Privacy Impact Assessment

for the

Enterprise Correspondence Tracking System (ECT)

December 3, 2007

Contact Point
Huong Mai
Manager, Applications Branch
Office of the Chief Information Officer
Department of Homeland Security
(202) 447-0384

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

Abstract

The Executive Secretariat of the Department of Homeland Security (DHS) operates the Enterprise Correspondence Tracking (ECT) system. The ECT is a correspondence workflow management system that assists DHS in responding to inquiries from the public, other government agencies, and the private sector. Tens of thousands of pieces of correspondence ranging from official rulings, policy statements, testimony, or even thank you letters are processed annually by DHS. The Executive Secretariat conducted this privacy impact assessment because the ECT collects and uses personally identifiable information (PII).

Introduction

Tens of thousands of pieces of correspondence ranging from official rulings, policy statements, testimony, or thank you letters are generated by or pass through DHS annually. This correspondence requires analysis, storage, categorization, and coordinated responses. The Enterprise Correspondence Tracking System (ECT) is a workflow system that DHS utilizes to respond efficiently to inquiries from the public and other government and private-sector agencies. ECT provides the capacity to handle correspondence that requires analysis, storage, categorization, and response from DHS personnel. ECT is designed to manage correspondence tracking with pre-defined routing inside workflow templates.

ECT is a completely self-contained information system within DHS and does not interface with any other DHS or non-DHS information system other than the DHS local area network for printing. The Executive Secretariat is the business owner of ECT. This means that the Executive Secretariat is the user of ECT and is primarily responsible for the system. The DHS Office of the Chief Information Officer physically and technically secures the system.

Each DHS organization may use ECT, and share incoming and outgoing information contained within ECT for:

- Briefing material for senior leaders;
- Maintenance of official documents;
- Documenting and responding to citizen 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 ECT 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 address of the individual sending the correspondence or initiating a telephone call to the agency. Other information that may be obtained, if provided, includes the e-mail address, telephone number, business or organizational address, or the Social Security Number of the individual as voluntarily provided by the sender of the correspondence. The ECT record, created by the receipt of this correspondence, will also include the subject matter of the correspondence. If the correspondence received by DHS is paper-based, personnel from the Executive Secretariat's 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 a citizen or a person acting on behalf of a citizen. Correspondence may also be sent from a member of

Congress acting on behalf of a constituent. The Executive Secretariat receives a letter which is scanned and attached to a workflow initiated on the requestor's behalf. Data received or compiled is placed into an ECT 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, each individual topic is placed in its own case file for resolution.

Based on the content of the inquiry, the case file is assigned to a responsible component to provide a response to the writer, or content for a response from the Office of the Executive Secretariat. Once a response has been prepared and, if necessary, approved by counsel, the signed response letter is scanned and attached to the case file and the case file is closed.

A second common transaction in ECT is the distribution of draft materials (memorandums, opinions, etc) throughout DHS component leadership. For example, a memorandum may be circulated to each component's leadership requesting comments by a certain date. Comments are sent through ECT and are channeled back to the original drafter.

ECT provides the ability to collaborate with other DHS users to respond to the incoming correspondence. The ECT 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. ECT ensures a timely response to the correspondence and provides quality assurance tracking in order to prevent correspondences from becoming lost in the bureaucracy.

Section 1.0 Information Collected and Maintained

1.1 What information is to be collected?

Information collected in ECT is the information that resides within and is associated with the correspondence received by DHS, such as contact information provided in part or in whole by the submitter of the correspondence or an attorney acting at the behest of an individual. An authorized ECT user, with the appropriate permissions, is allowed to store, edit, or change the following information associated with a correspondence once it has been provided by the submitter:

- Prefix
- First Name
- Middle Name
- Last Name
- Suffix
- Title
- Organization
- Home Phone
- Business Phone
- Mobile Phone
- Fax
- Email
- URL

- Instant Messenger ID
- Country of Origin
- Date of Birth
- Social Security number or Alien Registration Number
- Gender

1.2 From whom is the information collected?

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:

- 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

1.3 Why is the information being collected?

This information is collected in order to facilitate efficient, accurate and timely handling of incoming correspondence between the individual and DHS. The Executive Secretariat utilizes ECT in order to maintain a record of the contact; enable follow-up correspondence from the agency, or to forward the correspondence to an action office. For example, ECT collects PII in order to track incoming correspondence and to provide DHS with the capabilities to respond to directly to the individual/entity. 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 ECT.

1.4 How is the information collected?

This information is entered into ECT by:

- Scanning original documents into the ECT record as an Adobe PDF file;
- Typing the information received (verbally) into the ECT record; and
- Copying information received electronically and pasting them into the appropriate fields in an electronic form which comprises a portion of the ECT record.

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

The collection of documents within ECT is governed by 5 U.S.C. § 301 (general agency powers for recordkeeping) and the Privacy Act of 1974, as amended (5 U.S.C. § 552a). 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.

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

The scope of the information collected in ECT 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 name of one or both correspondents, the Social Security Number or Alien Registration Number, for example, are only collected if they are voluntarily given and they are relevant to the request or correspondence at hand. If information is provided that is not relevant it is either not collected (e.g., information taken by phone and is not written down), or grayed out to users (if in electronic form) because the information is not relevant to the request in any way. These practices differ because many submissions arrive at DHS as unsolicited correspondence. If information is extraneous it is either grayed out within ECT data fields, or not entered at all.

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 ECT by using an approved encryption scheme. Remote access to ECT is monitored and controlled at all times. Section 8.0 of this PIA outlines the robust technical security measures enabled for ECT.

To protect the integrity of the information in ECT, ECT users can enable a record level security lock down feature within the workflow template. This feature allows the ECT user to lock down certain fields within a record. These fields, such as a Social Security number, may be hidden from view, or grayed out so successive ECT users may view the item but not change the contents. Users are trained on how to apply record level security to their work and when the application may be appropriate.

Section 2.0 Uses of the System and the Information

2.1 Describe all the uses of information.

DHS uses ECT for managing correspondence, tracking requests by the public, private businesses, Congress or other public agencies; and to assist DHS in its responsiveness to requests received. Information within ECT may be disclosed to authorized recipients within DHS to assist in the agency response to inquiries from those individuals or entities identified above in Question 1.2.

ECT 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. ECT also provides the ability to manage correspondence and assigned actions to other individuals via an electronic mail system internal to ECT. There are cases which require the use of a Social Security number or an Alien Registration Number. For example, within the Transportation Security Administration, these numbers may be used for the identification of individuals on the *Do Not Fly List*, or for investigations when that information is submitted by the individual. The Citizen and Immigration Service will use an individual's Social Security number or an Alien Registration Number for the administration of immigration and naturalization adjudication functions.

ECT enables the Executive Secretariat to coordinate DHS-wide review and analysis of policy initiatives, regulations, testimony, correspondence, memoranda, reports, and briefing material for the Secretary, Deputy Secretary, and Chief of Staff. ECT also enables the Executive Secretariat to maintain the record copy of correspondence for the Secretary, Deputy Secretary and the Chief of Staff.

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

ECT does not perform data mining activity. Information, generated by an external correspondence, that would normally be located in several locations, is placed in a single case folder to improve productivity. Co-locating similar information related to a correspondence doesn't necessarily bring about a conclusion that a user may not otherwise make, or necessarily identify previously unknown areas of concern.

Correspondence and other contacts with the DHS can be coded based on issue or other common characteristic for analysis and the collection of metrics, for example, the number of immigration issues received through ECT. DHS can report on the time and volume of correspondence received for the entire agency or at the component level.

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

The information received in the original correspondence is assumed to be true and accurate unless follow-up documentation or correspondence indicates otherwise. 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, ECT has data integrity checks built into the system. The address is verified against the US Post Office. Mistakes in the spelling of the writer's name, prefix, and/or suffix, etc. can be corrected inside of ECT by any authorized user. (An authorized user must be appointed by the component head, and approved by the Executive Secretary). Requests for corrections can be submitted to the DHS Correspondence Department, US Department of Homeland Security, Washington, DC 20528.

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

Risk to privacy arises primarily from internal threats to the information contained within the ECT database. These risks include:

- The unauthorized or inadvertent release of PII collected over the normal workflow process of managing, researching, and replying to the correspondences contained within a case file.
- Unauthorized browsing for information on specific or groups of information for non official purposes. This is possible since the design of the ECT software potentially allows all ECT users to search every case file and folder stored within ECT. ;
  To counter the risk of an unauthorized disclosure of Privacy data, DHS has:
- 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 ECT 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 ECT.

Section 3.0 Retention

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

The retention period for records within ECT is defined in the draft U.S. Department of Homeland Security Headquarters Office "Correspondence Tracking and Management" Records Schedule.

Temporary records are maintained in the ECT database after the case is closed. Case folders containing correspondence or records deemed permanent by the Executive Secretary will be transferred to the National Achieves after 10 years of inactivity.

ECT 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.

ECT 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 supercession or obsolescence.

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

The retention schedule is under review by NARA.

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

The Executive Secretariat regularly reviews the case files to determine their status as a temporary or permanent record. This regular review reduces the amount and type of information being maintained. These records may include PII such as the Social Security Number if required for identification. The case files, with PII, may be transferred to the National Archives to maintain the integrity of the Case File.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organizations is the information shared?

The information contained within ECT 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
- United States Customs and Border Protection
- Domestic Nuclear Detection Office
- Executive Secretariat
- Federal Emergency Management Agency
- Federal Law Enforcement Training Center
- Chief Financial Officer
- 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
- Labor Relations Board

- Office of Legislative and Intergovernmental Affairs
- Management
- Military Advisor's Office
- Office of Operations Coordination
- Office of Policy
- National Protection Program Directorate
- Chief Privacy Officer
- Office of Public Affairs
- Science and Technology
- Screening Coordination Office
- United States Secret Service
- Transportation Security Administration
- White House Liaison
- US-VISIT

The number of individuals in each component with access to ECT depends on the size of the component and the volume of correspondence received. For example the Citizenship and Immigration Services currently has 60 ECT users while the Office of the General Counsel may have only two ECT users. The Executive Secretary is the final decision maker on who may have access to ECT, and what their roles (e.g. access rights) and responsibilities are. Access to ECT is limited and not generally available to the population of DHS.

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

Each DHS organization may share incoming and outgoing information contained within ECT for:

- Briefing material for senior leaders;
- Maintenance of official documents;
- Documenting and responding to citizen mail sent to DHS;
- Maintaining internal coordination within DHS; and
- Enabling the appropriate handling, records management, and customer service actions generated by the correspondence.

4.3 How is the information transmitted or disclosed?

All ECT information is maintained within a central, secured database. Documents are electronically routed inside the ECT 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 ECT system using approved encryption techniques to protect data confidentiality.

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

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

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

To counter this risk:

- 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 an ECT search. This limitation is in place because not all authorized ECT 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 ECT 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 ECT via the web browser. The user has the certificate for the ECT server stored on their workstation. This certificate is used to identify and authenticate the ECT 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 ECT system owner grants access based on a valid "need-to-know" that is determined by the users assigned official duties and intended system usage.
- Access to the security functions (e.g., audit trails, access control lists, and password files) is restricted to system administrators, database administrators, and the information system security officer (ISSO). All activity associated with these user groups is recorded in the audit trail.
- The ECT 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 ECT system automatically terminates interactive sessions within a DHS mandated time-out period of inactivity.
- The ECT 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 ECT ISSO, and investigated immediately.

Section 5.0 External Sharing and Disclosure

5.1 With which external organizations is the information shared?

Access to the information inside ECT is not granted to external organizations, nor shared through ECT with external organizations. Information contained inside ECT may be shared as hard copy in response to an external organization's request for information, or electronically, using an Internet mail agent. This allows the efficient transfer of documents to individuals outside of the DHS ECT system for tasking, or to provide information to those that require it, but do not have ECT access. For example, threatening correspondence may be shared with law enforcement personnel as required by law, or an opinion may be

requested from an attorney at the Department of Justice. If information is to be shared with an outside agency, the sharing is done outside of ECT.

5.2 What information is shared and for what purpose?

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

5.3 How is the information transmitted or disclosed?

Information within ECT is not transmitted or disclosed unless an external correspondence, such as a letter to a citizen responding to an earlier inquiry by that citizen, or an external tasking or inquiry (as previously described) is made. This usually involves writing a letter in reply, or sending a reply via electronic mail, depending upon the appropriateness of the response as governed by the Executive Correspondence manual. No external electronic communication occurs through ECT.

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

ECT does not share information directly with any external agencies, i.e., no external electronic connection is established. For hard copy sharing, no MOU or agreement is in place with external agencies.

5.5 How is the shared information secured by the recipient?

Any information shared with agencies outside of DHS are required to secure the information (whether it is PII or classified) properly.

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

Any training conducted by external agencies is pursuant to those agencies' policies and procedures regarding information sharing and handling.

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

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 do not have direct access to ECT. Other agencies will not have access to the information stored in ECT unless that information is

included in official correspondence to or from DHS; is related to the inquiry by that agency; involves the redirection of citizen mail to the agency responsible handling the requested information; or involves an official response by DHS to the inquiring agency.

Section 6.0 Notice

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

Notice is provided in the System of Records Notice DHS/All 002 (69 FR 183, September 22, 2004) as well as in this PIA. No further notice is possible because DHS is not soliciting information from individuals; rather, individuals and other agencies make an initial request from DHS for information.

6.2 Do individuals have an 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 DHS.

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?

An individual's right to consent to particular uses of the information is inherent in the nature of ECT. Citizen mail is tracked and answered. The information provided is not disclosed beyond those personnel inside of DHS with a valid need to know to respond to the citizen's question/request. Citizen Mail numeric reporting by correspondence topic or by DHS component is provided to DHS leadership as a matter of information on volume and current issues.

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

A Privacy Act Notice to the individuals submitting information is not provided given that the source of information is voluntarily provided by the individual/entity or received from another government entity for action. Information is not submitted directly to ECT.

Section 7.0 Individual Access, Redress and Correction

7.1 What are the procedures which allow individuals to gain access to their own 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 ECT 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.

7.2 What are the procedures for correcting 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, ECT has data integrity checks built into the system. The address is verified against the US Post Office. Mistakes in the spelling of the writer's name, prefix, and/or suffix, etc. can be corrected inside of ECT by any authorized user. (An authorized user must be appointed by the component head, and approved by the Executive Secretary). Manual requests for corrections can be submitted to the DHS Correspondence Department, US Department of Homeland Security, Washington, DC 20528.

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 ECT by the DHS Correspondence Department who will notify the writer if additional information is required. The System of Records Notice DHS/All 002 (69 FR 183, September 22, 2004) and this privacy impact assessment also outline the procedures for correcting information.

7.4 If no redress is provided, are alternatives available?

Redress is provided.

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

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 DHS Correspondence Department directly.

Section 8.0 Technical Access and Security

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

Only authorized DHS users will have access to ECT. In order to become an authorized user, the system administrator must actively add an account. Non-ECT users may receive a tasking or work assignment via email sent from ECT to a DHS email account generated by an authorized ECT user.

8.2 Will contractors to DHS have access to the system?

Contractors serve in support rolls to operate and maintain the ECT 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;
- Sign and submit an access request form.

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

In accordance with DHS 4300A- *Sensitive Systems Handbook*, ECT uses role-based access control to assign privileges to users of the system. Access to the data will be determined through specified role-based permissions as authorized by the system owner. These role-based access controls limit access to the ECT system based upon the principal of least privilege. The principal of least privilege states that a user may only have the minimum privileges on an information system to perform their assigned tasks. Role-based access controls, as implemented for ECT, allocates resources and associated permissions to specific users or groups of users.

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

Access to ECT is limited. All users sign an access form requesting access to ECT. Users are selected by component management based upon job function. That selection must be approved by the ECT System Owner after the Information System Security Officer verifies that the potential user has the minimum security clearance required for the information contained within ECT. The System Owner and the Office of the Chief Information Officer maintain and manage a list of authorized ECT users.

An ECT user, functioning as a supervisor, may assign specific viewing rights to other ECT users within the workflow. For example, an ECT supervisor who receives correspondence from a citizen 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 ECT user who receives the action.

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

ECT provides a complete audit trail that records all users' modifications and routing of records within ECT.

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

DHS has implemented role-based security measures within ECT that limit access to specific types of correspondence based upon security policy. Established workflow templates provide rules for routing correspondence to its proper designation. ECT tracks all changes to a case folder. There is a complete audit trail that records all user modifications and routing actions of records within ECT. 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.

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

DHS components provide privacy training to users of all information systems to include ECT. 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.

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

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.

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

As with 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. This risk is mitigated within ECT by auditing controls whereby actions taken by a user on a case folder are tracked. This auditing feature maintains accountability of an action taken by an authorized user. Specific audit trails record the actions of all ECT users to include specific audit information (user ID, time/date, action, and event success/failure).

There is a risk with ECT 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, the Executive Secretary's representatives for ECT at each DHS component are responsible for reviewing the ECT 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 ECT.

The risk of an unauthorized but cleared DHS employee from viewing material on ECT 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 ECT after a set period of inactivity. After the session is terminated, the ECT user must reestablish the ECT session access using the appropriate identification and authentication procedures.

Furthermore, the ability exists within ECT 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. An ECT user may also assign specific viewing rights to ECT users within the workflow. For example, an ECT user who receives correspondence from a private citizen, 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 Was the system built from the ground up or purchased and installed?

The ECT is a commercial-off-the-shelf (COTS) product. Other organizations utilizing similar products include the White House, the Office of Management and Budget, the US Department of Justice, the General Services Administration, the US House of Representatives, the US Senate, and the Department of Veterans Affairs. The implementations of this product at other government agencies do not interface with ECT at DHS. The DHS ECT is installed in a secure data center.

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

Data integrity, privacy, and security were analyzed as part of the decision to implement ECT. 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.

ECT 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 fair information principles. When analysis

determines that privacy risks may exist, either alternative design choices or appropriate technical, physical, and/or procedural mitigations are developed.

9.3 What design choices were made to enhance privacy?

DHS has implemented strict access control measures for authorized users, record level security to protect designated case files, and an automatic timeout feature to prevent unauthorized browsing of the information contained within ECT. The Executive Secretary has made protecting the PII of the public one of his primary goals. Consequently, privacy considerations have been included in the design process of ECT from its inception.

Responsible Officials

Fred L. Schwien
Business Owner
The Executive Secretary
Office of the Executive Secretariat
US Department of Homeland Security
Washington, DC 20528
202-282-8221

Chandler Sirmons
ECT System Owner
US Department of Homeland Security
7th and D. St., SW
Washington, DC 20528
202-447-0285

Approval Signature Page

Original signed and on file with the DHS Privacy Office
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security