U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Office of Communications (AOC)

Box Enterprise Software as a Service (Box Enterprise)

Responsible Official

Adam Newberry
Email: MultiMedia@faa.gov
Phone Number: 202-702-9946

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Aviation Administration's (FAA) Office of Communications (AOC) uses Box Enterprise Software as a Service (Box Enterprise SaaS) for file storage and sharing. Box Enterprise is a cloud-based service that is utilized by multiple lines of business within the FAA to transfer and share large files, including documents, photographs, graphics, audio and video. The use of Box Enterprise by the FAA is consistent with FAA's administrative needs and is consistent with FAA Policy under 49 United States Code (USC) 40101 and 49 USC 322.

Under the E-Government Act of 2002, the FAA developed this Privacy Impact Assessment (PIA) because Box Enterprise may transport or store Personally Identifiable Information (PII) on members of the public, including audio and video of interviews of individuals involved with the aviation industry (such as pilots and individuals who attend public aviation events or witnessed aviation events), audition tapes and contact information for paid actors, as well as litigation materials and contract solicitations and proposals. This PIA only addresses the records within Box Enterprise that relate to members of the public as described above.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

Box Enterprise is a FedRAMP approved cloud storage and transfer solution that is certified at the High level. Various FAA lines of business use Box Enterprise to meet their administrative requirements for file storage and transfer for large files, such as audio, video, large graphics, and bulk transfers of contract or litigation data. FAA offices currently using Box Enterprise to transfer or store PII that relates to members of the public include: Office of Communications (AOC), The Mike Monroney Aeronautical Center (MMAC) Media Division, the Office of the Administrator (AOA), Office of General Counsel (AGC), the Office of NexGen (ANG), the Power Services Group (AJW-22), the Air Traffic Organization (ATO) Safety Command Center, and the Flight Standards Service (AFS-830).

Box Enterprise is accessible via username and password. Personal Identity Verification (PIV) via MyAccess is planned. User information maintained within Box Enterprise includes name, FAA email address, role, and Box User ID (a unique string of numbers linked to the user), and amount of storage used. Users of Box Enterprise can send FAA employees, contractors or members of the public links to large files within Box Enterprise. For example, AOC can provide media outlets with audio and video files of aviation crashes or investigations. To do so, AOC sends a link to the Box Enterprise file, which is accessed by clicking on it by the external individual. The individual who receives the link only has access to that document and does not have access to other files within Box Enterprise. Links have expiration dates and are no longer accessible once the dates have elapsed.

The following programs use Box Enterprise as follows:

- AOC: AOC uses Box Enterprise as its primary file server and library repository for media graphics, media videos, and promotional videos, such as audio/video of investigations and interviews with the DOT Administrator meant for public consumption. PII present includes names and audio/video of members of the public,

such as pilots. Although these records might contain such PII, they are not a Privacy Act system of records as they are not searchable by unique identifiers, such as names.

- MMAC Media Division: MMAC Media Division uses Box Enterprise as its primary file server, much like AOC. MMAC Media Division uses Box Enterprise as a library repository for its media graphics, media videos, and promotional materials, such as audio/video of informational topics (i.e. FAA drug testing procedures, "Pilot Minute"), and interviews with MMAC personnel meant for public consumption, etc. Box Enterprise is the only repository for these records.

  PII, including audio and video of members of the public involved in the aviation industry (i.e. pilots), paid actors who make informational videos, and members of the Federal workforce (promotional materials) could be present. Audition tapes and photo releases for paid actors or members of the aviation industry are also saved within Box Enterprise. PII in these records could include these individuals' names, company names/addresses and phone numbers. Although these records might contain such PII, they are not a Privacy Act system of records as these records are retrieved by project title/type and not unique identifiers such as names.

- AOA: AOA uses Box Enterprise to securely transfer photographs to their final storage location. Photographs could include images of individuals who are attending FAA aviation events, such as individuals in the crowd, pilots or air traffic controllers. Records are retrieved via hyperlink and are not searchable by unique identifiers such as names.

- AGC: AGC utilizes Box Enterprise as a secure method to share and transfer large files to external stakeholders to fulfill the agency's obligations for various types of legal matters and proceedings. External stakeholders include the DOT, the Department of Justice (DOJ), and other Federal agencies, as well as opposing counsel in litigation. Box Enterprise is a critical tool, especially for eDiscovery productions, where vast amounts of electronic data need to be delivered regularly in a forensically sound manner under strict deadlines.

  AGC does not intentionally collect index, or store PII, but FAA documents provided to outside parties in litigation may sometimes include PII. In some situations, for example, there might be a protective order in place with the relevant court so that AGC staff are not burdened with the task of manual redactions across thousands of emails/documents, which could translate to hundreds of thousands of imaged PDF pages. PII from employees, contractors, and the public might be present in the

documents AGC receives or sends through Box Enterprise, but AGC does not collect or maintain such PII present in discovery files in any of its systems of records outside the litigation files. PII shared through the system is not indexed, organized, or searchable in any way. Therefore, although these records might contain PII, they are not a Privacy Act system of records.

AGC does not store FAA records on Box Enterprise. AGC only stores copies of records and copies of other documents that AGC is legally required to provide to outside parties as part of the litigation discovery process. The data is most frequently made up of collected and processed copies of Microsoft 365 data, such as emails from FAA users' mailboxes or files from their OneDrive. AGC uses Box Enterprise to transfer litigation data to and from the FAA. The data is stored only for one week and then deleted. The data types include documents, emails, audio, and video files.

Documents uploaded to Box Enterprise for delivery to outside parties are not indexed or retrievable in any organized manner. The receiving party (most often opposing counsel for the given case) downloads all the contents of the designated Box Enterprise folder to which they have been given temporary read-only access. Records are organized in folders for each litigation. A direct link to this folder is shared with the outside party to upload or download the case files.

- ANG: ANG uses Box Enterprise to send or receive video files that are too large for email. Records include technical videos (such as Unmanned Aircraft System Traffic Management (UTM) field tests) that are to be posted to YouTube. Occasional PowerPoint presentations with embedded video are also transferred. No PII is routinely present in these videos. However, it is possible that an individual's voice or image could be present in a video. Box Enterprise is not the final storage location for these records. Although these records might contain some PII, they are retrieved by a unique identifier and are not Privacy Act system of records. AJW-22: AJW-22, Power Services Group uses Box Enterprise to send and receive large file size contract solicitations and evaluations. Box Enterprise is not the final storage location for these records but used to share large files. The records present could include source selection proposals and solicitations. PII present could include the name and business contact information for points of contact for companies submitting proposals. Records are not retrieved by unique identifiers such as names.
- ATO Safety Command Center: ATO Safety Command Center uses Box Enterprise as a secure file transfer method for large files. Records include video and audio of radar for air traffic incidents. Audio and video recordings do not include PII of individuals. The only information present is radar references and flight numbers. Flight numbers can be personal identifiers in some cases. Records are retrieved using airport names (i.e. BWI/IAD) and flight numbers. Hyperlinks are used to

allow access to these records. Box Enterprise is not the official repository for these records.

- Flight Standards Service (AFS-830): AFS-830 uses Box Enterprise as a secure file transfer method for large files of photos and videos. Records include videos and photos that generally relate to the FAA's Rotorcraft Collective, content for social media or YouTube, and the "FAA Safety" magazine. These records are not the final product but are used to create the final product. PII on individuals is present, including photographs of individuals at aviation events such as Oshkosh, photographs or video of "influencers" such as Miss America, including their contact information, and copies of records that report if the "influencer" had any FAA enforcement actions against them. Although these records might contain some PII, they are not are not retrievable by unique identifiers such as names and are not Privacy Act records.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[2], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[3].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records, the existence of which is not known to the public.

The FAA employs multiple techniques to ensure that individuals are informed of the purpose for which the FAA uses, disseminates, and retains PII within Box Enterprise. Records stored or transported by Box Enterprise are not protected by the Privacy Act

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

because they are not retrieved by unique identifiers linked to an individual. The various programs all retrieve data in different manners. For example, records may be searchable by a project name or date.

Additionally, only AOC and the MMAC Media Division use Box Enterprise as the official repository for their records. The other programs utilizing Box Enterprise only use it for temporary storage or transport of records. Records transported or temporarily stored within Box Enterprise, such as records from AGC, may be stored in or pulled from systems that have an associated System of Record Notice (SORN). All SORNs are listed on the Department of Transportation (DOT) Privacy page. An individual whose information is temporarily stored in or transported via Box Enterprise would need to make a Privacy Act request of the official system of records, not Box Enterprise. The FAA does not make **Privacy Act** disclosures out of Box Enterprise; any such requests are redirected to the originating system of record.

Access-related records about individuals who access Box Enterprise are maintained in accordance with the Department's Privacy Act System of Records Notice (SORN), DOT/ALL 13, Internet/Intranet Activity and Access Records, 67 FR 30758 (May 7, 2002), which covers computer access records.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Records stored or transported by Box Enterprise are not protected by the Privacy Act. Records transported or temporarily stored within Box Enterprise, such as records from AGC, may be stored in or pulled from systems that have an associated SORN. All SORNs are listed on the Department of Transportation (DOT) Privacy page. An individual whose information is temporarily stored in or transported via Box Enterprise would need to make a Privacy Act request of the official system of record, not Box Enterprise.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII.

The FAA uses Box Enterprise and the information stored therein under the following authorities:

1) Title 49 United States Code (U.S.C.) § 40101, Policy, which covers matters relating to the public interest and consistent with public convenience and necessity.

2) 49 U.S.C. § 322, General Powers, which requires the Department of Transportation Secretary to carry out aviation duties and powers.

Records stored or transported by Box Enterprise are not protected by the Privacy Act. However, some data transported or stored within Box Enterprise may come from Privacy Act systems of records. All data within Box Enterprise that is subject to the Privacy Act is used only in accordance with the original purpose for the information collection, consistent with the applicable SORN.

System access data is used by the FAA to plan and manage system services in the performance of official duties, and to monitor and investigate improper computer use, as described in DOT/ALL 13, "Internet/Intranet Activity and Access Records", 67 FR 30758 (May 7, 2002).

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

The FAA minimizes its maintenance, use, and retention of data within Box Enterprise to the relevant and necessary information to meet its authorized business purposes. For the following FAA lines of business, Box Enterprise is not the initial collection or final storage location of records: AFS-830, ATO Safety Command Center, AJW-22, ANG, AOA, and AGC. Records collected and used by these Programs are subject to data minimization and retention policies outside of the scope of Box Enterprise.

AOC and MMAC Media Division do use Box Enterprise as the repository for records. However, these records are used to create final products used in other systems. For example, AOC and MMAC Media Division may store media graphics that are eventually used in media campaigns or may use recorded videos of pilots that are meant for the FAA's YouTube channel. These offices maintain still photography, video clips – edited and unedited, graphic design assets (raw materials), as well as the project files/information that form the final deliverables (i.e., a PowerPoint presentation that contains graphics, photos, and an edited video. Those videos, graphics, photos, and PowerPoint presentations themselves will all live on Box in volumes specific to their type and use case. The raw materials get used repeatedly to create additional deliverable projects. The project files themselves are frequently reopened for periodic updates or are repurposed into different deliverables altogether. Records held by AOC and MMAC Media Division are currently maintained as permanent, while a record retention schedule for these records is being developed in conjunction with the National Archives and Records Administration (NARA).

The proposed schedule is that these records are destroyed after 20 years, but longer retention is authorized if required for business use.

System access records within Box Enterprise are maintained pursuant to General Record Schedule 3.2, Information Systems Security Records, Item 030. User profiles created as part of the user identification and authorization process to gain access to the system are temporary and are destroyed when business use ceases.

Operational reporting, error reporting and performance monitoring of the system records are maintained pursuant to General Record Schedule 3.1, General Technology Management Records, item 030. These records are temporary, and may be destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

Records within Box Enterprise are not protected by the Privacy Act. Records transported or temporarily stored within Box Enterprise, such as records from AGC, may be stored in or pulled from systems that have an associated SORN. All SORNs are listed on the Department of Transportation (DOT) Privacy page. All use of data within Box Enterprise is in accordance with the applicable SORNs that cover the source systems of the data.

Profile and logging PII collected by the FAA is used as specified by the DOT's system of records notice, DOT/ALL 13, Internet/Intranet Activity, and Access Records.

In addition to other disclosures generally permitted under 5 U.S.C. §552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use under 5 U.S.C. § 552a(b)(3) as follows:

- To provide information to any person(s) authorized to assist in approved investigations of improper access or usage of DOT computer systems;

- To an actual or potential party or his or her authorized representative for the purpose of negation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings;

- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records; and
- To other government agencies, where required by law.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

Source systems are responsible for the quality of data they provide to Box Enterprise for secure transport. Box Enterprise does not edit or perform quality checks on the data it receives.

External users are allowed access only to the records that they have been sent a hyperlink to by an authorized FAA employee or contractor. For example, AOC can provide media outlets with audio and video of aviation incidents or investigations. To do so, AOC sends a link to the Box Enterprise file, which the external user can click on. The individual who receives the link only has access to that specific file and does not have access to other files on Box Enterprise. Hyperlinks have expiration dates and are no longer accessible once the date has elapsed. External users cannot edit files linked to the hyperlinks they receive.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for federal information systems under the FISMA and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information, and Information Systems, dated March 2006, and NIST Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated August 4, 2022. Box Enterprise implements administrative, technical, and physical measures to protect against loss, unauthorized access, or disclosure. The principle of the least privilege is used to grant access to FAA federal employees and contractors, and user actions are tracked in the Box

Enterprise system access/audit logs. Data within Box Enterprise is encrypted both in transit and at rest.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

The FAA's Information Security and Privacy Service (AIS), Security Governance Division is responsible for the administration of FAA Order 1370.121B, "FAA Information Security and Privacy Program & Policy." FAA Order 1370.121B defines the various privacy requirements of the Privacy Act of 1974, as amended (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the Federal Information Security Management Act (FISMA), DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information technology management policies and procedures. In addition to these, other policies and procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII. Federal and contract employees are given clear guidance on their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of Box Enterprise relative to the requirements of OMB Circular A-130, Managing Information as a Strategic Resource OMB Circular A-130, *Managing Information as a Strategic Resource.*

Responsible Official

Adam Newberry
System Owner, Box Enterprise

Approval and Signature

Karyn Gorman
Chief Privacy Officer KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2026.04.24 09:50:37 -04'00'
Office of the Chief Information Officer