Privacy Impact Assessment

MSPB Secure File Sharing System

May 11, 2021

Contact

D. Fon Muttamara
Chief Privacy Officer
Merit Systems Protection Board
1615 M Street, NW
Washington, D.C. 20419
privacy@mspb.gov

Abstract

The U.S. Merit Systems Protection Board (MSPB) uses Box, Inc.'s (Box) software as a service (SaaS) cloud platform. MSPB utilizes Box to securely share files between its offices at all locations, and between MSPB and external entities we authorize to access our records or information or to share their own records or information with us. MSPB conducted this Privacy Impact Assessment (PIA) because personally identifiable information (PII) is collected, used, and maintained by the agency through its use of Box. Additionally, records transferred through Box may include PII of MSPB employees, other Federal employees, and third parties. This PIA covers all MSPB offices' use of Box. Because of the varied nature of the agency's work and the different types of records submitted by appellants and agencies as part of MSPB's adjudicatory function, and records shared by or with MSPB in connection with its statutory function to conduct studies, records transferred using Box could conceivably include almost any type of unclassified PII.

Overview

MSPB implemented Box to provide a secure internal and external file sharing platform with key stakeholders and external entities (e.g., Federal agencies, notably the Department of Justice (DOJ), the Office of Special Counsel, the Office of Personnel Management (OPM) and the Equal Employment Opportunity Commission, Federal courts, appellants, court reporting services, and members of the public). Box can function across multiple platforms, including smartphones, tablets, and computers, whether inside or outside the MSPB network. At this time, MSPB utilizes Box as a transport infrastructure only, and MSPB has not designated Box as an official record-keeping system, document archival system, or document backup system.

Box underwent a rigorous security assessment and satisfies MSPB security requirements. Box enables end users to upload up to 32 gigabytes of most file types – documents, videos, photos, etc. – from a phone, tablet, or computer. Users can then access those files for a set number of days, as managed by MSPB's Box Administrator, from anywhere using Box on the Internet.

Box manages the hardware, software and cloud environment, and MSPB manages user access and security controls for our implementation of the Box platform. Box collects, maintains, and uses the following information from MSPB users: username and MSPB email address. MSPB collects email addresses, names, and passwords from non-MSPB users, which Box uses to authenticate access within the system. Box also maintains audit logs of user activity, such as logins, uploads, downloads, file name, Internet Protocol (IP) address, and browser.

MSPB data that passes through Box is Controlled Unclassified Information (CUI). Box is not authorized to process, store, or transmit classified data. Box has a Security Categorization of Moderate based on baselines established in Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems."

Because of the varied nature of MSPB's work and the different types of records submitted by appellants and agencies as part of MSPB appeals, and the type of personnel information transferred by Federal agencies to MSPB, the records and information shared via Box could conceivably include any type of CUI and PII. Therefore, it is not possible to list with certainty every type of information that users could potentially share via the system. MSPB will only share information within MSPB offices, between Federal agencies, and with external entities that have authority to access information maintained by the agency, or that have authority to share with MSPB, and that is shared to accomplish an authorized purpose.

Box collects metadata about shared files, such as the file creation date, but not the content of the files. Files made available to users via Box are deleted after 30 days through automated means, as determined by MSPB's Records Officer. This retention period is consistent with the National Archives and Records Administration's (NARA) General Records Schedule (GRS) 5.2: Intermediary Records, which states that the records are temporary and must be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Access to Box is restricted to MSPB employees and contractors and approved external entities. A user is granted an MSPB Box account only when approved by an MSPB office or program director. An external entity may be granted access to an MSPB Box account only after coordination between the office or program director, the Chief Information Officer, and the Chief Privacy Officer. While Box has the capability for mobile and off-network access, MSPB limits its employees from accessing or utilizing Box outside the MSPB network or on mobile devices. Information in Box must only be accessed on an MSPB-issued device or MSPB-specific interface, such as our Virtual Desktop Infrastructure, that has been provisioned by MSPB's Office of Information Resources Management. Box interfaces with MSPB's Active Directory Federation Services to authenticate internal users when Box is accessed from within the MSPB network. Once authenticated, internal Box users have access to files for which they have been granted explicit authorization. MSPB's Box Administrator can retrieve audit log information by a Box user's name or email address to view which records have been accessed.

Once an MSPB user is successfully authenticated and logs into Box, they may securely share files and records with any non-MSPB users by creating folders and granting access to them. Secure file sharing is accomplished through Box using designated shared folders or a password-enabled Uniform Resource Locator (URL or web address) created by the MSPB user and shared with the external user. All access to shared folders and files is controlled by the MSPB user. Non-MSPB users may send or retrieve records through Box by accessing the web address that an MSPB user sends to their email address. If an external user uploads a file into a folder designated by an MSPB user, a notification is sent to the MSPB user that a record has been uploaded.

Every file is encrypted in transit between the user (independent of platform) and Box data centers, compliant with FIPS standards. Once encrypted data reaches the Box network, files are encrypted when stored ("at rest") at all times using the 256-bit Advanced Encryption Standard (AES). All primary processing facilities are located within the United States.

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?

MSPB's use of Box is consistent with all applicable laws, regulations, and policies. MSPB's use of Box is primarily for secure file sharing in response to records requests under the Privacy Act of 1974 (Privacy Act) and the Freedom of Information Act (FOIA), and its statutory authority to conduct objective, non-partisan studies that assess and evaluate Federal merit systems policies, operations, and practices. Other instances of secure file sharing may be permitted in support of MSPB's adjudicatory function. The applicable laws, regulations, and policies, may include:

Statutes:

- 5 U.S.C. § 1204(a)(3)
- 5 U.S.C. § 552: FOIA.
- 5 U.S.C. § 552a: Privacy Act.

MSPB Regulations:

- 5 C.F.R. Part 1201: MSPB regulations on practices and procedures.
- 5 C.F. R. Part 1204: MSPB regulations implementing the FOIA.
- 5 C.F.R. Part 1205: MSPB regulations implementing the Privacy Act.

Office of Management and Budget (OMB) Memoranda:

- OMB M-10-06, Open Government Directive (December 8, 2009).
- OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, (June 25, 2010).

Presidential Directives and Executive Orders:

- Presidential Memorandum on Transparency and Open Government (Jan. 21, 2009).
- Executive Order 13571, Streamlining Service Delivery and Improving Customer Service (Apr. 27, 2011).
- Presidential Memorandum, Building a 21st Century Digital Government (May 23, 2012).

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

A SORN does not apply to Box because it is used only as a transport infrastructure and is not designed as an official record-keeping system, document archival system, or document backup system. A SORN may apply to files *transported* via Box depending on the content of the record. The SORN that is most commonly applicable is MSPB/GOVT - 1, Appeals and Case Records, 77 Fed. Reg. 65206 (Oct. 25, 2012). This SORN governs the information that MSPB collects during the adjudication process at MSPB and sets forth how MSPB maintains and protects appeals and case records, including any decisions rendered during adjudication. Another SORN that may apply is MSPB – 2, Surveys for Special Studies of the Civil Service, 86 Fed. Reg. 7307 (Jan. 27, 2021), which governs the information that MSPB collects in order to develop and administer surveys for special studies of the civil service, such as the Merit Principles Survey (MPS), and to evaluate and distribute the results of such surveys. Additionally, other published SORNs may apply depending on the nature of information in the shared document, and how the information is retrieved.

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

Authorized by the Federal Risk and Authorization Management Program (FedRAMP), the Box platform is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements and last underwent Certification and Accreditation on September 12, 2019. Box SaaS has a FedRAMP authorization at the Moderate Impact level. MSPB is leveraging Box's FedRAMP security assessment, which utilized a FedRAMP Third-Party Assessment Organization (or 3PAO) to perform an independent security assessment. Appropriate security controls have been identified and implemented by Box to protect against risks identified in the security risk assessment.

As part of MSPB's Box security controls, auditing procedures are in place to ensure compliance with security standards. Box provides reporting and an audit trail of account activities on both user and account files. Audit logs can only be accessed by MSPB's Box Administrator as needed to ensure compliance with security requirements. Box does not collect data on the content of the shared files. Box has application access controls that limit access to files and folders using role-based permissions to safeguard against unauthorized access, use, and disclosure of information. MSPB's Box Administrator can retrieve Box user account and audit log information by user account name or user account email address. Box has controls that ensure every user can only access his or her own files.

For MSPB employees, privacy awareness training and information security awareness training are required before accessing MSPB systems, including Box. MSPB contractors are required to receive privacy training from their company prior to beginning work on an MSPB contract. MSPB contractors who have access to the system are subject to the limitations and access controls provided in the contract, including obligations under the Privacy Act. Similarly, MSPB contractors are subject to privacy and information security provisions in their contracts. For external, non-MSPB users, a warning banner provides notification that any information transmitted through the system may be monitored, intercepted, searched, and seized by MSPB.

The following access and security controls are utilized to protect privacy and reduce the risk of unauthorized access and disclosure:

- Box has a Security Categorization of FISMA Moderate. The Box SaaS has a FedRAMP authorization at the Moderate Impact level. MSPB has assessed and implemented all applicable security controls that are MSPB's responsibility for a FISMA Moderate baseline.

- Box is accessible to MSPB employees and contractors who have been approved by an MSPB office or program director. Non-MSPB users from external entities have limited access privileges to MSPB-designated Box accounts and can only submit or retrieve files in the MSPB Box account specifically designated for their use by invitation to retrieve or upload records.

- Box has specific controls in place that ensure users can only access their own files. All files and folders are associated with a specific user. Each user has specific permissions associated with each file and folder, which specifies how a user may interact with a file. Every time a user attempts to access a file or folder, Box uses these permissions to verify that a user has explicit authorization to interact with the file. This process ensures that a user has access only to the files or folders to which the user is allowed, and that the user is restricted to the authorized type of interaction with the specific files or folders.

- In Box, every file is encrypted in transit with high-grade TLS encryption compliant with FIPS 140-2 standards. Once encrypted data reaches the Box network, files are 256-bit AES encrypted at rest at all times. All primary processing facilities are located within the United States. Box personnel can see the encrypted files and metadata about those files, such as the file creation date, but not the information within the files themselves.

- MSPB's Box policies only permit utilizing the system at the CUI level or lower.

- All MSPB users and contractors must complete privacy awareness training and information security awareness training annually or when they begin work on an MSPB contract, respectively, as well as read and agree to comply with MSPB's Information Technology (IT) Rules of Behavior (RoB) and Box Terms of Service prior to accessing Box and annually thereafter.

- Box is configured with automatic audit logging, which includes logging of Box Administrator activity. Further, logs are maintained separately from other system data to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Box audit logs can only be accessed in read-only mode by authorized MSPB's Box Administrator who has privileged access. Box audit logs are automatically monitored by the Box Security Incident and Event Management (SIEM) tool, which will flag any alteration of Box audit logs. MSPB's Box Administrator has exclusive access to the audit logs.

- MSPB has established breach response protocols to ensure appropriate handling and reporting of any suspected or confirmed breach.

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

Files made available to users via Box are deleted after 30 days through automated means, as determined by MSPB's Records Officer. This retention period is consistent with NARA GRS 5.2: Intermediary Records, which states that the records are temporary and must be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Box audit logs of administrative information that are maintained by MSPB are deleted after 45 days through automated means, as determined by MSPB's Records Officer, unless a business use requires a longer retention. This retention period is consistent with NARA GRS 3.2: System Access Records, which states that the records are temporary and must be destroyed when no longer needed for business use.

Box collects metadata about shared files, such as the file creation date, but not the content of the files. Box stores audit logs of administrative information (including user account information) for a period of seven years or until MSPB terminates its Box account.

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.

The PRA does not apply to Box. The agency uses Box as a transport infrastructure only.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Specific to Box user accounts, Box collects and maintains the following information:

- For Box users managed by MSPB: username, MSPB email address, IP address, and browser.
- For Box users utilizing a commercial Box account: email address, IP address, and browser.
- Box also maintains audit logs of user activity, such as logins, uploads, and downloads.

Additionally, records transferred through Box may include significant quantities of personal information relating to the substantive work of MSPB or from the submitting agency or individual. Because of the varied nature of the agency's work and the different types of records submitted by appellants and agencies as part of MSPB appeals, and by other external users, e.g., related to MSPB's statutory studies function, Box could be used to share any CUI or PII that an MSPB user has authorization to disclose to an external, non-MSPB user or to receive from another agency or individual. Consequently, it is not possible to list with certainty every type of information that will be disseminated using Box. Specific to the files shared via Box, Box collects metadata about files, such as the file creation date, but does not collect information on the content of the files.

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

The sources of the information in Box come from two types of users: MSPB users and non-MSPB users. MSPB users include both MSPB employees and MSPB contractors. MSPB users are required to provide their username and an MSPB email address to the agency, which is then entered into Box to create an MSPB Box account. Non-MSPB users include employees of other Federal agencies, individuals, employees of state or local government agencies, employees of a private company or law firm, and other external entities that are authorized to transfer information to MSPB. Non-MSPB users provide their email address to MSPB, but not to Box. The email address is used by MSPB to send password-enabled web address to those users to submit or retrieve files using Box. The email address is also used by Box to authenticate the user and apply the correct permission settings set by the MSPB account holder.

The sources of information are as follows:

- Directly from the individual;
- Government sources (MSPB's offices, other Federal entities, state, local and tribal governments, and foreign governments); and
- Other sources (members of the public, the media, and the private sector, e.g., including court reporters and legal research publishers).

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.

A username and email address are submitted to MSPB by the end user; therefore, the username and email address used to create a Box account for MSPB users and the email address used to send a password-enabled web address to non-MSPB users should be accurate. If this information is not correct, the user can reach out to the MSPB point of contact by phone, email, or fax to correct the information.

For any records submitted through Box that are maintained in an MSPB system of records, if an individual asserts that information contained therein is not accurate, relevant, timely, or complete, the individual can submit a request to the Office of the Clerk of the Board seeking an amendment of records pursuant to MSPB's Privacy Act regulations at 5 C.F.R. Part 1205.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that the system will collect and maintain more information than is relevant and necessary to accomplish the agency's mission.

Mitigation: This risk is partially mitigated. Box is a transport infrastructure that does not exercise control over the contents of records shared in the system. Therefore, Box does not collect or analyze the contents of records in the system. On the agency side, MSPB's authorities and procedures ensure that there are limits on the types of information that MSPB may request or send via Box. For example, MSPB will not transmit classified materials via Box. Additionally, MSPB provides the statutory protections afforded under the Privacy Act, along with the privacy tenets in the Fair Information Practice Principles and strives to only collect personal information that is necessary to accomplish the agency's mission.

Privacy Risk: There is a privacy risk that information will be collected without the proper legal authority.

Mitigation: This risk is partially mitigated. MSPB's internal policies mandate that Box users may only transmit or receive information that is authorized by statutes, regulations, or other authorities, and only for purposes to assist in the performance of agency responsibilities and to conduct the agency's mission. These authorities may be found generally in this PIA and in MSPB's SORNs governing the type of information being transmitted.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

MSPB uses Box to assist in the secure sharing of CUI or PII records by its offices with entities that MSPB authorizes to access such information in support of MSPB's functions. MSPB may utilize Box to transmit and receive records from outside entities instead of using email because Box encrypts data in transit and at rest. MSPB will also utilize Box to transmit responses to FOIA requests, and these releases will contain only public information. The ability to send records via Box will reduce the need to use U.S. postal mail or commercial delivery services to ship records, providing a more efficient and faster method to interact with our stakeholders while also reducing the risk of a privacy breach or spillage through the transmittal of physical records through the mail. Box will also dramatically reduce the volume of paper records created and maintained and will assist MSPB in meeting the obligations of moving to all electronic recordkeeping.

Box provides a secure, efficient, and effective means to transmit sensitive and voluminous records in support of our operations, including the adjudication of appeals, the disclosure of records under FOIA and the Privacy Act, and the administration of surveys for special studies relating to the civil service.

Examples of MSPB uses of Box include, but are not limited to:

- Transmittal of information to and from external entities, including other U.S. Government agencies and law enforcement organizations;
- Secured transmittal of records within MSPB of voluminous records, such as case-related information;
- Secured transmittal of information with external entities and individuals, such as legal publishers and requesters seeking information under the Privacy Act or FOIA;
- Transmittal of information to the judicial branch related to MSPB's adjudication of appeals;
- Transmittal of other administrative agency records, such as human resources records;
- Transmittal of information to MSPB staff in other offices; and
- To disseminate training materials.

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 MSPB plans to use such results.

No.

3.3 Are there other offices with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information sent by the system will be used inappropriately.

Mitigation: This risk is partially mitigated. MSPB has implemented several measures to ensure that MSPB Box users handle information in accordance with the uses described above. MSPB users are approved for an account by their office director to ensure that only MSPB employees requiring a Box account receive one for the performance of their official duties. Box's built-in controls limit access to the user's account to ensure that the information is available only to individuals who have the authority to access the information. Additionally, all files and folders are associated with a specific user, and each user has specific permissions associated with the information in their account, which specify how a user may interact with a particular file. Every time a user attempts to access a file or folder, Box uses these permissions to verify that a user has explicit authorization to interact with the file. This process ensures that access is restricted to the authorized type of interaction with those specific files or folders.

Box audit logs are available on a read-only mode to MSPB's Box Administrator. That individual has the capability to review Box audit logs for security monitoring, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. Box audit logs are automatically monitored by Box's SIEM tool. Any alteration of Box audit logs is flagged by SIEM, which sends a notification to MSPB's Box Administrator. This ensures that MSPB's Box Administrator is alerted to any unauthorized alterations of the audit logs.

Files securely shared via Box are deleted after 30 days through automated means. In addition, each MSPB office with a Box account can further customize the security and permissions associated with its files. For example, MSPB offices with a Box account can determine how users in their office may access records in the account. MSPB offices may also specify other limitations, such as limiting access only to users with an mspb.gov email address or prohibit downloading a certain file. Overall, Box users are given only the privileges they need to access a file, and the file is deleted through automated means.

Additionally, MSPB's Box Administrator can automate functionality that will place records into a restricted "Quarantine" area if they meet certain parameters, such as records containing social security numbers or specific words or phrases that may indicate a level of protection higher than CUI. When this functionality is enabled, MSPB's Box Administrator must review and take action to release these records from the Quarantine area before they are accessible to MSPB Box users.

Privacy Risk: There is a risk that users could use information received from the system for purposes other than that for which the information was provided.

Mitigation: This risk is partially mitigated. The MSPB Box user determines the recipient(s) who may access the records through an invitation or web address. Additionally, MSPB communicates applicable restrictions on further dissemination of the records as a part of the release of the information. For example, information released under a routine use in an MSPB SORN is restricted from disclosure outside of the stated use approved by MSPB's privacy office. Other records, such as records released in response to a FOIA request, constitute public information and do not require additional protections.

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.

A warning banner notifies Box users at login that any information transmitted through the system may be monitored, intercepted, searched, and seized by the agency, and that users therefore have no reasonable expectation of privacy regarding such information. Additionally, links to the Box Privacy Policy and Terms of Service are displayed in the footer of every page in Box. Finally, individuals are provided written notice of the agency's collection of information via Box through this PIA.

With regard to files transmitted through Box, MSPB utilizes Box only as a transport infrastructure and has not designed Box as an official record-keeping system, document archival system, or document backup system. As such, additional notification to individuals is provided by existing authorities for collecting and maintaining information to carry out MSPB's mission. For example, MSPB's SORN covering appeal records, MSPB/GOVT – 1, Appeals and Case Records, 77 Fed. Reg. 65206 (Oct. 25, 2012), provides notice about the collection of information related to the adjudication of the appeals and covers the appeal records transmitted through Box. Additionally, another MSPB SORN, MSPB – 2, Surveys for Special Studies of the Civil Service, 86 Fed. Reg. 7307 (Jan. 27, 2021), provides notice about the collection of information related to the development and administration of surveys for special studies of the civil service, such as the MPS.

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

Box collects basic information and metadata to administer the service (e.g., username, email address, type of browser, and IP address). For this collection of information, users may consent to the use of Box by signing up for an account when they receive the invitation to review the files shared by MSPB. Individuals may decline to provide this information by requesting that MSPB transmit the records in a different manner, such as through a password-protected compact disc or CD, through MSPB's e-Appeal Online Repository, or through FOIAonline.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that Box users will not be given the opportunity to consent to the uses of their information.

Mitigation: This risk is mitigated. Individuals must proactively sign-up for a Box account to access the records. Individuals will be able to decline consent by not opening a Box account. Additionally, to provide transparency and allow Box users to understand how their communications and other information are handled, the following measures are in place:

- MSPB's security-warning banner is displayed on the login screen that Box users see when they log into Box. It informs users that any information they transmit through a computer or mobile device, including information transmitted through Box, may be monitored, intercepted, searched, and seized by the agency, and that Box users therefore have no reasonable expectation of privacy regarding such communications.

- Links to the Box Privacy Policy and Terms of Use are displayed in the footer of every page in the Box system.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

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

Box is not designated by MSPB as an official record-keeping system, document archival system, or document backup system. As such, records transmitted through Box are deleted after 30 days through automated means, as determined by MSPB's Records Officer. This retention period is consistent with NARA GRS 5.2: Intermediary Records, which states that the records are temporary and must be destroyed upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Box audit logs of administrative information maintained by MSPB are deleted after 30 days through automated means, as determined by MSPB's Records Officer, unless a business use requires a longer retention. This retention period is consistent with NARA GRS 3.2: System Access Records, which states that the records are temporary and must be destroyed when no longer needed for business use.

Box collects metadata about shared files, such as the file creation date, but not the content of the files. Box stores audit logs of administrative information (including user account information) for a period of seven years or until MSPB terminates its Box account.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information collected by the system may be retained longer than necessary.

Mitigation: This risk is partially mitigated. MSPB applies NARA-approved records retention schedules to files submitted through Box. Records transmitted through Box are deleted after 30 days through automated means. Box audit logs of administrative information maintained by MSPB are deleted after 30 days unless there is a business use which requires a longer retention.

Section 6.0 Information Sharing

6.1 Is information shared outside of MSPB 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.

Since Box is a secure file sharing solution, it may be used to share information outside of MSPB as part of normal agency operations. Examples of non-MSPB entities that the agency may share records with via Box include:

- Other Federal agencies;
- State and local agencies;
- Parties and their representatives to the adjudication of an MSPB appeal;
- Legal publishers;
- Court reporters;
- Members of the public (including Privacy Act and FOIA requesters); and
- Stakeholders of MSPB's Office of Policy and Evaluation (to administer surveys of special studies or training materials).

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

Because Box is used solely as a transmittal platform, the authority to share information using Box is contained in the SORN that covers that information. For example, appeal records may be shared with DOJ or OPM as authorized by the routine uses in MSPB's appeal records SORN, MSPB/GOVT – 1, Appeals and Case Records, 77 Fed. Reg. 65206 (Oct. 25, 2012). This SORN governs the information that MSPB collects during the adjudication process and sets forth how MSPB maintains and protects appeals and case records. Other SORNs may apply depending on the content of the records and whether the records are indexed and retrieved by a personal identifier.

6.3 Does the project place limitations on re-dissemination?

MSPB informs external parties of restrictions and limitations on re-dissemination. This includes releases under the routine uses of MSPB's SORNs, and MSPB only authorizes the disclosure of this information if the stated use is compatible with the purpose of the collection, as outlined in the applicable SORN. Other records, such as records transmitted pursuant to a FOIA request, constitute public information and MSPB has no authority to limit the re-dissemination of records released pursuant to a FOIA request.

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

Since Box conceivably could be used to transfer any type of record, there will be instances in which information disclosures are not tracked if there is no legal requirement to do so. MSPB utilizes FOIAonline to track requests for information disclosure pursuant to FOIA, the Privacy Act, the routine uses in MSPB's SORNs, and statutes and regulations. FOIAonline is a web-based application and assists MSPB in tracking and recording requests received for the disclosure of information. This includes requests subject to the accounting provisions of the Privacy Act. The information retained as part of this accounting requirement includes the agency or individual requesting the information, a description of the requested information, the reason for the request, the date of the request, the date of the release, the authority for the release, and the limitations and obligations on the requesting agency or individual with regard to use and further dissemination.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information will be shared outside the scope of the applicable SORN or without the proper authority or accounting.

Mitigation: This risk is partially mitigated. All MSPB Box users are required to complete annual privacy awareness training, which informs users on their Federal information privacy requirements, including the proper handling of PII.

External parties provided PII under a routine use are subject to Privacy Act limitations on disclosures. Any use of the records must be compatible with the purpose of the collection, as outlined in the applicable SORN. Other records, such as records received pursuant to a FOIA request, constitute public information and MSPB has no authority to limit the re-dissemination of records released under a FOIA request.

Section 7.0 Redress

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

Individuals (non-MSPB users) may contact Box, in accordance with their Privacy Policy and Terms of Service, to access the administrative information and metadata collected by Box.

With regard to the information transmitted using Box, individuals seeking notification of and access to their records in an MSPB system of records may submit a request in writing to the Merit Systems Protection Board, Office of the Clerk of the Board, 1615 M Street, NW, Washington, DC 20419. This request may also be sent to the agency by email at privacy@mspb.gov. Individuals requesting access must comply with MSPB's Privacy Act regulations regarding verification of identity and access to records (5 C.F.R. Part 1205).

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

External, non-MSPB users must contact Box to correct inaccurate or erroneous information collected and maintained by Box. This includes the administrative and metadata collected to administer their Box account. If the individual provided an incorrect email address to MSPB, the individual would need to contact MSPB to provide the correct email address to receive the web address to access shared records in Box.

With regard to the information transmitted using Box, individuals seeking amendment of their records in an MSPB system of records may submit a request in writing to the Merit Systems Protection Board, Office of the Clerk of the Board, 1615 M Street, NW, Washington, DC 20419. This request may also be sent to the agency by email at privacy@mspb.gov. Individuals requesting amendment must follow MSPB's Privacy Act regulations regarding verification of identity and amendment to records (5 C.F.R. Part 1205).

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

This PIA provides notice to individuals on how to correct their information. Additionally, MSPB's Privacy Act regulations and SORNs covering the types of records transmitted through Box provide notice to the individual.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals will not be able to correct inaccurate or erroneous information collected about them.

Mitigation: This risk is partially mitigated. The recipient's email address is submitted to MSPB by that user; therefore, this information should be accurate. For any records maintained in an MSPB system of records and transmitted using Box, an individual may seek amendment of any records they assert is not accurate, relevant, timely, or complete. Information on how to submit an amendment request is outlined in MSPB's Privacy Act regulations at 5 C.F.R. Part 1205.

Section 8.0 Auditing and Accountability

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

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

MSPB ensures that the practices stated in this PIA are followed by leveraging training, IT RoB, role-based access, and other standard operating procures and policies. MSPB's Box Administrator has access to system logs and may conduct audits to ensure that there is no misuse of the system or information. See Section 1.3 for additional security and privacy safeguards.

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

All MSPB users and contractors must complete privacy awareness training and information security awareness training annually or when they begin work on an MSPB contract, respectively, as well as read and agree to comply with MSPB's Information Technology (IT) Rules of Behavior (RoB) and Box Terms of Service prior to accessing Box and annually thereafter.

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

An MSPB user is granted a Box account only when approved by an MSPB office or program director. This ensures that MSPB Box accounts are only provided to employees who need to utilize Box in the performance of their official duties. MSPB deploys role-based access controls and enforces a separation of duties throughout all MSPB operations to limit access to records and ensures that only MSPB employees who have an official need to know will have access to the information. The need to know is determined by the respective responsibilities of the employee and the needs of the office. MSPB employees who do not have a need to know do not have access to a Box account and cannot access the records transmitted using Box.

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

MSPB's use of Box does not require information sharing agreements or MOUs. New uses of information are not permissible without review and authorization by MSPB stakeholders, including MSPB Chief Privacy Officer and Chief Information Officer. If new uses of the information are approved, they will only be utilized once appropriate notice has been provided, including updating the PIA and, if applicable, revising applicable SORNs. Within MSPB, access to records transmitted using Box is determined by the respective responsibilities of the employee and the needs of the office. Box is not intended to be an external collaboration tool; therefore, external, non-MSPB users will not have access to records in Box other than the records they are submitting to MSPB or to which they have been granted access by MSPB.

Responsible Officials

D. Fon Muttamara
Chief Privacy Officer
U.S. Merit Systems Protection Board

Approval Signature & Date

William Spencer

Digitally signed by William Spencer
Date: 2021.06.11 15:43:09 -04'00'

William D. Spencer
Acting Executive Director
& Senior Agency Official for Privacy
U.S. Merit Systems Protection Board