Privacy Impact Assessment

Microsoft Online Services Business Productivity Online Suite – Federal (BPOS-F)

Technology, Planning, Architecture, & E-Government

- Version: 3.0
- Date: April 13, 2011

Privacy Impact Assessment for the

Microsoft Online Services Business Productivity Online Suite – Federal (BPOS-F)

April 13, 2011

Contact Point
Mr. McClam
USDA/OCIO/
Cyber and Privacy Policy and Oversight
(410) 721-4111

Reviewing Official
Mr. Miller
Microsoft Online Services
Risk Management/Privacy
(425) 882-8080

Abstract

This Privacy Impact Assessment (PIA) addresses the Microsoft (MS) Business Productivity Online Suite - Federal (BPOS-F) system. The BPOS-F system provides enterprise class communications and collaboration server software, delivered as a service via subscription. The suite includes Microsoft Exchange Online, Microsoft SharePoint Online, and Office Communications Online. This PIA is being conducted based on the results of the PTA which indicated that a PIA was required.

Overview

The BPOS-F major application is a cloud computing-based subscription service offering from Microsoft. The application provides messaging and collaboration solutions including Microsoft Exchange Online, Microsoft SharePoint Online, and Office Communications Online. These online services are designed to provide the United States Department of Agriculture (USDA) with streamlined communication, high availability, comprehensive security, and simplified IT management.

Microsoft Exchange Online is a remotely hosted enterprise messaging solution managed by Microsoft. It provides a reliable, security-enhanced messaging environment with the flexibility to meet changing business needs.

Microsoft SharePoint Online is a managed collaboration solution that provides USDA employees with a way to efficiently work together, quickly locate organizational resources, search for experts and corporate information, manage content and workflow, and gain business insight to make better-informed decisions.

Microsoft Office Communications Online provides USDA with real-time communications services including instant messaging (IM) and Personal Computer (PC)-to-PC audio and video. The service also provides presence—meaning that users can see at a glance whether someone is available online and contact that person with a click using IM or a 1:1 audio conference.

Sending an email is an example transaction within the BPOS-F system. Initially, a user is assigned an account, which allows them to send e-mail. Microsoft does not analyze or filter the e-mail, and will attempt to deliver any e-mail a user prompts to be sent regardless of content. USDA must implement policy and training within the organization to ensure that their employees only send e-mail that conforms to their organization's policies and security requirements.

The BPOS-F system interfaces with the Proofpoint Email Archiving System, which provides e-mail archiving services for USDA accounts.

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?

In the course of running the service, Microsoft will collect and maintain three categories of information:

- Microsoft will ask USDA to provide authentication and address book personal information regarding employees and other end-users, such as e-mail address, name, work address, and telephone number. This populates Active Directory and the address book (Global Address List) and is required for authentication and the interactive features provided by the service.
- Information at USDA's discretion may be submitted to Microsoft through a support ticketing system, to assist in responding to support incidents or troubleshooting.
- In the course of providing the service, individual components of the Service, may collect the following information:
  - Microsoft Exchange Online - emails, email attachments, address book information, contact lists, and calendar information.
  - Microsoft SharePoint Online - files, documents, and contacts.
  - Office Communications Online – Voice over Internet Protocol and video communications, instant messages, real time desktop sharing, and files.

  All other information that may be stored on the BPOS-F system would be from USDA personnel through e-mail, SharePoint and other collaborative systems. This data is the sole responsibility of the USDA and its users.

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

Information will be provided by USDA administrators on USDA personnel that will utilize the BPOS-F system.

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

In order to support the services requested by USDA, BPOS-F collects information directly from USDA administrators to allow users to authenticate and communicate with the systems.

1.4 How is the information collected?

Information used by Microsoft to provide the services agreed to for USDA will be provided by USDA personnel through the BPOS-F Administration Center. Administrators and other support personnel would be the ones most likely to provide the initial data on users and updates will be managed thereafter using a ticketing system.

1.5 How will the information be checked for accuracy?

The accuracy of the data provided to Microsoft by USDA will be the sole responsibility of the USDA; Microsoft will not have the ability to verify the information.

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

Collection of information by USDA personnel will be governed by 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.

Information collected on the BPOS-F system may include (but not be limited to) full names, e-mail addresses and business addresses. The actual information collected will be from all fields held within the USDA Active Directory that is used to synchronize data with Microsoft; therefore the above fields are just examples. The information for USDA personnel will be protected using all moderate impact security controls required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3 for compliance with FISMA. The BPOS-F system is currently undergoing a full security authorization, and once completed this system will be fully authorized for use.

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.

Information collected by the BPOS-F system will be used solely for the purposes of providing services for USDA. The information collected will be used to populate Active Directory to name and identify all users of the system. This is done to provide audit and accountability functionality to the USDA and to provide general user management.

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

No tools will be used to analyze the privacy data collected by the system; the data will only be used to manage the service.

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

No commercial or publicly available data will be used unless the USDA makes this same information public on their own accord. It will not be provided publically unless authorized by the USDA.

2.4 <u>Privacy Impact Analysis</u>: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access controls are in place to protect the information system and its components. All systems will be segmented from the public and secured or hardened following Microsoft and NIST SP 800-53, Revision 3 guidance.

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?

Information will be maintained as long as users are actively using the system. If a user leaves USDA and no longer requires access, personnel from USDA will be required to disable and then remove the account as required.

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

Per USDA, this system does not qualify as an electronic records keeping system. Records will be maintained in accordance with guidance defined by the Client (US Government Agency that contracts for the use of the system).

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

Data is retained on users as they actively use the system, therefore the account information is required until the user no longer needs access. The active management of accounts will enable USDA to remove personnel that no longer require access and account management features provide for additional security including the ability to change passwords or re-create accounts if needed for security reasons.

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?

None. All information will stay within the accreditation boundary of the BPOS-F system.

4.2 How is the information transmitted or disclosed?

Information will be transmitted through an encrypted connection established between USDA and Microsoft.

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.

The same moderate impact NIST 800-53, Revision 3 security controls will be used for all components that hold data within the BPOS-F accreditation boundary.

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?

E-mail archiving services will be provided by Proofpoint Inc. via an encrypted connection between BPOS-F and the Proofpoint Email Archiving System on behalf of USDA.

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.

The information that is shared between BPOS-F and Proofpoint is compatible with the intent of the original collection – to create/maintain user accounts, in accordance with the contractual Statement of Work. It will be the responsibility of USDA to address any requirements for the information entered.

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

The connection from Microsoft to Proofpoint Inc. for e-mail archiving is encrypted and the moderate impact NIST 800-53, Revision 3 security controls are implemented and documented within each System Security Plan (SSP).

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

By having data transmitted to and stored at an additional facility the risk is increased, however the use of encryption decreases the potential compromise of data. This risk may be reduced further by USDA by limiting the private information that gets stored and using file level encryption for sensitive data.

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?

The exact mechanism may be slightly different for each government client. Notice is provided during the new account request process. The user must acknowledge the informed consent provisions with a signature during the new account request process.

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

The exact mechanism may be slightly different for each government client. Typically the agency employee, contractor, or stakeholder does not have the opportunity to decline to provide non-PII information. The information requested is required to assign and set up the user accounts. The user has the right to correct or update information at any time be sending an email request to the agency help desk.

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 exact mechanism may be slightly different for each government client. Generally, the requirement is for each account to be uniquely tied to an individual, all other information may be changed, updated or deleted by sending an email request to the agency help desk..

6.4 <u>Privacy Impact Analysis</u>: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The exact mechanism may be slightly different for each government client. The risk to the individual is very low. The user must acknowledge the informed consent provisions with a signature during the new account request process. The information collected is not considered to be PII and there is no perceived risk.

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?

Personnel information will be available for their review through the use of the internal address books maintained by USDA. The user may view their information by going into Outlook, select the "Search address book" icon then enter their name with last name first. Once located, the user must double click on his/her directory listing and their detailed information will appear.

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

The user has the right to correct or update information at any time by sending an email request to the Agency help desk. At the present time the user does not have the ability to update/correct their data directly, however, this feature will be available in the future.

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

During the new user request process users are informed of their right to correct or update information at any time by sending an email to the Agency help desk.

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

The user has the right to correct or update information at any time by sending an email to the Agency help desk.

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

There are no additional privacy risks associated with the redress.

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?

Access to the system by Microsoft personnel will be limited to administrative personnel in support of the service. The BPOS-F SSP details which groups have access to the various components of the system based on their relevant roles.

8.2 Will Department contractors have access to the system?

All personnel that have access to the system services will be established and controlled by USDA. Contractors for Microsoft may have access to the system for administrative purposes if a contractor is required in support of the service.

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

Microsoft provides security and awareness training to personnel managing the BPOS-F system on an annual basis. USDA will be responsible for training for their employees and contractors.

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

Certification and Accreditation activities are currently underway for the BPOS-F system, and are estimated to be completed in April 2011.

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

The BPOS-F system uses the moderate impact security controls from NIST SP 800-53 Revision 3 in establishing security mechanisms to protect the system. This includes border protection, auditing and alerting for tracking and monitoring events on the 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?

The information collected to support the use of the service is general information on users. The moderate impact NIST 800-53, Revision 3 security controls have been implemented on the system to protect the data within the BPOS-F accreditation boundary.

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?

BPOS-F is a suite of applications that provide e-mail and collaboration software in a secured managed hosting environment.

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

No. No known technology of the system would raise privacy concerns as the information collected is information from users (employees and contractors of USDA).

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"?

Yes.

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

This system does not use or interface with 3rd party websites.

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

None.

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

N/A

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?

N/A

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

N/A

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

N/A

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?

N/A

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)?

N/A

10.10 Does the system use web measurement and customization technology?

No, the system does not use any web measurement or customization technologies.

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

N/A

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.

N/A

Responsible Officials

Mr. Miller

Microsoft Online Services Risk Management/Privacy

Microsoft Corporation

Approval Signature

____

Mr. McClam
United States Department of Agriculture