

BOX Privacy Impact Assessment



6/25/2025

USITC Privacy Program

The Privacy Impact Assessment assesses the risks to personally identifiable information of members of the public that is processed, used, maintained, or disseminated by the United States International Trade Commission.

BOX Privacy Impact Assessment

USITC PRIVACY PROGRAM

OVERVIEW

Under the E-Government Act of 2002, U.S. International Trade Commission (USITC or Commission) must conduct a Privacy Impact Assessment (PIA) for USITC systems that collect, use, process, maintain, or disseminate personally identifiable information (PII) about members of the public. Office of Management and Budget (OMB) Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 2003) provides implementation guidance on how agencies should assess the risks to PII that they collect, use, process, maintain, or disseminate.

This document includes guidance to help complete the PIA. Upon completion of this form, please submit it to privacy@usitc.gov for review by the USITC Privacy Program. Once the PIA has been reviewed and approved, USITC will publish it on the USITC website, unless doing so would raise security concerns.

1 SYSTEM, PROJECT, OR PROGRAM INFORMATION

1.1 What is the specific purpose of the USITC's use of the system and how does that fit with the USITC's mission?

BOX is a cloud-based file sharing and collaboration service that the following USITC offices use:

- The **Office of Unfair Import Investigations (OUII)** participates, on behalf of the U.S. public, in Commission investigations of unfair methods of competition and unfair acts in the importation and sale of articles under Section 337 of the Tariff Act of 1930 (Section 337), many of which involve intellectual property rights. OUII uses BOX as a raw discovery and document delivery tool. OUII also uses BOX to share documents with counsel for parties that have signed onto an administrative protective order (APO) in a Section 337 investigation and to allow counsel to share documents pertaining to Section 337 investigations with OUII.
- The **Office of the Secretary (OSE) Docket Services** processes over the counter and electronically filed documents in the Electronic Documents Information System (EDIS), the repository for documents filed in investigations before the USITC. Applicable statutes require the USITC to release certain documents that contain confidential business information (CBI) to authorized parties. In addition, 19 U.S.C. § 1337(n) requires the USITC to release to Customs and Border Protection (CBP) the necessary documents to administer USITC exclusion orders issued in Section 337 investigations. OSE uses BOX to deliver these CBI-containing documents to authorized private parties, USDOC, and CBP.
- The **Office of Operations, including Offices of Analysis and Research Services (OARS), Economics (EC), Industry and Competitiveness Analysis (ICA), Investigations (INV), and Tariff Affairs and Trade Agreements (TATA)** collect and analyze data on private sector entities, trade, and industry competitiveness and use BOX for its file sharing capabilities.

- The **Office of the General Counsel (OGC)** uses BOX to assist with sharing documents during litigation and other activities.
- **The Office of the Chief Information Officer (OCIO)** uses user account information to conduct account administration tasks (e.g., creating an account, modifying account information) for system maintenance purposes.

2 INFORMATION COLLECTION

2.1 What types of PII are collected? Please select all applicable items and provide a general description of the types of information collected.

PII means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Tax ID Number | <input checked="" type="checkbox"/> Personal Cell Number |
| <input type="checkbox"/> Mother’s Maiden Name | <input type="checkbox"/> Credit Card or Financial Account Number | <input checked="" type="checkbox"/> Personal Email Address |
| <input type="checkbox"/> Social Security Number (SSN) | <input type="checkbox"/> Patient ID Number | <input checked="" type="checkbox"/> Work Address |
| <input type="checkbox"/> Date of Birth | <input checked="" type="checkbox"/> Employment or Salary Record | <input type="checkbox"/> Physical Characteristics (eye or hair color, height, etc.) |
| <input type="checkbox"/> Place of Birth | <input type="checkbox"/> Medical Record | <input type="checkbox"/> Sexual Orientation |
| <input checked="" type="checkbox"/> Home Address | <input type="checkbox"/> Criminal Record | <input type="checkbox"/> Marital Status or Family Information |
| <input checked="" type="checkbox"/> Work Phone Number | <input type="checkbox"/> Military Record | <input type="checkbox"/> Race or Ethnicity |
| <input checked="" type="checkbox"/> Work Email Address | <input checked="" type="checkbox"/> Financial Record | <input type="checkbox"/> Religion |
| <input checked="" type="checkbox"/> Logon Credentials (e.g. username, password) | <input checked="" type="checkbox"/> Education Record | <input type="checkbox"/> Citizenship |
| <input type="checkbox"/> Driver’s License Number | <input type="checkbox"/> Biometric Records (e.g. fingerprints, photograph, etc.) | <input type="checkbox"/> Other:
<input type="text"/> |
| <input type="checkbox"/> Passport or Green Card Number | <input type="checkbox"/> Sex or Gender | <input type="checkbox"/> None |
| <input type="checkbox"/> Employee No. or other Identifier | <input type="checkbox"/> Age | |
| | <input checked="" type="checkbox"/> Home Phone Number | |

Explanation: BOX requires individuals, including USITC employees and outside parties, to create user accounts to be able to access or upload documents. Creation of these user accounts requires individuals to input the above-identified PII, including name and contact information. Outside parties may use BOX to share documents that include additional types of PII not indicated above. However, the USITC does not request such information from outside parties for them to use BOX. BOX account information for some entities (e.g., sole proprietors) may include personal information, such as contact information for individuals.

2.2 About what types of people do you collect, use, maintain, or disseminate PII? Please describe the groups of individuals.

BOX stores information on members of the public, USITC employees and contractors, vendors, suppliers, individuals, and other agencies or government entities (e.g., Congress, US Department of Commerce (USDOC), and Federal, state, and local agencies) involved in transmission of information for cases before the USITC (e.g., representatives of companies or law firms). This information includes both account information for users accessing BOX and information included in documents transferred through BOX.

2.3 Who owns and/or controls the PII?

The USITC has entered into a contract with BOX to use the system to securely transmit information. BOX owns the data related to user account information, and the USITC owns the content of the information submitted using BOX software.

2.4 What specific laws, regulations, or policies authorize the collection of the PII? If the system collects Social Security Numbers (SSNs), please provide the authorities for this collection.

Statutory authority includes the following: 19 U.S.C. §§ 1330–1335, 1337, 1671 *et seq.*, 2151, 2213, 2251–2254, 2436, 2482, 2704, 3204, 3353, 3372, 3381, 3804; and 7 U.S.C. § 624.

BOX does not collect SSNs.

2.5 Does the system derive new data or create previously unavailable data about an individual through aggregation or derivation of the information collected?

New users accessing BOX use their email addresses as usernames and are prompted to create passwords, which are used to authenticate their access to the system.

2.6 Given the amount, type, and purpose of information collected, discuss what privacy risks were identified and how they will be mitigated.

Possible risks to the privacy of individuals' data include unauthorized access by both internal and external users, breaches of the system data, and the retention of records beyond the retention period or limit. Risks are mitigated through the use of access controls and other security controls based on guidance in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. Records are retained and disposed of in accordance with retention requirements, as discussed in section 3.4.

3 USES OF THE SYSTEM AND THE INFORMATION

3.1 Describe all uses of the information. Describe how the information supports the USITC mission or a business function.

BOX is a cloud-based file sharing and collaboration service that the following USITC offices use:

- **OUII** investigates, on behalf of the U.S. public, unfair methods of competition and unfair acts in the importation and sale of articles under Section 337, many of which involve intellectual property rights. OUII uses BOX as a raw discovery and document delivery tool. OUII also uses BOX to share documents with outside parties that have signed onto APOs in Section 337 investigations and to allow outside parties to share documents pertaining to Section 337 investigations with OUII.
- **OSE Docket Services** processes over the counter and electronically filed documents in EDIS, the repository for documents filed in investigations before the USITC. Applicable statutes require the USITC to release certain documents that contain CBI to authorized parties. In addition, 19 U.S.C. § 1337(n) requires the USITC to release to CBP the necessary documents to administer USITC exclusion orders issued in Section 337 investigations. OSE uses BOX to deliver these CBI-containing documents to authorized private parties, USDOC, and CBP.
- **The Office of Operations including OARS, EC, ICA, INV, and TATA** collect and analyze data on private sector entities, trade, and industry competitiveness and use BOX for its file sharing capabilities in order to share information on collaborative research projects within USITC.
- **OGC** uses BOX to assist with sharing documents during litigation and other activities. OGC shares documents with counsel for outside parties to Commission investigations and, on occasion, with counsel representing the USITC, including attorneys at the Department of Justice (DOJ) and contracted private outside counsel.
- **OCIO** uses user account information to conduct account administration tasks (e.g., creating an account, modifying account information) for system maintenance purposes.

In addition to these uses, USITC users who have administrative accounts in BOX can review audit logs of user activity within BOX (e.g., whether users view, upload, download, or modify information). Users are granted access to BOX files based on need-to-know.

3.2 How can it be ensured that the PII is accurate, relevant, timely, and complete at the time of collection?

BOX relies on users to verify the accuracy of their data before creating a new account to access the system. Users may access their BOX accounts in order to change information about their BOX account (e.g., incorrect contact information). Individuals may also submit a Privacy Act request to USITC to update their information that is stored in documents submitted to the USITC.

3.3 How can the USITC ensure that only the minimum PII elements are collected?

When a new user creates a BOX account, the BOX registration page identifies the required and optional data fields. The required fields consist only of data elements needed for users to establish an account and for the

USITC to sufficiently identify and contact a user about their account or for information relating to a case or investigation (e.g. name, email address, username, password).

3.4 What is the retention period for the system data? Has the applicable records disposition schedule been approved by the National Archives and Records Administration (NARA)?

User account records are covered by NARA General Records Schedule 3.2, item 030, Information Systems Security Records.

3.5 What methods are used to archive and/or dispose of the PII in the system?

The USITC destroys hard copies of files stored in BOX and electronically removes electronic files. When USITC employees leave the USITC, their BOX accounts are deactivated, and they can no longer access BOX through their USITC account. Documents contained within BOX follow records disposition schedules unique to these records. USITC offices may use BOX as needed for their mission-related needs.

3.6 Will the data in the system be retrieved by a personal identifier?

Most often, users do not retrieve records via personal identifiers because users typically access records through specific BOX folders designated by matter (e.g., by case or investigation). However, there are some instances when USITC employees may query BOX by name or e-mail address, but such use is generally limited to the system administrator. These instances could include, but are not limited to, account management and maintenance (e.g., a user leaves the USITC and a system administrator needs to find all instances of BOX folders shared with them or users violates the terms of use and their access needs to be removed).

3.7 If the answer is “yes” to the previous question, is the system covered by an existing Privacy Act System of Records Notice (SORN)?

SORN ITC-12 System Access Records, September 27, 2017, applies to the user account records in BOX. The USITC does not typically retrieve the files transferred through BOX by PII. As a result, the USITC has determined that a SORN is not necessary for those files.

4 INTERNAL SHARING AND DISCLOSURE OF INFORMATION

4.1 With which internal components of the Commission is the information shared?

As noted in section 3.1, the following USITC offices access and use BOX: OUII, OSE, the Office of Operations (including OARS, EC, ICA, INV, and TATA) and OGC. In addition, the OCIO accesses BOX to conduct system maintenance activities.

4.2 For each recipient component or office, what information is shared and for what purpose?

Each USITC office accesses and uses user account information and documents in BOX based on the corresponding need, as described in section 3.1.

4.3 How is the information transmitted or disclosed?

User account information can be viewed electronically in BOX. Documents can be viewed and downloaded electronically from BOX or printed and transmitted via paper copy.

4.4 Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Possible risks to the privacy of individuals' data through internal sharing include unauthorized access by internal users and breaches of PII. Risks are mitigated through the use of access controls to limit access only to individuals with a need-to-know. All USITC employees and contractors are required to complete annual information security and privacy awareness training to understand the requirements for safeguarding PII and to abide by rules of behavior for using USITC information systems. In addition, USITC system administrators are required to complete training that addresses their responsibilities as users with privileged access to BOX.

5 EXTERNAL SHARING AND DISCLOSURE

5.1 With which external (non-USITC) recipient(s) is the information shared?

The USITC does not share BOX user account information with external parties.

The USITC uses BOX to transfer files to external parties where an authorized collaboration exists. For example, the USITC uses BOX to share documents with counsel for parties in USITC investigations pursuant to an administrative protective order (APO), with USDOC and CBP pursuant to USITC statutory requirements (e.g., Section 337, the American Manufacturing Competitiveness Act of 2016), or with other external recipients when necessary for other authorized activities where information must be shared (e.g., sharing information with the Department of Justice (DOJ) or other outside counsel representing the USITC in litigation).

5.2 What information is shared and for what purpose?

The USITC does not share BOX user account information with external parties.

The USITC uses BOX to share information for authorized purposes related to the USITC's exercise of its statutory functions, including administrative and mission-related functions. As noted above, the USITC uses BOX to share investigation-specific information and files, including CBI, with parties to Commission investigations and other federal agencies (e.g., USDOC and CBP). BOX enables the USITC to securely effect service on or otherwise share files with private parties, collect information from external parties, and share information with other federal

agencies as statutorily required. The Commission also uses BOX to transfer administrative records to DOJ and outside counsel, when necessary, for purposes of litigation of non-mission, administrative matters (e.g., employment litigation).

5.3 How is the information transmitted or disclosed?

Third-party users access data through BOX. BOX requires users to authenticate to the system (e.g., via username and password) prior to accessing the data. In addition, BOX settings allow administrators to limit users' access to only the data relevant for their role.

5.4 Are there any agreements with external entities concerning the security and privacy of the data once it is shared, such as a Memorandum of Understanding (MOU)?

When the USITC shares CBI, it establishes information-sharing agreements to ensure that information is protected. For example, CBI that the USITC shares with authorized representatives of parties to import injury and unfair import investigations is subject to an APO. Private parties must sign onto the APO issued for a specific Commission investigation before the USITC can release CBI to them for that investigation. Similarly, the USITC shares CBI with other federal agencies (e.g., USDOC and CBP), as statutorily authorized, under interagency agreements or memoranda of understanding.

5.5 Are privacy requirements included in contracts and other acquisition-related documents? If yes, please describe these requirements.

Yes. All contract staff are bound by contract language stating they will not disclose sensitive information, including PII, and are required to sign nondisclosure agreements. In addition, the contract language states that contract staff must complete required USITC trainings regarding privacy and information security.

5.6 What type of training is required for users from agencies outside USITC prior to receiving access to the information?

The USITC does not provide staff at the USDOC or CBP with training on how to use data from BOX. The MOUs referenced in section 5.4 state that employees, interns, or qualified contractors of the respective agencies who are granted access to information shared under the MOU have a qualified background investigation completed in accordance with applicable agency standards based on the type of information they are accessing.

5.7 Are there any provisions in place for auditing the recipients' use of the information?

USITC users who have administrative accounts in BOX can review audit logs of user activity within BOX (e.g., whether users view, upload, download, or modify information). Users are granted access to BOX files based on need-to-know.

5.8 Given the external sharing, please discuss any privacy risks that were identified and describe how they were mitigated.

Privacy risks include unauthorized access to data and insecure methods of sharing data. As noted in section 5.3, external users access information through BOX. BOX security controls (e.g., authentication and user access controls) help reduce the likelihood of unauthorized users obtaining access to the system.

6 NOTICE

6.1 Is notice provided to the individual prior to collection of information? If notice was not provided, why not?

The login page for the BOX website includes a link to BOX's privacy policy:

<https://www.box.com/legal/privacypolicy>. In addition, this PIA provides individuals with notice regarding the USITC's use of BOX. SORN ITC-12 provides notice regarding records retrieved via personal identifier.

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

Individuals are not required to provide their information to BOX. However, if they do not provide the necessary information, they will be unable to create a user account, login to the system, or submit or view documents.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Prior to creating a BOX account, potential users may read the BOX Terms of Use Agreement to understand how BOX account information is used. If they object to how the data is used, they are not required to create a BOX account, and thus would not consent to Box's use of their data.

6.4 Given the notice provided to individuals above, describe what privacy risks were identified and how they were mitigated.

Potential risks with respect to notice include insufficient notice to users. Some users might not understand what types of information are collected by BOX and how this information is used. This risk is mitigated through the publication of this PIA on the USITC website and by including a link to the USITC Privacy Policy on the BOX homepage.

7 INDIVIDUAL ACCESS AND REDRESS

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their information?

Users may update their BOX account information by contacting BOX or logging into their accounts. The user may contact USITC to update information in a document stored within BOX.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

The BOX website provides information to users on how to update their account information.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

Not applicable. Users can update their information by contacting BOX or the USITC.

7.4 Discuss any opportunities or procedures by which individuals can contest the accuracy of their information in the system or actions taken as a result of USITC reliance on information in the system.

Users may contest the accuracy of their information by contacting the USITC or BOX, in accordance with the procedures outlined in this section.

8 TECHNICAL ACCESS AND SECURITY

8.1 Who has access to the PII in the system?

BOX user account information is accessible only by USITC staff authorized to conduct account administration tasks (e.g., creating an account, modifying account information) for system maintenance purposes. External parties who are authorized to submit files to or retrieve files from BOX for a particular matter have access to the PII in the files that they are authorized to view for that matter.

8.2 Does the system use roles to assign privileges to users of the system?

External BOX users (e.g., non-USITC staff) are assigned access to folders depending on their role and need-to-know. For USITC staff, users are assigned role-based privileges based on need-to-know and their job responsibilities.

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

Users are assigned roles based on their job title and function.

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

Users are granted access to information in BOX on a need-to-know basis and are granted the least privilege needed to conduct their duties. BOX implements auditing controls in accordance with the NIST 800-53 guidance to track user behavior and identify misuse of the system

8.5 How is the PII secured? What administrative, technical, and physical security safeguards are being used to guard against privacy risks?

BOX implements security controls in accordance with the NIST SP 800-53 guidance. These controls are designed to minimize unauthorized access, use, and dissemination of PII.

8.6 Describe what privacy training is provided to users. How often do users complete the training?

All USITC personnel are required to complete annual privacy awareness training to understand their roles and responsibilities for protecting PII.

8.7 Is the USITC following all IT security requirements and procedures required by federal law to ensure that information is appropriately secured? If yes, does the system have a current authority to operate (ATO)?

BOX has a current ATO and addresses information security requirements in accordance with the Federal Information Security Modernization Act (FISMA) and the relevant policies and guidance, such as NIST SP 800-53.

8.8 Given access and security controls, describe what privacy risks were identified and describe how they were mitigated.

Privacy risks include unauthorized access to data and possible breaches of data. These risks are mitigated through the implementation of security controls in accordance NIST SP 800-53 guidance.
