DHS may share the information with law enforcement or other government agencies as necessary to respond to potential or actual threats to national security pursuant to the agency's published Privacy Policy and the routine uses outlined in the Benefits Information System system of records notice, DHS-USCIS-007, September 29, 2008 73 FR 56596.

**Disclosure:** Furnishing this information is voluntary; however, failure to furnish the requested information may prevent the ability of Case Status Online to send status updates on cases which are pending.

### CRIS-Change of Address Online

**Authority:** The collection of alien address information is required by Section 265 of the Immigration and Nationality Act (8 U. S.C. 1305).

**Purpose:** The data collected for a Change of Address notification is used by U.S. Citizenship and Immigration Services for statistical and record purposes and may be furnished to Federal, State, local and foreign law enforcement officials and intelligence agencies for national security purposes.

**Routine Uses:** The address information entered into Change of Address Online will be used by and disclosed to DHS personnel and contractors or other agents who need the information to assist in ensuring that address information is updated within the proper claims processing systems. Additionally, DHS may share the information with law enforcement or other government agencies as necessary to respond to potential or actual threats to national security pursuant to the agency's published Privacy Policy and the routine uses outlined in the Benefits Information System system of records notice, DHS-USCIS-007, September 29, 2008 73 FR 56596.

**Disclosure:** Furnishing this information is voluntary; however, failure to report a change of address is punishable by fine or imprisonment and/or removal.