UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR ELECTRONIC COMMENT FILING SYSTEM VERSION 4.0 (ECFS 4.0) BOUNDARY

February, 2022

Annual Review Date

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: February, 2023

Record of Approval

Document Approval		
Drafter Name: Alexander Egorov		**Bureau/Office: OMD**
SAOP Approval		
Printed Name: Linda Oliver		**Acting Senior Agency Official for Privacy**
Signature: Linda L. Oliver Digitally signed by Linda L. Oliver Date: 2022.02.28 15:09:03 -05'00'	**Date**	

Record of Approval

Date	Description	Author
02/15/2022	Validation of information – System Owner	Marlene Dortch
01/28/2022	Validation of completeness – IT Compliance Lead	Liem Nguyen

Revision History

Date	Description	Name
1/25/2022	Original Document Created	Alexander Egorov

ECFS 4.0 System Boundary

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 ELECTRONIC COMMENT FILING SYSTEM VERSION 4.0 (ECFS 4.0)
NAME OF BUREAU Office of Managing Director (OMD)
DOES THE SYSTEM CONTAIN PII? Yes. The PII in the system is available publicly through the Search for Filings feature of the system, using any search criteria.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Full name, home address, phone numbers, work phone numbers, email address, work email address. The FCC collects, maintains, or processes a variety of information on ECFS depending on the needs and purposes of the bureaus and offices across the enterprise. Given the broad use of ECFS for Commission proceedings, rulemakings, and other interactions with the public, the system could conceivably include any type of PII; therefore, it is not possible to list with certainty every PII data element that users could potentially share with the system. While ECFS 4.0 requests only the data elements identified in the table, the system requires users to acknowledge and consent to any information they submit via ECFS being made public.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/CGB-2; 71 Fed. Reg. 17233
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 44 U.S.C. 36; 47 U.S.C. 151 and 154
DOES THE SYSTEM LEVERAGE THE FCC'S ACCOUNTING FOR DISCLOSURE CONTROL (ACCESS TO THE INFORMATION)? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.

DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. Enterprise File Service (EFS).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Enterprise File Service (EFS)
NAME OF BUREAU Office of Managing Director (OMD)
DOES THE SYSTEM CONTAIN PII? Yes. Any PII in the system is available publicly through the Search for Filings feature of the ECFS system, using any search criteria.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The FCC collects, maintains, or processes a variety of information on EFS depending on the needs and purposes of the bureaus and offices across the enterprise. Given the broad use of EFS for Commission proceedings, rulemakings, and other interactions with the public, the system could conceivably include any type of PII; therefore, it is not possible to list with certainty every PII data element that users could potentially share with the system. While EFS does not require any data elements, ECFS requires users to acknowledge and consent to any information they submit being made public.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC/CGB-2; 71 Fed. Reg. 17233
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 44 U.S.C. 36; 47 U.S.C. 151 and 154
DOES THE SYSTEM LEVERAGE THE FCC'S ACCOUNTING FOR DISCLOSURE CONTROL (ACCESS TO THE INFORMATION)? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. ECFS.

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) Amazon Web Services

C. If the IT systems in the ATO Boundary are in the cloud, are 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.

In order to comply with the requirements of the Communications Act of 1934, as well as various statutes and regulations, the FCC offers multiple avenues through which the public can be involved in its decision-making process and can inform the FCC of concerns regarding compliance with FCC rules and requirements. Collecting and maintaining these types of information allows the FCC to be fully informed in decision-making, implementation, and enforcement endeavors. Such a system also allows staff access to documents and improves staff efficiency. Records in this system are available for public inspection. At a minimum, ECFS collects name and address for every comment filed by the public.

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

[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.

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.

PII is collected directly from individuals who have filed comments related to FCC rulemakings and docketed proceedings or other
matters arising under the Communications Act of 1934, as amended, and the Rehabilitation Act.

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

The ECFS 4.0 requires users to enter just the PII that is required for the application to perform.
Any user may submit many types of PII in connection with his/her/its comments, but the ECFS 4.0 application does not require users to provide any PII beyond the contact information data elements identified above.
Additionally, users must agree that the information they post will become public.
Therefore users are discouraged from uploading any unneeded information.
There are no check boxes or required fields for users to provide extra PII.

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 ECFS 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 those data are submitted to the FCC.

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?

Information, including PII, is collected directly from users who file comments in ECFS 4.0. The information, including PII, is shared with EFS, which ECFS utilizes for attachments: Users from the public upload file attachments, which are stored in EFS, and which can be downloaded from EFS by a user who searches in ECFS. The internal connection between ECFS and EFS is reflected in CSAM. ECFS 4.0 does not have any external connections or ISAs in place.

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")?

Unless specifically designated as confidential, material submitted to ECFS is open for public review.

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

Information in the system within this boundary is retained and destroyed in accordance with applicable FCC policies and procedures, as well as with the FCC records disposition schedule or General Records Schedules approved by the National Archives and Records Administration (NARA).

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	____Moderate	_X_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. 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 5 [NIST].

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?

The Search for Filings feature of the system makes all PII stored in the system publicly available.

FCC employees and contractors will have access to PII in the system through the Search for filing feature of the system (i.e., the same as the general public). But FCC employees and contractors also have access to city, state, and zip code for comment filers through access to the metadata. Public users do not have access to city, state, and zip metadata.

B. Does this system leverage Enterprise Access Controls?

Yes. The identification of authorized users of the ECFS 4.0 system and the definition of access privileges are in accordance with the requirements of the related security controls indicated in the ECFS 4.0 SSP. Any users requiring administrative privileges on the ECFS 4.0 system accounts must be approved and then subjected to additional scrutiny by the System Owner and FCC.

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

Yes. The Privacy Team keeps an accurate accounting of disclosures of information.