MILLENNIUM
CHALLENGE CORPORATION
UNITED STATES OF AMERICA

Millennium Challenge Corporation
Privacy Impact Assessment
Box.com

February 22, 2022
Millennium Challenge Corporation
1099 Fourteenth Street N.W., Suite 700
Washington, DC 20005-3550

Point of Contact

Miguel G. Adams
Chief Information Security Officer and
Deputy Privacy Officer
Department of Administration and Finance
Millennium Challenge Corporation
(202) 521-3574

Authorizing Official

Christopher E. Ice
Acting Chief Information Officer and
Chief Privacy Officer
Department of Administration and Finance
Millennium Challenge Corporation
(202) 521-3716

Abstract

The Millennium Challenge Corporation (MCC) plans implement the Box Enterprise Cloud Content Collaboration Platform known as "MCC-Box". This platform provides a secure way to share files and improve collaboration with external users. Beyond file sharing, Box provides an enterprise content platform and safe workspace for internal and external teams to collaborate in a central workspace to create, edit, review, and share files and folders.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

A summary of laws, and regulations related to privacy include:

- Privacy Act of 1974, as amended, 5 U.S.C. § 552a
- E-Government Act of 2002 (Public Law 107-347)
- Federal Information Security Modernization Act of 2014 (Public Law 113-283)
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Memo M-99-18, Privacy Policies on Federal Web Sites
- OMB Memo M-03-22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
- OMB Memo M-10-23, Guidance for Agency Use of Third-Party Websites

Guidance on privacy issues can be found in the following publication:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing
- NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Office of Worker's Compensation Programs, Federal Employee' Compensation Act File (DOL/GOVT-1);

- Employee Transportation Facilitation (DOT/ALL-8);
- GSA/GOVT-2 Employment Under Commercial Activities Contracts (GSA/GOVT-2);
- Travel Charge Card Program (GSA/GOVT-3);
- GSA SmartPay Purchase Charge Card Program (GSA/GOVT-6);
- HSPD-2 USAccess (GSA/GOVT-7);
- Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records (OGE/GOVT-1);
- General Personnel Records (OPM/GOVT-1);
- Employee Medical File System Records (OPM/GOVT-10);

- Executive Branch Confidential Financial Disclosure Reports (OPM/GOVT-2);
- Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers (OPM/GOVT-3);
- Recruiting, Examining, and Placement Records (OPM/GOVT-5);
- Personnel Research and Test Validation Records (OPM/GOVT-6);
- Applicant Race, Sex, National Origin,, Disability Status Records (OPM/GOVT-7);
- File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals and Fair, Labor Standard Act (FLSA) Claims and Complaints (OPM/GOVT-9);
- OSC Complaint, Litigation, Political Activity and Disclosure Files (OSC/GOVT-1).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The records contained in this platform consist of non-recordkeeping copies and intermediary records covered under GRS 5: General Operations Support. Because the Box platform is not an authorized agency recordkeeping system, users are required to store recordkeeping copies of final or substantive content (both sent and received) in an approved agency recordkeeping system (such as SharePoint Online) within 20 days of creation or receipt. The copies stored in the Box platform are deleted 30 days from upload or creation.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

N/A

Section 2.0 Characterization of the Information

2.1 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

N/A

2.2 What are the sources of the information and how is the information collected for the project?

User collaboration content. The system will be used to transfer onboarding employment documentation to Human Resources (HR) and Domestic and International Security (DIS). Data will include sensitive personally identifiable information.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No

2.4 Discuss how accuracy of the data is ensured.

This system processes or transfers Privacy related Records between authorized parties or users. The system will only process and store temporary Privacy related Records for up to 30-days. Other processing of permanent Privacy related Records is outside the scope of this transfer system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Potential leak of social security number and other sensitive Personally Identifiable Information.

Mitigation: Temporary Records are uploaded to this transfer system from authorized Human Resource (HR) and Domestic and International Security (DIS) personnel. All data, including temporary Records, are automatically deleted after 30 days.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

MCC's Box will provide an environment for files to be shared and for transient files to be temporarily stored and deleted after 30 days. This platform enables users to invite team members to easily set up a workspace for individuals to share content in document libraries to collaborate on files.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how MCC plans to use such results.

No. This function is disabled.

3.3 Are there other Components with assigned roles and responsibilities within the

system?

Yes. There are numerous administrative roles as defined in our MCC's Governance Plan. Specifically administrative roles are as follows:

Admin Role	Capability for Box
Primary Admin	Primary Admins manage users and groups, view and edit all their organization's files and folders, log in to any user's account within their organization, edit settings for their organization, and run or access reports.
Co-Admin	Co-admins perform the same duties as the organization's Admin, but they cannot make changes to the Administrator's permissions or other Co-admins permissions.
Group Admin	Group Admins add existing users to their groups, create new users that will be assigned to their groups, and assign folder access to their groups. They can also run reports for their groups.

3.4 Privacy Impact Analysis: Related to the Uses of Information.

Privacy Risk: The information system is a transfer system that does not originate personally identifiable information (PII) (see Section 1.4). As such, the information system will not provide notice or consent to specific uses of information collected. Individuals should contact mccprivacy@mcc.gov if there is a need to provide consent on other MCC information systems.

Mitigation:

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Individuals using the system will see a Warning Banner when accessing MCC's Box.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

External users must acknowledge the Warning Banner before accessing the system.

4.3 Privacy Impact Analysis: Related to Notice Privacy

Privacy Risk: Only Temporary Records are processed in the system. Privacy Notice not required.

Mitigation:

Section 5.0 Data Retention

5.1 Explain how long and for what reason the information is retained.

Transitory content will be retained for 30 days. Content owners will determine the retention for collaboration content.

5.2 Privacy Impact Analysis: Related to Retention

The content stored in the Box platform is retained for 30 days so that it can be used and transferred to an appropriate recordkeeping system. Users are required to store recordkeeping copies of final or substantive content (both sent and received) in an approved agency recordkeeping system within 20 days of creation or receipt.

Privacy Risk: Temporary Records are deleted from the system.

Mitigation: To mitigate against records loss or alienation, users are required to move recordkeeping copies of final or substantive content (both sent and received) to an approved agency recordkeeping system within 20 days of creation or receipt.

Section 6.0 Information Sharing

6.1 Is information shared outside of MCC as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The solution will allow for collaboration, dissemination, and receipt of information between external parties and MCC staff. Box provides an environment for files to be shared and for transient files to be temporarily stored and deleted after 30 days. Box enables users to invite team members to easily set up a workspace for individuals to share content in document libraries to collaborate on files. With MCC's Box, invitations are sent to external users with a link and the external user must verify their email and authenticate to begin using the platform. Because the platform is used exclusively for transfer of, or short-term collaboration on, files, users must save recordkeeping copies of all final documents and substantive content to an approved MCC recordkeeping system.

6.3 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

N/A

6.3 Does the project place limitations on re-dissemination?

Collaboration content permissions are controlled by content owners.

6.4 Describe how the project maintains a record of any disclosures outside of the MCC**.**

N/A

Section 7.0 Redress

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

N/A

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

N/A

7.3 How does the project notify individuals about the procedures for correcting their information?

N/A

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

N/A

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

Agency employees attend privacy training annually.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Requests to access the system will be managed by our Service Desk via MCC's Service Catalog.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within MCC and outside?

N/A

Responsible Officials

Miguel G. Adams
Chief Information Security Officer and
Deputy Privacy Officer
Department of Administration and Finance
Millennium Challenge Corporation

MIGUEL G. ADAMS (affiliate)
Digitally signed by MIGUEL G. ADAMS (affiliate)
Date: 2022.02.22 14:27:52 -05'00'

Approving Signature

Christopher E. Ice
Acting Chief Information Officer and
Acting Chief Privacy Officer
Department of Administration and Finance
Millennium Challenge Corporation

CHRISTOPHER E. ICE (affiliate)
Digitally signed by CHRISTOPHER E. ICE (affiliate)
Date: 2022.02.25 10:18:38 -05'00'