Privacy Impact Assessment
for the

Digital Mail Pilot Program

June 18, 2010

Contact Point
Ronald Boatwright
Program Manager, Mail Management
Office of the Chief Administrative Officer
(202) 343-4220

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

Abstract

The Department of Homeland Security (DHS) Office of the Chief Administrative Officer (OCAO) plans to implement a Digital Mail Pilot Program for DHS Headquarters (HQ) and Components within the National Capital Region. The Digital Mail Pilot Program will give users the opportunity to receive their mail via email thereby improving DHS business processes and increasing security. The purpose of this Privacy Impact Assessment (PIA) is to demonstrate that the Digital Mail Pilot Program has considered and incorporated privacy protections of personally identifiable information (PII) that may be collected, used, disseminated, and maintained throughout the entire lifecycle of the program.

Overview

The purpose of the Digital Mail Pilot Program is to enable DHS to fulfill guidance in the DHS Management Directive (MD) 0590:

- Promote the most-cost effective use of mail service consistent with program requirements for timely, efficient, and responsive service through the use of internal mail, the U.S. Postal Service (USPS), express delivery services, and other carriers;
- Establish a Safe Mail Program to lower the risk of terrorist attack or criminal acts through the use of the mail system; and
- Establish a security program with the objective of assuring employee safety and facility survival.

The objective of the Digital Mail Pilot Program is to give pilot-designated users the opportunity to receive their incoming mail via email to determine whether business processes are improved so as to warrant full implementation within HQ and Components. To enable a smooth transition from DHS receiving hard copy mail to digital mail, HQ and Components will use change management processes to ensure that significant changes are implemented in an orderly, controlled, and systematic fashion to effect organizational change. A set of initial digital mail requirements will be tested and validated throughout the digital mail pilot program to further refine the requirements and increase the customer's awareness of the changes to the way mail will potentially be managed throughout DHS within the National Capital Region. A set of participants from HQ and each Component will participate in the pilot program on a voluntary basis.

The entire digital mail process occurs in the Consolidated Remote Delivery Site (CRDS), a building that has 24- hour security that has been approved by the DHS Office of the Chief Security Officer (OCSO). Once the inbound First Class Mail is released from a containment area after Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) testing, the First Class Mail will be sorted by mail stop using a mail sorting machine. The First Class Mail that contains the mail stops that are participating in the pilot will be separated from the rest of the mail and taken to the digitization room. At that point, the CRDS contractor opens the mail on three sides and removes the contents.

After screening and sorting of the mail that will be part of the pilot, a barcode is then applied to the envelope, and each page of the contents is placed behind the envelope. The barcode provides a tracking mechanism for each piece of scanned mail and ensures that only one envelope with its contents (batch) creates a Portable Document Format (PDF) image. Once the image is scanned, the addressee is verified again as a pilot participant by matching the mail stop, the name on the mail piece, and the name in the participant database that has been created. Once the

addressee is verified as a participant, the email is generated and sent to the addressee within the DHS network (DHS email address/computer to DHS email address/computer). PDF files associated with the pilot will be kept on a DHS-approved external hard drive for no longer than two business days; the external hard drive will be stored in a DHS OCSO approved safe when not in use. After two business days, the files will be deleted. Since digital mail uses email for transmission, the emails will be handled in accordance with the DHS OCIO policies on email. In addition, the hard copy will still be delivered to the addressee and will serve as the federal record. The type of information varies Sensitive Personally Identifiable Information (SPII)[1] may be transmitted. To date, 12.8 percent of the mail received as a part of this pilot contained SPII, and there have not been any reports of SPII-containing mail being sent to an incorrect individual. Due to the procedures that have been put in place, the error rate for this pilot will remain at less than one percent.

Section 1.0 Characterization of the Information

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

The Digital Mail Pilot database will collect information related to federal personnel who are participating in the pilot, which includes: names, work telephone numbers, and work e-mail addresses. The pilot will also disseminate information that is received in the mail to the intended addressee or designated recipient; this mail will be retrieved by a barcode placed on each envelope.

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

The information for the database will come from DHS employees that are voluntarily participating. The information that will be disseminated within the DHS network can come from a variety of sources which include other government agencies, businesses, and the public.

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

Collection and dissemination of the content in the mail is intended to reduce the costs of managing and storing paper, improve business processes within DHS, and reduce the risks associated with mail threats, such as anthrax, to DHS employees. Information for the database is being collected to verify that the addressee is a pilot participant.

1.4 How is the information collected?

The information is received via mail that is sent to DHS.

1.5 How will the information be checked for accuracy?

The DHS Global Address Listing (GAL) and a database of participants are the sources of information where addressee names, e-mail addresses, and mail stops will be verified for the purpose of the Digital Mail Pilot Program. The participant database will not allow a digitized piece of mail to be sent to a non-participant. If the addressee is not a pilot participant, which can immediately be determined by the mail stop, only the hard copy will be delivered to the addressee just as regular mail is normally delivered.

[1] Examples of Sensitive PII include Social Security number or alien registration number.

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

The Digital Mail Pilot will handle information that the Consolidated Remote Delivery Site (CRDS) Program has already been authorized to disseminate on behalf of offices throughout DHS per 5 U.S.C § 301 and MD 0590.

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

A privacy risk presented by the digitizing of mail is that more information will be collected than is necessary to distribute mail. This risk is mitigated by the limited information collected (names, work telephone numbers, and work e-mail addresses) from participants in order to disseminate the mail to the intended recipient. Further, after the hard copy mail is digitized, it will not be maintained, but rather is delivered to the addressee in the same manner as other First Class Mail.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

Collection and dissemination of the content in the mail is intended to improve business processes within DHS and reduce the risks associated with mail threats, such as anthrax, to DHS employees. Information for the database is being collected to verify that the addressee is a pilot participant.

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

The DHS GAL and the participant database will be used to verify the addressees' e-mail addresses. The only data that will be produced/collected pertains to the volume of incoming First Class Mail.

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

Information that another agency, commercial entity, or the public sends in the mail to DHS can be transmitted to the addressee, just as the hard copy would be.

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.

There is a risk of unauthorized access and that people other than the intended recipient will use the information in that a third party contractor is opening the mail. This risk is mitigated by the following controls:

1. Limiting access to a limited number of DHS Entry on Duty (EOD) approved contractors supporting the Digital Mail Pilot;

2. Limiting the retention of PDF documents on the external hard drive to two business days;
3. Maintaining camera surveillance in the digitization room; and
4. Limiting retrieval of mail by barcode.

Section 3.0 Retention

3.1 What information is retained?

The electronic version of each digitized piece of mail will be retained for a maximum of two business days in the CRDS. The electronic version will be deleted from the external hard drive within two business days. Since digital mail uses email for transmission, the emails will be handled in accordance with the DHS OCIO policies on email. After the recipients receive their digitized mail, they will receive the hard copy letter in the mail.

3.2 How long is information retained?

The electronic version will be deleted from the DHS-approved external hard drive within two business days.

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

The hard copy will serve as the federal record. As a result, the retention schedule that was previously used for specific content of each piece of mail will be used by the addressee. The specific retention schedule depends on the category of information into which the mail falls. Since digital mail uses email for transmission, the emails will be handled in accordance with the DHS OCIO policies on email.

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 risk that the digitized mail may be retained for a longer period than is necessary is mitigated by the storage limitation of two business days. Risks associated with the hard copy letter are mitigated by the fact that the hard copy document is mailed to the recipient immediately upon successful scanning at the CRDS.

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?

Information will be shared with the DHS participants who are the intended recipients of the mail.

4.2 How is the information transmitted or disclosed?

Digitized mail will be sent by e-mail as a PDF attachment using the DHS network (DHS e-mail account/computer to a DHS e-mail account/computer).

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.

There is the risk of digitized mail being sent to the wrong recipient. The Digital Mail Team will mitigate the risks by:

1. Verifying the recipient's name and identity in the DHS GAL and the participant database prior to sending the digitized mail;
2. Providing directions in each email in the event that the email was sent to the wrong individual; and
3. Limiting dissemination of e-mails from the contractor to the addressee (or designated representative) to within the DHS network (DHS email address/computer to DHS email address/computer); and

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 in the Digital Mail Pilot Program is not shared with any external organizations, except for contractors that work in support of DHS.

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 information in the Digital Mail Pilot Program is not shared with any external organizations, except for contractors that work in support of DHS.

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

Pilot information is not shared outside of the Department.

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

The information in the Digital Mail Pilot Program is not shared with any external organizations.

Section 6.0 Notice

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

The participants of the pilot (addressees) are participating voluntarily and have agreed to have their mail digitized. Official mail is considered to be property of the government, and the proper measures are being taken to safeguard the information. Notice is also provided through this PIA.

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

Addressees are participating voluntarily and have agreed to have their mail digitized.

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

The mail will be handled and used in the same way as it has been previously. The only change is the internal delivery method.

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.

Notice that mail will be read and digitized is provided at the time the individuals agree to participate in this pilot program as well as through this PIA.

Section 7.0 Access, Redress and Correction

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

For the purposes of the participant database, individuals can access their information on the DHS GAL or provide an update to the program office. Directions are issued by the DHS office with which the participant is already working. The pilot does not change that process in any way.

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

Participants can update their profile to reflect updated information on the DHS GAL or provide an update to the program office. External mailers can send mail to the office with their corrected information, just as they do with the mail already.

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

Directions are issued by the DHS office with which the participant is already working. The pilot does not change that process in any way.

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

Not applicable.

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

This pilot program does not change the procedures for access and correction of incorrect mailings.

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?

There will be a list of contractors at the facility that handle the receipt and scanning of mail. CRDS contractors have signed a Non-Disclosure Agreement. There is also a separate list of documented pilot participants (DHS employees).

8.2 Will Department contractors have access to the system?

Yes, contractors who have a DHS e-mail account/computer and are participants in the pilot will receive digitized mail. CRDS contractors will digitize and transmit the emails from a DHS computer at the CRDS, which is a facility that has 24-hour security, including camera surveillance, and has been approved by the DHS OCSO.

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

A Town Hall meeting will be held in preparation for the pilot where privacy protection, such as how the contractor is safeguarding SPII, will be discussed briefly. The contractors also receive mandatory training as part of the contract Performance of Work Statement (PWS).

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

Certification and Accreditation on all DHS laptop computers has been completed by the DHS OCIO.

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

In order to prevent the misuse of data, this pilot has limited the dissemination of e-mails from the contractor to the addressee (or designated representative) to within the DHS network

(DHS email address/computer to DHS email address/computer), and has the capability to audit/track emails in the event that an addressee improperly forwarded an email.

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?

The Digital Mail Pilot Program uses the DHS email network. No new systems will be developed or implemented for the pilot. There is more of an audit capability associated with digital mail than there is with regular mail. For example, a hard copy piece of mail could be given to someone that should not have it without any proof or evidence. Since the Digital Mail Pilot Program uses email, the capability to track the forwarding of messages exists.

Section 9.0 Technology

9.1 What type of project is the program or system?

The Digital Mail Pilot Program is a pilot.

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

The pilot is basic research to determine whether DHS can move forward with the full implementation of digital mail. For the full implementation, OCIO has assigned Project # 09-083. A workflow diagram has been completed for the pilot.

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

The Digital Mail Pilot is using DHS-approved computers and storage devices.

Responsible Official

Ronald Boatwright
Program Manager, Mail Management
Office of the Chief Administrative Officer
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security