UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT FOR THE BOX BOUNDARY

October 2, 2020

OFFICE OF THE GENERAL COUNSEL

WASHINGTON, DC 20554

Record of Approval

Document Approval		
Privacy POC		
Printed Name: Bahareh Moradi		**Attorney, Office of General Counsel**
Approval Structure		
Printed Name: Margaret Drake		**Senior Agency Official for Privacy**
Signature: Margaret Drake	**Date** 10/2/2020	

Record of Approval

Date	Description	Author

Table of Contents

List of Tables

Box

1.1. Introduction

Section 208 of the E-Government Act of 2002[1] requires agencies to conduct a **Privacy Impact Assessment (PIA)** whenever they procure or develop an information technology system that will collect, maintain, or disseminate information about individual people. The PIA must document how the system will use information it collects about individuals and, unless it contains classified or sensitive information, it must be made available to the public. The PIA was intended to be a tool for agencies to protect personal information throughout a technology system's life cycle. The Office of Management and Budget (OMB) has commented: "*In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks.*"[2]

The FCC is subject to the requirements of the E-Government Act and is committed to identifying and addressing privacy risks whenever it develops or makes changes to its information systems. The questions below explore important privacy issues identified in the Act and in later guidance by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). A longer discussion of the FCC's PIA policies can be found in Chapter 9 of the FCC's Privacy Act Manual (FCC Inst. 1113.1).

System owners, in collaboration with the Information System Security Officers (ISSOs) should complete the **Initial Privacy Assessment (IPA)** prior to filling out the PIA. The FCC Senior Agency Official for Privacy (SAOP) uses the IPA to determine whether a system will collect the kind of information that would make it subject to the requirements of Section 208, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination..

If you have any questions, please contact the Privacy Team at privacy@fcc.gov.

[1] 44 U.S.C. § 3501 note.

[2] OMB Memorandum No. M-03-22 (Sep. 26, 2003), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf.

1.2. Authority To Operate (ATO) Boundary Overview

For each IT system that resides within the ATO Boundary, please use the table below to provide the system name, a brief description of the what the system does, whether it contains Personally Identifiable Information (PII) and a brief description of the PII (if applicable), the applicable System of Records Notice, the legal authorities to collect and maintain the PII, and whether the PII is shared with other systems (internal or external).

Please copy the table as necessary to complete the information for each system within the boundary.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Box
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Box stores FCC documents containing various types of PII. Any information that can be stored on the FCC network can also be stored in Box. This includes names, contact information, financial information, log-in information, and various identification numbers. Because Box is a collaboration tool that may be used by FCC staff to perform the Commission's enforcement and other activities, the PII maintained in the system will depend on the particular business processes for which a Box folder or set of folders is set up and is subject to change based on Commission needs.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? N/A – this system serves as a collaboration tool and the PII contained in Box is covered by other SORNs that are applicable to specific systems of records.
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The information in this system is collected, maintained, and disseminated pursuant the Communications Act of 1934, as amended, and other rules and regulations the FCC enforces. In addition, given the varied nature of the data, PII may be maintained under a number of other statutes including, but not limited to, 5 USC, 42 USC, 29 USC, 18 USC, and 26 USC.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No.

A. Is this a new ATO Boundary or an existing ATO Boundary?

☒ New Boundary

☐ Existing Boundary

B. If the ATO Boundary is/will consist of cloud-based computing system(s),[3] please check the box that best describes the service the FCC receives/will receive from the cloud computing provider:

☒ The FCC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS) [list applicable system(s)]

☐ The FCC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service or PaaS) [list applicable system(s)]

☐ The FCC has deployed its own application/s on the cloud network and controls how these application/s are configured and operate (Infrastructure as a Service or IaaS) [list applicable system(s)]

C. If the IT systems in the ATO Boundary are in the cloud, are the they FedRAMP certified?

☒ Yes, all the IT systems are FedRAMP certified

☐ No, none, or only some, of the IT systems are FedRAMP certified

1.3. Collection of Data

A. Please explain why it is necessary to collect PII to carry out the purpose of each of the system(s) that maintain PII within this Boundary.

The FCC uses Box as a record storage tool for internal and external collaboration. Information in Box is used, disseminated, and maintained for the FCC to perform a variety of regulatory, licensing, enforcement, policy, personnel management, and other activities. PII may be present in some of these activities and is collected based on the nature of the activity.

Some FCC Bureaus/Offices (B/Os) may use Box as their primary record storage tool. In these situations, the B/Os have identified what files they will store in Box, what PII is

[3] *See* NIST, *The NIST Definition of Cloud Computing*, Special Pub. No. 800-145 (Sep. 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

contained in these files, and who requires access to these files. B/Os are also responsible for managing the PII and determining whether it is needed.

B. For each system within this Boundary, will this PII be collected from individuals themselves, or from third-parties? If collected from individuals themselves, link to the Privacy Act Statement[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

Box doesn't collect an individual's PII directly. FCC staff and contractors upload data that has been created or obtained in connection with the Commission's business activities. Third-parties can also upload information into Box to be shared with the FCC. For example, mail sent to the FCC that contains PII provided by and pertaining to members of the public mail may be stored in FCC's instance of Box after it is digitized by a third-party vendor. Alternatively, FCC can share individual folders with third-parties.

C. What steps is the FCC taking to limit the collection of PII to only that which is necessary?

Box stores FCC documents containing various types of PII because Box is a record storage and collaboration tool. The PII maintained in the system will depend on the particular business processes for which a Box folder or set of folders is set up and is limited to that which is necessary for the particular business purpose(s).

D. What steps will the FCC take to make sure this PII is accurate, complete, and up-to-date?

Due to the nature of the system and the anticipated broad use of these services across the enterprise, it is the responsibility of the parties providing the data to ensure the completeness, accuracy, and currency of data at the time it is submitted to the FCC.

[4] A Privacy Act Statement must inform individuals about (1) the authority to solicit information, (2) the principal purpose(s) for collecting the information, (3) the routine uses for disclosing the information, and (4) whether providing the information is mandatory or voluntary.

1.4. Use of the Data

A. Please explain the data flow, including whether the PII will be ingested from, or shared with, another system. Are internal connections reflected in the Cyber Security Asset Management tool (CSAM)? Are Information Sharing Agreements (ISAs) in CSAM for external connections?

No automated sharing occurs. Data flow is user-driven when users place files in Box via User Interface.

B. Will the information be shared with third-parties as part of the operations of the information system (e.g., through an application programming interface or "API")?

No system interconnections are active. APIs are published but not for information sharing.

C. How long will the PII be retained and how will it be disposed of?

The records retention policy depends on the specific type of record stored in Box.

1.5. Data Security and Privacy

A. What are the system's ratings for confidentiality, integrity, and availability?

Confidentiality	**__High**	**_X_Moderate**	**___Low**
Integrity	**__High**	**_X_Moderate**	**___Low**
Availability	**__High**	**_X_Moderate**	**___Low**

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

The FCC protects its information resources with a dynamic set of security measures. Some of these measures (e.g., network firewalls, physical security) protect the entire FCC enterprise, while other measures (e.g., user access restrictions, encryption) are applied to specific information systems, like Box. Following the risk-based policy established in the Federal Information Modernization Act (FISMA), the FCC applies more security measures (also known as security "controls") to information systems that present higher operational risks. Consistent with this policy, the FCC applies specific security controls to systems that collect and process PII. A comprehensive list of the security and privacy controls the FCC may apply to its information systems can be found in National Institute of Standards and Technology (NIST) Special Publication No. 800-53 (revision 4), https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

C. Does the system inherit privacy controls from an external provider? If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of the document.

No.

1.6. Access to the Information

A. Which FCC employees and contractors will have access to the PII in this information system?

FCC Employers and Contractors: Access to Box is restricted to authorized FCC system owners and end users - including contractors - who have completed cybersecurity and privacy training. All system owners and end users must adhere to the FCC Rules of Behavior. Access to the information stored within Box is dependent on the particular business purpose(s) and the access permissions granted to a specific user. For example, system administrators may have access to system data and system audit logs in order to manage access roles, monitor system usage, perform system audits, and complete other necessary job functions. FCC end users have access only to the Box folders necessary and relevant to their job duties.

External Users: External Users may only access FCC data in Box if they have received a link to a shared folder or document. Box permits the FCC user to update settings on each folder, which includes either the auto-deletion or unsharing of a folder/document on a set date.

B. Does this system leverage Enterprise Access Controls?

FCC Employers and Contractors: Yes.

External Users: No, some information must be actively shared with external users.

C. Does the system leverage the FCC's Accounting for Disclosure control?

Yes.

Appendix A - Acronyms and Abbreviations

[Populate based upon abbreviations used in the document.]

Table A-1: Acronyms and Abbreviations

Acronym	Definition