U.S. Department of Transportation

Privacy Impact Assessment

Office of the Secretary (OST)
Executive Secretariat (S-10)
Correspondence Control Management System (CCMS)

Responsible Official

Kristen Baldwin
Deputy Chief Information Officer
Office of the Chief Information Officer
DOTCIO@dot.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

12/8/2014

X Claire W. Barrett

Claire W. Barrett
Departmental Chief Privacy & Information Ass...
Signed by: CLAIRE W BARRETT

Executive Summary

The Correspondence Control Management System (CCMS) is an application used to control and manage official correspondence (mail, email, fax) to and from the U.S. Department of Transportation Secretary, Deputy Secretary, Chief of Staff, and Executive Secretariat to members of the public and others. CCMS automates key business functions and provides a document repository for storing the associated correspondence documents. CCMS is not publically available and does not solict information from the public however correspondence maintained in the system may include Personally Identifaiable Information (PII) of members of the public . The PII in CCMS managed correspondence is maintained solely for purposes of responding to requestor providing the information. The Office of the Secretary, Executive Secretariat (S-10) is the responsible organization for this system.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

Introduction & System Overview

The U.S. Department of Transportation developed the Correspondence Control Management System (CCMS) web-based application to reduce the time and labor required to manage Executive Correspondence; documents requiring the signature of the Secretary, the Deputy Secretary or a Department Administrator or Executive. The system is manaed by the Executive Secretariat and is used by Operating Administrations and other Offices within the Office of the Secretary engaged in Executive Correspondence. Through CCMS, authorized users may upload incoming correspondence and responses for review, review and comment/edit responses, As well as access the comments and edits of others.

CCMS does not require any PII from the public. However, the PII included in correspondence (mail, email, fax) sent to the Office of the Secretary are saved in CCMS. The PII provided is, as appropriate, used to develop the response to requestors and to facilitate correspondence with the requestors. Individuals whose information may be included in the system include those who write, or are referred in writing by a second party, to the Secretary, Deputy Secretary, Deputy Under Secretary, and their immediate offices. In addition, individuals who are the subject of an action requiring approval or action by one of the forenamed, such as appeal actions, training, awards, foreign travel, promotions, selections, grievances, and discipline.

Correspondence submitted by, or on behalf of, an individual, including resumes, letters of reference, etc. Responses to such correspondence. Staff recommendations on actions requiring approval or action by one of the forenamed.

Once signed by the apporopriate office, the entire correspondence package,is archived for future reference and review in accordance with approved Privacy Act notices and records disposition schedules.

The records maintained in CCMS are maintained by the Executive Secretariat on behalf of the Seretary,Deputy Secretary, Associate Deputy Secretary and Director of the Executive Secretariat and records maintained by the Special Assistants to the above officials.

The Secretary is the principal advisor to the President on national transportation affairs and is the principalrepresentative of the President's Administration in relations to Congress, other elements of Government, the transportation community and the public, with respect to transportation needs, policies, programs, resources and actions.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

CCMS does not require any Personally Identifaiable Information (PII) from the public. However, the PII voluntarily sent to the Office of the Secretary by mail, email, or fax are saved in CCMS for sole purpose of preparing a response and corresponding to the same party requesting answers.The Department provides general notice to the public of this records collection through its Privacy Act system of records notice (SORN), DOT/OST 041 – Correspondence Control Mail (CCM) , 70 FR 19554, April 11, 2000. which provides general notice to the public. Records created after January 1, 1974 are indexed by name of correspondent, referring individual, and subject category (e.g., ''employment'' for applicants). Records created prior to that date are indexed by name of correspondent .

In addition, this PIA, published on the Department's Privacy Program website (www.dot.gov/privacy) provides additional information on the privacy risks and mitigation strategies for the system.

Individual Participation and Redress

DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision making process regarding the collection and use of their PII and be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Under the provisions of the DOT's Privacy Act/Freedom of Information Act (FOIA) procedures, individuals may request searches of CCMS to determine if any records have been added that may pertain to them. The Freedom of Information Act (FOIA) is a Federal law that gives you the right to access any U.S. Department of Transportation (DOT) records unless DOT reasonably foresees that the release of the information in those records would harm an interest protected by one or more of the nine exemptions (such as classified national security, business proprietary, personal privacy, investigative documents) or release is prohibited by law. The DOT will review all Privacy Act requests on an individual basis and may waive exemptions if the release of information to the individual would not cause harm to applicable exemptions such as law enforcement or national security.

Notification procedure: Individuals wishing to know if their records appear in this system may inquire in writing to the system manager:

[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

Kristen Baldwin
1200 New Jersey Ave., SE
Washington, DC 20590
DOTCIO@dot.gov
(202) 366-9201

Included in the request must be the following:

Name,
Mailing address,
Phone number or email address,
A description of the records sought, such as the subject matter of the correspondence, addressessees of incoming correspondence, and date(s) and auhtor(s) of the response(s), and if possible, the location of the records.

Contesting record procedures: Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for why the records should be corrected. Requests should be submitted to the attention of the OST official responsible for the record at the address below:

Claire W. Barrett
Departmental Privacy Officer
1200 New Jersey Ave., SE
E31-312
Washington, DC 20590
Email: privacy@dot.gov
Fax: (202) 366-7024

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

CCMS is intregal to the operations of the Department in furtherance of its responsibilities to ensure a safe and reliable transportation system as authorized by 49 CFR. The purpose of the system is to provide history of correspondence addressed to and signed by the Secretary and Deputy Secretary of Transportation.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

CCMS only collects the information necessary to accomplish CCMS's stated purpose. CCMS does not require any Personally Identifaiable Information (PII) from the public. However, the PII voluntarily sent to the Office of the Secretary by mail, email, or fax are saved in CCMS for sole purpose of providing a response to the same

party requesting answers. CCMS also collects basic user contact information, security information, organizational information to establish authorization capacities. User contact information is used to identify the user and to send responses to letters or emails of the enquiring public. Responses are sent via postal mail or email.

CCMS records have significant permanent value to the public's understanding of the Department's operations. Records are maintained in accordance with approved NARA records disposition schedule, NC1-398-80-01.

Hard-copy records for 1967–1969 and duplicate microfilms for 1974–1989 are in the custody of National Archives and Records Administration, NARA. Records reside on the system as defined by DOT policies and as disk space on the system allows prior to conversion to Microfilm at an approved schedule by the DOT. Microfilm Records from 1990 through the present are retained in the Departmental headquarters building.

Computer microfilm records, and remote reader terminals, which permit access to the system records, are locked after office hours. During office hours computer is accessible only through terminals operated by, and under the surveillance of, authorized employees of the Executive Secretary.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

CCMS collects PII and this information is not used in any manner that is not specified in notices and is only used for the purposes collected. Consistent with the Privacy Act system of records notice for this system, data entered and stored in CCMS is used for communications and referral to the appropriate office within as well as outside the DOT for actions involving matters of law or regulation such as the Civil Service Commission for employee appeals, the Department of Justice in matters of law enforcement. Additionaly, the Department may share PII maintained in CCMS for purposes staded in the Department's Prefetory Statement of General Routine Uses.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Authorized users enter data via the application, and through the lifecycle of the documented correspondence from initial data entry through revisions of the draft as well as the final approval of the communications, data contained in the system undergoes several iterations of quality checks to ensure the data gathered is accurate.

In order to preserve data quality and integrity in the event that data in the system becomes corrupt or needs to be restored, differential system backups are done nightly and a full backup is performed weekly. The backups are transported to the alternate storage site on a weekly basis.

OST ensures that the collection, use, and maintenance of information collected for operating CCMS is relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, it is accurate, complete, and up-to-date.

The redress process described in the Individual Participation and Redress section is a mechanism to maintain and improve accuracy of information.

Security

DOT shall implement administrative, technical, and physical measures protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

CCMS takes appropriate security measures to safeguard PII and other sensitive data. CCMS applies DOT security standards, including but not limited to routine scans and monitoring, back-up activities, and background security checks of technical employees and contractors.

The DOT network has been designed for ultimate protection from internet attacks and there are protective devices strategically placed to prevent unwanted attacks from within the network. DOT has employed intrusion detection / prevention and firewall devices throughout the network to protect the network from many of the malicious codes.

Antivirus software is utilized for malicious code protection on systems where real-time scans on media are performed. A full system scan is performed on a weekly basis and virus definitions are automatically updated on all servers and all the clients.

Identification and Authentication (I&A) safeguards require each user to positively identify themselves by a unique user-identification and password prior to being granted system access. The I&A safeguards serve as the mechanism for associating a specific user with the recorded audit events. The user's password proves proper identity, enabling the trusted system to perform authentication. Access to sensitive information in CCMS requires a valid user identifier and password combination for all federal, state, and external users. E-authentication assurance level requirements dictate the authentication mechanisms that must be implemented for external users. All authorized users must read and sign a "Rules of Behavior" document prior to being granted access to CCMS.

All system components hosted by the DOT are located within restricted areas in the Southeast Federal Center (SFC) Headquarters Facility. Only employees designated by the Facility Security Officer have access to the computer room and switching closets. All maintenance personnel requiring access to the computer room or areas where related telecommunication devices are stored must sign in at the front desk first to gain access the facility. Maintenance personnel must sign-in to access the computer room and are required to be escorted at all times.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

OST is responsible for identifying, training, and holding OST employees and contractors accountable for adhering to DOT/OST privacy and security policies and regulations. OST will follow the Fair Information Practice Principles as best practices for the protection of PII associated with the CCMS. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records.

Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual Security and privacy awareness training as well as the DOT/OST Rules of Behavior. The OST Information System Security Officer and OST Privacy Officer will conduct periodic security and privacy compliance reviews of the CCMS consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems.

CCMS audit logs are periodically reviewed for any anomalies. The CCMS auditing system captures account maintenance and events. The System Owner, Information Systems Security Manager (ISSM) and/or Cybersecurity Management Center (CSMC) will determine the frequency and any changes which need to occur on the system due to the current threat environment. Only authorized system, database, and application administrators have rights sufficient to access audit logs based on their particular roles. The logged auditable events are adequate to support after-the-fact investigations based on previous requests made by the CSMC.

Responsible Official

Kristen Baldwin
Deputy Chief Information Officer
Office of the Chief Information Officer
Office of the Secretary
OCIO@dot.gov

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
Office of the Secretary
Privacy@dot.gov