Privacy Impact Assessment for the

Complaint Tracking System (CTS)

June 29, 2009

Contact Point
Rose Bird
Director, Privacy Incidents and Inquiries
Department of Homeland Security
(703)235-0780

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

AILA InfoNet Doc. No. 09080562.pdf

Abstract

The Privacy Office of the Department of Homeland Security (DHS) operates the Complaint Tracking System (CTS). CTS is a correspondence workflow management system that assists the DHS Privacy Office (hereinafter referred to as Privacy Office) in responding to complaints, comments, and requests for redress from the public, other government agencies, and the private sector. The Privacy Office conducted this privacy impact assessment because CTS collects and uses personally identifiable information (PII).

Overview

The DHS Privacy Office receives numerous complaints, comments, and requests for redress of privacy issues throughout the year. This correspondence requires analysis, storage, categorization, and coordinated responses. The Complaint Tracking System (CTS) is a workflow system that DHS Privacy Office personnel utilize to respond efficiently to inquiries from the public and other government and private-sector agencies. CTS allows users to manage correspondence tracking with pre-defined routing inside workflow templates.

CTS is a completely self-contained information system within DHS. It interfaces with other systems using the Lockheed Martin Intranet Quorum database to collate contact information. It also uses the DHS local area network for printing. The DHS Privacy Office is the business owner and sole user of CTS and, as such, is primarily responsible for the system.[1]

While only the DHS Privacy Office may use CTS, the system does share information with additional DHS organizations for:

- briefing material for senior leaders;
- maintenance of official documents;
- documenting and responding to public mail sent to DHS;
- maintaining internal coordination within DHS; and
- enabling the appropriate handling, records management, and customer service actions generated by the correspondence.

Information collected in CTS is derived from the written and electronic correspondence received from DHS components, the public, other government agencies, and the private sector. This information may include the name and home address of the individual sending the correspondence or initiating a telephone call to the agency. Other information that may be obtained but is not required, includes the e-mail address, telephone number, business or organizational address, or the Social Security Number of the individual. The CTS record, created by the receipt of this correspondence, will also include the subject matter of the correspondence. If an individual submits paper-based correspondence, personnel from the Privacy Office scan the document(s) and an image of the correspondence is maintained in a case file.

The most common transaction begins with a piece of correspondence or telephone call from an organization, individual, or a person acting on behalf of an individual. A member of Congress acting on behalf of a constituent may also initiate correspondence. If the Privacy Office receives a letter, it will scan

[1] The DHS Office of the Chief Information Officer physically and technically secures the system.

AILA InfoNet Doc. No. 09080562.pdf

the letter and attach it to a workflow. Data received or compiled is placed into a CTS case folder. A case folder contains one or more case files for an individual or an organization. Since an individual may contact DHS on several topics over several years, CTS users place each individual topic in its own case file for resolution.

Based on the content of the inquiry, the case file is either assigned to a Privacy Office user or forwarded to a responsible DHS component to provide a response to the submitter. Once a response has been prepared and, if necessary, approved by the Privacy Officer, the signed response letter is scanned and attached to the case file, and the case file is closed in the DHS Privacy Office database.

CTS provides the ability to collaborate with other DHS users to respond to the incoming correspondence. The CTS record created will include the step notes (progress notes) that document the actions taken in a particular case, as well as relevant notes from the case as it is being tracked. CTS ensures a timely response to the correspondence and provides quality assurance tracking.

The collection of documents within CTS is governed by 5 U.S.C. § 301 (general agency powers for recordkeeping), the Privacy Act of 1974, as amended (5 U.S.C. § 552a), and 6 U.S.C. § 142 (providing for appointment of a Privacy Officer to assure, in part, that personal information contained in Privacy Act system of records is handled in full compliance with fair information practices). Pursuant to 5 U.S.C. § 301, DHS is authorized to implement Departmental regulations that manage DHS's day-to-day operations. These operations include regulating employees, managing agency business, and controlling agency papers and property.

Section 1.0 Characterization of the Information

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

CTS may contain the following personal data elements:

- Prefix
- First Name
- Middle Name
- Last Name
- Suffix
- Title
- Organization
- Home Phone
- Home Address
- Business Address
- Social Security Number (SSN)
- Business Phone
- Mobile Phone
- Fax
- E-mail address
- URL
- Country of Origin
- Date of Birth
- Gender
- Alien File Number

The system also uses preexisting records from other DHS components that use the Intranet Quorum system. These components may have already entered information about individuals who previously contacted or interacted with DHS.

AILA InfoNet Doc. No. 09080562.pdf

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

The sources of the information are the original incoming correspondence sent by the original requestor, and any related correspondence received back from assigned responder. The sources include but are not limited to:

- Internal DHS Components (see Question 4.1)
- The White House
- The Vice President
- Other Federal agencies
- Congressional offices
- State and local governments
- Foreign officials or governments
- U.S. and foreign corporations
- Non-government organizations
- The general public

The system also uses the information collected previously by other DHS components that use the Intranet Quorum and other databases. This information usually comes from individuals/entities that previously corresponded or interacted with those components.

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

The Privacy Office collects this information in order to facilitate efficient, accurate and timely handling of incoming complaints, comments, and requests for redress of privacy issues between the individual and DHS. The Privacy Office utilizes CTS in order to maintain a record of the contact, enable follow-up correspondence, and forward the correspondence to an action office. The collection of PII facilitates DHS's ability to forward correspondence without confusion by uniquely identifying the action item by its actual identity. Additionally, the collection of PII assists DHS in its analysis, storage, categorization, and responses within CTS.

1.4 How is the information collected?

System users enter information into CTS by:

- typing the information received verbally into the CTS record;
- typing the information received via mail into the CTS record;
- scanning original documents into the CTS record as an Adobe PDF file;
- collection from existing DHS data sources; and
- copying information received electronically and pasting them into the appropriate fields in an electronic form which comprises a portion of the CTS record.

1.5 How will the information be checked for accuracy?

The Privacy Office checks the information for accuracy by comparing the information entered into the CTS record to the source of the information. These sources include phone calls, mail, and electronic mail from the individual. The Privacy Office can also check information against preexisting records shared

AILA InfoNet Doc. No. 09080562.pdf

with other DHS components through the Intranet Quorum database. By using this function, all DHS components can increase the accuracy of the information by checking information about an individual gained from recent inquiries against information gathered in past inquiries. This process ensures that information is current.

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

The collection of documents within CTS is governed by 5 U.S.C. § 301 (general agency powers for recordkeeping), the Privacy Act of 1974, as amended (5 U.S.C. § 552a), and 6 U.S.C. § 142 (providing for appointment of a Privacy Officer to assure, in part, that personal information contained in Privacy Act system of records is handled in full compliance with fair information practices).

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

The scope of the information collected in CTS is limited to the amount of data necessary to act upon the request, correspondence, or other possible action item received by DHS. Although each correspondence is very likely to collect the full name of a correspondent, the date of birth, for example, is only collected if it is voluntarily given and relevant to the request or correspondence. If submitters provide information that is not relevant, it is either not documented (e.g., information taken by phone and is not written down) or grayed out within CTS data fields (if in electronic form). These practices differ because many submissions arrive at DHS as unsolicited correspondence.

The threat from electronic eavesdropping is a privacy risk. To counter this threat, remote access is strictly controlled and allowed only on an as-needed basis. Authorized DHS users may only access CTS by using an approved encryption scheme. Remote access to CTS is monitored and controlled at all times. Section 8.0 of this PIA outlines the robust technical security measures enabled for CTS.

Another privacy risk is the collection of additional information in the database. The database contains a text field for general comments into which a Privacy Office user can add information. This information can be viewed by users of other DHS systems that link into the Intranet Quorum database. The training of staff using CTS and systematic review process of the CTS system mitigates this privacy risk. During each work flow step in CTS, a system user can check that only information outlined in Section 1.1 is maintained in the system.

To protect the integrity of the information in CTS, CTS users can enable a system level security lock down feature within the workflow template. This feature allows the CTS user to lock down certain fields within a record. These fields, may be hidden from view, or grayed out so successive CTS users may view part or all of the item but not change the contents. Users receive training on how to apply system level security to their work and when the application may be appropriate.

AILA InfoNet Doc. No. 09080562.pdf

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

DHS uses CTS for managing correspondence and tracking complaints, comments and requests for redress of privacy issues by the public, private businesses, Congress, or other public agencies. It assists DHS in its responsiveness to complaints received. System users may disclose information within CTS to authorized recipients within DHS to assist in the agency response to complaints, comments and requests for redress from those individuals or entities identified in Question 1.2.

CTS provides a gateway to information and applications, the ability to collaborate with other users to share ideas and resources, and allows the user to customize layout and presentation. CTS also provides users with the ability to manage correspondence and assigned actions to other individuals via an electronic mail system internal to CTS. Some cases require the use of a Social Security number or an Alien Registration Number. An example of a complaint that might include an Alien Registration Number would be a complaint about border control enforcement issues.

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

CTS has customized reporting features built into the system. These reports allow the Privacy Office to report on the number of privacy complaints, the categories of complaints, and the disposition of complaints. Reports will also include the component from which the complaint originated.

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

CTS 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.

The following controls ensure that information is handled in accordance with the described uses above:

- Implemented mandatory personnel security policies and procedures that require all personnel to be the subject of a favorable background investigation prior to being granted access to sensitive information systems;
- Required the completion of appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access;
- Employed a formal sanctions process for personnel failing to comply with established information security policies and procedures;

- Controlled physical access to information system devices that display information to prevent unauthorized individuals from observing the display output;
- Employed role-based access controls within CTS and limits access to selected groups for prescribed functions;
- Required that access to the information within ECT be limited to authorized personnel by implementing record level security on specifically identified case folders, thereby restricting access to those files; and
- Provided initial and follow-on security awareness education for each individual with access to CTS.

Section 3.0 Retention

3.1 What information is retained?

The data described in Section 1.1 is retained by CTS. CTS also maintains a record of correspondence between the Privacy Office and the complainant.

3.2 How long is information retained?

The draft DHS Headquarters Office "Correspondence Tracking and Management" Records Schedule defines the retention period for records within CTS.

Source records are deleted when data is entered into the database and verified, or when the file is no longer required to serve as a back-up to data in CTS.

E-mail records are destroyed after they are copied into a recordkeeping system. Records of telephone communications, including message registers and logs, are deleted six months after creation.

Files related to complaints are destroyed three months after receipt. These files include complaint letters and responses to those letters. This retention period does not include files on the basis of which investigations were made or administrative action taken. It also does not apply to records incorporated into personnel records.

Files related to the acknowledgement of complaints are maintained for three months. These files include letters, e-mails, and records of telephone calls used to inform an individual that the Privacy Office received his or her complaint.

Communications related to redress are maintained for seven years after a final determination is made regarding the case.

Contact information from the submitter is maintained for seven years after a case is closed or seven years from the end of the calendar year in which the complaint is submitted. The longer time period of these two is always used.

CTS generates some standard reports such as: reports that summarize pending workload; preparer workgroup statistics; and the status of suspense actions. These reports are generated on an ad hoc basis and are considered temporary. These reports are destroyed when no longer needed for current agency use.

AILA InfoNet Doc. No. 09080562.pdf

CTS system documentation, system and file specifications, codebooks, record layouts, user manuals, and final reports, regardless of medium are considered temporary records. They are maintained for the life of the system (until the system is upgraded and new documentation is generated). These documents are destroyed three years after their supersession or obsolescence.

Case folders containing correspondence or records deemed permanent by the Executive Secretary will be transferred to the National Archives after seven years of inactivity.

Finally, any electronic record created to serve as a substitute for a hard copy record maintains the same retention schedule as that hard copy record.

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

No. DHS CTS is working to develop a schedule to cover records about individuals utilizing the redress process, which it will submit to NARA for review and approval. The retention periods described in Section 3.2 reflect General Records Schedules (GRS) published by the National Archives Records Administration (NARA). A finalized NARA Schedule will contain these retention periods.

Until a retention schedule is submitted and approved by NARA, no records collected for the redress process will be destroyed.

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

The longer a system retains information, the longer it needs to secure the information and assure its accuracy. A system must have risk mitigation plans that respond to these security and accuracy risks. With CTS, unsecured information can lead to the loss or theft of PII. Harms that result from the loss or theft of PII include identity theft, blackmail, and other harms. Inaccurate data can cause errors in the correspondence process. These inaccuracies can slow the correspondence process or misroute important letters, e-mails, or phone calls. Security and accuracy issues can also lead to complaints reaching the public. Once in the public space, a complaint can cause harm or embarrassment to the person/group who sent it to the Privacy Office.

Section 8.0 details the security measures used to safeguard the information. These security measures protect information throughout its lifecycle.

To further mitigate these risks, the Privacy Office regularly reviews the case files to determine their status as a temporary or permanent record. These regular reviews reduce the amount and type of information being maintained. These records may include PII, such as the SSN, if required for identification. The case files, with PII, may be transferred to the National Archives to maintain the integrity of the Case File. These regular reviews also allow the Privacy Office to ensure that the system complies with the NARA schedule that governs this data collection.

AILA InfoNet Doc. No. 09080562.pdf

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 information contained within CTS may be shared with any of the Executive Secretariats for the DHS components and offices listed below:

- Office of the Secretary
- Citizenship and Immigration Services
- Citizenship and Immigration Services Ombudsman
- Office for Civil Rights and Civil Liberties
- United States Coast Guard
- Counter-Narcotics Enforcement
- Labor Relations Board
- Office of Legislative and Intergovernmental Affairs
- Management
- Military Advisor's Office
- Office of the General Counsel
- Recovery and Rebuilding of the Gulf Coast Region
- United States Immigration and Customs Enforcement
- Office of Inspector General
- Office of Intelligence and Analysis
- Office of Policy
- National Protection Program Directorate
- Office of Public Affairs
- Science and Technology
- Screening Coordination Office
- United States Customs and Border Protection
- Domestic Nuclear Detection Office Executive Secretariat
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Chief Financial Officer
- Transportation Security Administration
- White House Liaison
- US-VISIT
- United States Secret Service
- Office of Operations Coordination

The information contained in CTS will be shared only if a complaint is specific to a DHS component. In this case, only information associated with that specific complaint will be shared. PII from the complaint may be suppressed or not shared if practicable.

4.2 How is the information transmitted or disclosed?

CTS maintains all information within a central, secured database. Documents are electronically routed inside the CTS system according to a pre-configured workflow template so that a defined business process will follow the same steps each time. Users connect to the CTS system using approved encryption techniques to protect data confidentiality.

If a complainant requires the assistance of another DHS component, CTS Privacy Office users will forward information about the individual's complaints, comments, and requests for redress to that component via DHS e-mail.

AILA InfoNet Doc. No. 09080562.pdf

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.

A risk to privacy from an application such as CTS arises from:

- The design enabling all users to search every workflow stored within CTS; and
- The ability of DHS personnel with CTS access to examine workflows for which they have no need to access or to commit other security policy violations exist with CTS as it does for all information systems where authorized users have the ability to read, write, or modify data.

To counter these risks:

- DHS has implemented record level security, a security technique that enables a user to control who specifically has access to a particular document or record in order to prevent other users from seeing the contents of a workflow retrieved via a CTS search. This limitation is in place because not all authorized CTS users have a "need to know" for all information in a particular workflow.
- DHS has implemented user access controls requiring positive user identification (ID) and authentication. Each CTS user is identified by a unique user ID, and their passwords must conform to DHS complexity requirements. (Password complexity refers to the mandatory use of a combination of text, numbers, and punctuation characters in a password that cannot be easily guessed by a potential intruder.) Users connect to CTS via the web browser. The user has the certificate for the CTS server stored on their workstation. This certificate is used to identify and authenticate the CTS server and initiate an encrypted secure socket layer (SSL) session.
- DHS develops, disseminates, and periodically reviews and updates formal, documented access control policy that addresses purpose, scope, roles, responsibilities, and compliance, as well as formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
- The CTS system owner grants access based on a valid "need to know" that is determined by the users assigned official duties and intended system usage.
- DHS restricts access to the security functions (e.g., audit trails, access control lists, and password files) to system administrators, database administrators, and the information system security officer (ISSO). An audit trail records all activity associated with these user groups.
- The CTS system enforces assigned authorizations for controlling the flow of information within the system in accordance with applicable policy. Data integrity is safeguarded by role-based access and privileges.
- The CTS system automatically terminates interactive sessions within a DHS mandated time-out period of inactivity.
- The CTS system audit trails and system logs record the activities of all users. Suspected security incidents involving unauthorized access (or attempted unauthorized access) are recorded, reported to the CTS ISSO, and investigated immediately.

AILA InfoNet Doc. No. 09080562.pdf

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The information collected and retained in CTS may need to be shared under certain circumstances with other federal agencies when necessary to address an individual's redress request. CTS may share information provided by an individual seeking redress with other federal departments and programs in order to determine the appropriate response to the redress request. For example, CTS may exchange information with DOJ where the complaint has information that pertains to pending litigation.

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.

The sharing of PII is compatible with the original collection and covered by routine uses in DHS/ALL-028 Complaints Tracking System SORN. These routine uses include:

(1) Disclosure of information to contractors, interns, or service providers, who are not DHS employees, but have an agency relationship with DHS to accomplish DHS responsibilities. This routine use permits DHS to contract for services to augment that which is accomplished by DHS employees. This disclosure occurs only in the context of the operation of DHS TRIP or the DHS component redress programs;

(2) Sharing of information when there appears to be a specific violation or potential violation of law, or identified threat or potential threat to national or international security, such as criminal or terrorist activities, based on individual records in this system. This routine use operates only in the situation when the information indicates some sort of violation of law or threat, such as when someone would provide false or fraudulent documents;

(3) Sharing of information with the NARA for proper handling of government records;

(4) Sharing of information when relevant to litigation associated with the Federal government; and

(5) Sharing of information to protect the individual who is the subject of the record from the harm of identity theft in the case of a data breach affecting this system.

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

Any information shared with agencies outside of DHS are required to secure the information

(whether it is PII or classified) properly.

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

External sharing can increase the risk of theft or loss of PII. This increase results from inconsistencies in data security plans between entities and the creation of additional records. Different entities may have different encryption regulations, physical security protections, and other data security measures. External sharing also can result in the creation of additional paper or electronic records. These records could include printed e-mails and notes taken from phone conversations. Using the following measures, CTS mitigates these external sharing risks.

Any correspondence transmitted using the Internet mail agent is documented in an audit trail. This audit trail maintains a record of the individual sending the correspondence, what documents, if any, were transmitted, and the destination of the transmission.

To mitigate an inadvertent release of PII, other information systems outside of DHS do not have direct access to CTS. Other agencies will not have access to the information stored in CTS unless that information is included in official correspondence to or from DHS; is related to the inquiry by that agency; involves the redirection of an individual's mail to the agency responsible handling the requested information; or involves an official response by DHS to the inquiring agency.

Only the minimum amount of information necessary is shared with outside agencies, depending upon the reason for sharing this information as authorized by the Executive Secretary or required by statue. For example, if a threat to the President is received, that correspondence will be provided to the appropriate law enforcement agency.

If an inquiry is received from a member of Congress, the reply may include PII depending upon the topic of the original correspondence, and the reply generated by the appropriate DHS office

Section 6.0 Notice

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

Notice is provided in the DHS/ALL-028 Complaints Tracking System SORN as well as in this PIA. The Privacy Office also posts a Privacy Policy on the bottom of the webpage with its contact information. These features notify the submitter of the way that the Privacy Office uses their personal information.

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

The general public is not obligated in any way to submit correspondence to DHS. Individuals have an inherent right to decline sending information to the Privacy Office.

AILA InfoNet Doc. No. 09080562.pdf

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

An individual's right to consent to particular uses of the information is inherent in the nature of CTS. An individual's mail is tracked and answered. The information provided is not disclosed beyond those personnel inside of the Privacy Office with a valid need to know to respond to the individual's complaint, comment or request for redress. An individual's mail numeric reporting by correspondence topic is provided to DHS leadership as a matter of information on volume and current issues.

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.

The Privacy Office provides contact information on its webpage. Individuals/entities can use this contact information to submit complaints, comments and requests for redress, however, the Privacy Office does not specifically solicit this information. Individuals/entities voluntarily submit this information. Individuals/entities can reasonably assume that the Privacy Office will use their contact information to respond to the complaints, comments and requests for redress. This process ensures that individuals/entities are aware of the collection of personal information.

Additionally, the Privacy Office provides a Privacy Policy link at the bottom of its webpage. This Privacy Policy describes the uses of personal information if an individual/entity sends it the Privacy Office in the following paragraph titled "If You Send Us Personal Information" found in the Privacy Policy:

> If you choose to provide us with personal information -- like filling out a Contact Us form with personal information and submitting it to us through the Web site -- we use that information to respond to your message and to help us get you the information you have requested. We only share the information you give us with another government agency if your inquiry relates to that agency, or as otherwise required by law. We never create individual profiles or give it to any private organizations. The Department of Homeland Security never collects information for commercial marketing.

This paragraph adds an additional layer of notice available to the individual/entity beyond the initial notice inherent in the complaint, comment and request for redress processes.

Section 7.0 Access, Redress and Correction

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

Individuals may gain access to their own information by submitting a Privacy Act (PA)/Freedom of Information Act (FOIA) request. Individuals may also contact the DHS Privacy Office with CTS PA/FOIA requests at the following: OIA/PA D-3, The Privacy Office U.S. Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-0550, Washington, DC 20528-0550.

AILA InfoNet Doc. No. 09080562.pdf

7.2 What are the procedures for correcting inaccurate or erroneous information?

Should an inaccuracy be discovered during the resolution of the case file, the organization tasked with resolving the case file may contact the originating submitter.

Additionally, CTS has data integrity checks built into the system. The submitter's address is verified against the U.S. Post Office. Mistakes in the spelling of the writer's name, prefix, and/or suffix, etc. can be corrected inside of CTS by any authorized user. Manual requests for corrections can be submitted to The Privacy Office, US Department of Homeland Security, Washington, DC 20528-0550.

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

Individuals may be notified of the procedures for correcting their information within CTS by the DHS Correspondence Department who will notify the writer if additional information is required. The DHS/ALL-028 Complaints Tracking System SORN and this PIA also outline the procedures for correcting information.

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

Redress is provided.

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

Any risk that the individual may not correct his information is mitigated by allowing individuals to request access or amendment of their records at any time. Individuals may access their information by using the PA/FOIA process outlined on the DHS web site at www.dhs.gov/privacy or by contacting The Privacy Office directly.

Section 8.0 Technical Access and Security

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

Only a limited number of Privacy Office personnel have access to the database through unique user names and passwords. The System Owner and the Office of the Chief Information Officer maintain and manage a list of authorized CTS users.

The CTS supervisor may assign specific viewing rights to other CTS users within the workflow. For example, if the CTS supervisor receives correspondence from an individual, he or she may choose to enable

successive individuals to only view the document, but not to modify or delete the contents. When doing so, any access rights to the document must be specifically assigned to an individual CTS user who receives the action.

8.2 Will Department contractors have access to the system?

Contractors serve in support roles to operate and maintain the CTS information system. Contractors serve in the data entry and processing capacity. As a condition of their contracted service with DHS, all contractors:

- Sign a Non-Disclosure Agreement;
- Undergo a background investigation;
- Sign and acknowledge rules of behavior; and
- Sign and submit an access request form.

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

All users of DHS information systems are expected to adhere to DHS Management Directive 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. Users are trained on how to apply record level security to their work and when the application may be appropriate.

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

Enterprise Correspondence Tracking System (ECT) received an Authority to Operate (ATO) from the Chief Information Security Officer (CISO) on August 31, 2006. This ATO reflects that fact that ECT has met the requirements for Certification and Accreditation under FISMA to the satisfaction of CISO and Chief Information Officer. CTS is a subsystem of ECT and uses this ATO.

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

DHS has implemented role-based security measures within CTS that limit access to specific types of correspondence based upon security policy. Established workflow templates provide rules for routing correspondence to its proper designation. CTS tracks all changes to a case folder. There is a complete audit trail that records all user modifications and routing actions of records within CTS. The monitoring, testing, and the evaluation of the security controls to ensure that the implemented controls continue to work properly, safeguarding the information is an annual requirement under FISMA. These technical controls are documented in the System Security Plan. The testing of these controls will be documented in the Security Assessment. Both of these documents contain sensitive information and are not releasable to the public.

AILA InfoNet Doc. No. 09080562.pdf

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?

In any correspondence tracking system, there is a risk that malicious or inadvertent actions taken on a particular correspondence may not be traceable back to an individual. CTS mitigates this risk by auditing controls that track actions taken by a user on a case folder. This auditing feature maintains accountability of an action taken by an authorized user. Specific audit trails record the actions of all CTS users to include specific audit information (user ID, time/date, action, and event success/failure).

There is a risk with CTS of an authorized individual having more permissions than required to perform their job function. This risk exists when any new user account is created and is common vulnerability on modern information systems. To counter this risk, CTS supervisors are responsible for reviewing the CTS permission matrix to ensure that:

- individual users are only granted the permissions that they are authorized to hold and for which they have an authorized need; and
- there are no unauthorized individuals with access to CTS.

The risk of an unauthorized but cleared DHS employee from viewing material on CTS to which he or she is not authorized to view is mitigated by the use of session locks and process termination routines that will disable access to CTS after a set period of inactivity. After the session is terminated, the CTS user must reestablish the CTS session access using the appropriate identification and authentication procedures.

Furthermore, the ability exists within CTS to configure a case folder so that fields may be hidden and users may be prevented from modifying or deleting the contents of a field. A CTS user may also assign specific viewing rights to CTS users within the workflow. For example, a CTS user who receives correspondence from an individual may restrict the individuals who can view the people record, the workflow record or the documents attached to the workflow.

Section 9.0 Technology

9.1 What type of project is the program or system?

The CTS is a modification current commercial-off-the-shelf (COTS) product Intranet Quorum.

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

CTS is currently in the development stage. System developers are using a modification of the Intranet Quorum system as a basis for CTS. They are currently implementing specific reporting processes and access control procedures into the system.

AILA InfoNet Doc. No. 09080562.pdf

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

CTS used a privacy risk management process based on information life cycle analysis and information management principles as established by the National Institute of Standards and Technology (NIST) and DHS. Technical and programmatic design choices are informed by this approach, which analyzes proposed changes in terms of their life-cycle processes—collection, use and disclosure, processing, and retention and destruction—and the potential they may create for noncompliance with relevant statutes or regulations (the Privacy Act in particular) or for violations of the fair information practice principles. When analysis determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed.

Personal access and controls relating to PII include:

- User-ID and password;
- Record level security; and
- Automatic session timeout after a set period of inactivity.

In order to support privacy protections, CTS will only collect the minimum of personally identifiable information needed to process the redress inquiry. In addition, CTS uses an information technology infrastructure that will protect against inadvertent use of personally identifiable information not required by the government. Access to the system containing information collected for this program will be strictly controlled. Only employees and contractors with proper security credentials and passwords will have permission to access CTS.

Additionally, the record system will track access to electronic information. Access logs will be periodically reviewed. All DHS employees and assigned contractor staff receive privacy training on the use and disclosure of personal data. The procedures and policies in place are intended to ensure that no unauthorized access to records occurs and that operational safeguards are firmly in place to prevent system abuses.

Responsible Officials

Rose Bird

Director, Privacy Incidents and Inquiries

Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

AILA InfoNet Doc. No. 09080562.pdf