

Privacy Impact Assessment

Technology, Planning, Architecture, & E-Government

- Version: 1.1
- Date: April 14, 2011
- Prepared for: USDA OCIO TPA&E





Privacy Impact Assessment for the Proofpoint Email Archiving System

April 14, 2011

Contact Point

Charles McClam

**Deputy Chief Information Officer, Policy and Architecture
(202) 720-5862**

Reviewing Official

Alexei Rodriguez

**Vice President of Operations and Computer Security Officer
Proofpoint, Inc.
(408) 517-4710**

Abstract

Proofpoint, Inc. (Proofpoint) manages and operates the Proofpoint Email Archiving System (System) used by USDA email users. USDA email users include USDA employees and contractors. The System provides email archiving storage management for the USDA's email system which is hosted and operated by Microsoft Business Productivity Online Suite-Federal (BPOS-F). This PIA is being conducted to assess the risk associated with the personally identifiable information that is processed, stored and transmitted within the System.

Overview

The Proofpoint Email Archiving System is owned and operated by Proofpoint. The USDA has contracted with Proofpoint to provide an email archiving solution for their new email service that will be provided by Microsoft's BPOS-F. An email archiving appliance resides within the BPOS-F network that integrates with Microsoft Exchange email system. The archiving appliance encrypts a copy of all email messages and transfers them to the Proofpoint Email Archiving System located in the Proofpoint Network Data Centers located at Santa Clara, CA. and Atlanta, GA.

USDA email users will access their email system that will be hosted, operated and managed by Microsoft as part of their BPOS-F service. The email archiving appliance will also be hosted, operated, and managed by Microsoft to facilitate secure email archiving. The email archiving appliance integrates with Active Directory for unified login and access control management. The archiving appliance will integrate with Microsoft Exchange to provide reliable, native format email message archiving. The archiving appliance will be accessed by USDA email users through a secure web interface and provide email archiving search and discovery, supervision, and enforcement. The archived email messages are stored in the Proofpoint Email Archiving System. The system will be used by Microsoft. USDA will not have access to the system or the contents. The system is part of a managed service offering in which USDA will receive services, but will not have access to the information or the system itself.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

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

Data that is archived in the system include name and email address of any individuals who send or receive email through the USDA's BPOS-F email messaging system. In addition any other information that is deemed to be PII and is contained within a USDA email message will be archived within the application. Examples of the type of information that may be contained within an email message may include; the sender or recipient's name, email address, phone number, mailing address, as well as the content of the email message and the content of any email message attachment.

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

The sources would include all senders and recipients of email messages contained in the USDA email system.

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

The name and email address information of the USDA email users is collected to facilitate email message archiving. All other information (the sender or recipient's name, email address, phone number, mailing address, content of the email message and the content of any email message attachment) that is contained within the email message will also be collected.

1.4 How is the information collected?

The email archiving appliance will pull a copy of all email messages contained within the USDA email system, encrypt the copy of the email message, and send it to the Email Archiving System located in Santa Clara, CA. The Email Archiving System will then replicate a copy of all of the archived email messages from Proofpoint's primary data center located in Santa Clara, CA to their alternate data center located in Atlanta, GA.

1.5 How will the information be checked for accuracy?

Information collected from the email system is done automatically with no additional check for accuracy.

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

Departmental Regulations (5 U.S.C 301) and *Records Management by Agency Heads; General Duties* (44 U.S.C. 3101). In addition, it is required under the Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Guidance can be found in Appendix III to OMB

Circular No. A-130 and NIST SP-800-30, Risk Management Guide for Information Technology Systems.

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

Risk: Information contained in emails could be accessed by unauthorized users.

Mitigation: Only authorized USDA email users have access to the System. All information collected and archived by the system is encrypted.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The Email Archiving System automatically archives USDA email and provides a single search point to retrieve the archived email.

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

The data is not analyzed. It is only archived and available for retrieval.

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

The Email Archiving System 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.

Only authorized USDA email users email messages are archived by the System. Only authorized USDA email users may access the information that is stored on the System. User access is determined by the USDA.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

The system can be configured to retain data for a specified period of time. This feature must be configured by the user and is dependent on the organization's data retention policy. The default data retention period is currently set to 2 months.

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

Information stored in the Email Archiving System is subject to the NARA General Records Schedule 20, item 14, *Electronic Mail Records*. The retention period will be configured and enforced per USDA policy in accordance with NARA.

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

Risk: Running out of storage space on the Email Archiving System.

Mitigation: Disk space is monitored continuously and additional storage capacity is added on a quarterly basis.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

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

Information is not shared with any other organization.

4.2 How is the information transmitted or disclosed?

Information is transmitted over a secure SSL connection from the email archiving appliance to the Email Archiving System. The information is not disclosed. Only authorized USDA email users can access the information.

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.**

Not applicable.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

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

Information is not shared with any other organization.

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 USDA.

Information is not shared outside of the USDA.

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

Information is not shared outside of the USDA.

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

Not applicable.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

Yes. All USDA email users are provided notice in the form of the login warning banner prior to accessing the USDA email system. As indicated in the Proofpoint SSP (control SC-14), Proofpoint does not allow public access to the system. Only authorized USDA employees/contractors have access to the email system.

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

Users may decline to provide information by not emailing to a USDA email address.

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

Users may decline to provide information by not emailing to a USDA email address.

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.

Risk: Individuals are not aware information is being collected about them.

Mitigation: The user is notified by the standard login warning banner

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

Individuals can access their information by logging into the email archiving appliance and accessing their archived email messages.

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

If the user's name or email address is incorrect they can notify the help desk and request the information be corrected. All other information that is stored in the Email Archiving System is information that is contained within the email message.

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

Each user is sent an e-mail notification when their USDA email address is created and their information is added to the email archiving appliance. The email informs them that their information is available and to contact their Help Desk for any discrepancies.

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

Information Redress is provided to users. Users may correct inaccurate or erroneous information contacting their Help Desk.

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

Risk: Inaccurate or erroneous information

Mitigation: Inaccurate or erroneous information can be corrected by contacting the USDA Help Desk.

Section 8.0 Technical Access and Security

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

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

Only authorized USDA email users may access the system. USDA has procedures and documentation for email user access and account creation.

8.2 Will Department contractors have access to the system?

Yes, if they have a USDA email account.

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

USDA mandates Annual Computer Security Awareness Training.

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

USDA has granted the Email Archiving System an Interim Authorization to Operate (IATO) on December 17, 2010.

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

Proofpoint has deployed auditing software and the logs are used to track unauthorized access attempts on the system. Also, all data is encrypted prior to being stored on the Email Archiving System.

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?

Risk: Non-authorized personnel obtaining access to the information.

Mitigation: The Email Archiving System is Internet Protocol and account restricted. Only authorized users and administrators may access the system. Also, all data is encrypted prior to being stored on the system.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

The Email Archiving System will provide the email archiving solution to the USDA's new email system.

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

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Not applicable. The Email Archiving System is not designed and utilized to engage with the public and is therefore not within the scope of the memorandums.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Not Applicable.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Not Applicable.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not Applicable.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not Applicable.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not Applicable.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not Applicable.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not Applicable.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require

either the creation or modification of a system of records notice (SORN)?

Not Applicable.

10.10 Does the system use web measurement and customization technology?

Not applicable.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Not applicable.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable.

Responsible Officials

Approval Signature

Alexei Rodriguez
Vice President of Operations / ISSO
Proofpoint, Inc.

Agency's Chief FOIA Officer
or Senior Official for Privacy
or Designated Privacy person