UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE COMMISSION REGISTRATION SYSTEM (CORES) BOUNDARY

OCTOBER 2023

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: April 2024

Record of Approval

Document Approval	
Drafter Name: Kenneth Wisneski	**Bureau/Office: OMD/OCIO**
SAOP Approval	
Printed Name: Elliot S. Tarloff	**Senior Agency Official for Privacy**
X ELLIOT TARLOFF Digitally signed by ELLIOT TARLOFF Date: 2023.10.04 10:14:18 -04'00' **Signature & Date**	

Record of Approval

Date	Description	Author
09/28/2023	Validation of information – System Owner	Dr. Hua Lu
10/04/2023	Validation of completeness – IT Compliance Lead	Liem Nguyen

Revision History

Date	Description	Name
8/10/2023	Original Document Created	ISSO – Kenneth Wisneski
8/16/2023	System Owner & Business Analyst edited all sections in document.	Dr. Hua Lu & Alan Muhealden
9/22/2023	SAOP edited Sections 1.3, 1.3B, and 1.3C	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff
9/26/2023	Update Sections 1.3, 1.3B and 1.3C	ISSO
9/28/2023	Update to Section 1.4B	SAOP
9/28/2023	Deleted FO_Service in Section 1.2 (A part of FO ADMIN System)	ISSO

CORES 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://obamawhitehouse.archives.gov/omb/memoranda_m03-22

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).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Commission Registration System (CORES)
NAME OF BUREAU Office of the Managing Director (OMD)
DOES THE SYSTEM CONTAIN PII? Yes. Users register and update PII in CORES, which is retrievable by individual identifiers by internal administrative users and in other FCC systems.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The PII is related to individuals who register to do business with the FCC and receive an FCC Registration Number (FRN). The PII elements include contact information, financial information, authentication and security information.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/OMD-25 Financial Operations Information System, 81 Fed. Reg. 69522
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The Communications Act of 1934, as amended, 47 U.S.C.; 44 U.S.C. §§ 3101, 3102, 3309; Section 7701 of the Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c)(1); Federal Financial Management Improvement Act of 1996; Financial Officers Act of 1990; the Federal Managers Financial Integrity Act of 1982; Executive Order 9397.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.

DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS?

Yes. All the systems on the CORES boundary have the same data sources and share access to the PII. Additionally, when an FCC system authenticates a user via FRN, PII is passed and can be parsed by the calling system (i.e., when CORES or another FCC systems calls the FO API service to authenticate FRN/password for authentication, the return not only validates whether the combination is correct, but also sends relevant FRN registration information, PII included). PII is also shared with GENESIS and contained within documents stored in Alfresco. Under certain circumstances, PII also is shared with partner agencies.

INFORMATION ABOUT THE SYSTEM

NAME OF THE SYSTEM

Financial Office Application Programming Interface (FO API)

NAME OF BUREAU

Office of the Managing Director (OMD)

DOES THE SYSTEM CONTAIN PII?

Yes.

PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE)

FO API is a closed system, more commonly referred to as a deny-all system. This application keeps a list of system IP addresses that are allowed to access the RESTful API services. When an FO API RESTful webservice is called, the calling system or individual must pass authentication with an API User account (with a unique user/system ID and password). When CORES or another FCC systems calls the FO API service to authenticate FRN/password for authentication, the response not only validates whether the combination is correct, but also sends relevant FRN registration information, which includes PII. The FO API system therefore contains PII data from the User Registration, CORES, fee filer, and ROSIE databases, including contact information, identity information, and authentication information, which is retrievable by unique identifier.

IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)?

FCC/OMD-25 Financial Operations Information System, 81 Fed. Reg. 69522

WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII?

The Communications Act of 1934, as amended, 47 U.S.C.; 44 U.S.C. §§ 3101, 3102, 3309; Section 7701 of the Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c)(1); Federal Financial Management Improvement Act of 1996; Financial Officers Act of 1990; the Federal Managers Financial Integrity Act of 1982; Executive Order 9397.

DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT?

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

DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS?

Yes. When CORES or another FCC systems calls the FO API service to validate FRN/password for authentication, the return not only validates whether the combination is correct, but also sends relevant FRN registration information, which includes PII, to the calling system.

INFORMATION ABOUT THE SYSTEM

NAME OF THE SYSTEM

Financial Office Application Programming Interface - Cloud (FO APICL)

NAME OF BUREAU

Office of the Managing Director (OMD)

DOES THE SYSTEM CONTAIN PII?

Yes. The system contains, and retrieves information by, user account login names, which are email addresses.

PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE)

The FO APICL system contains a user account login name, which is an email address.

IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)?

FCC/OMD-25 Financial Operations Information System, 81 Fed. Reg. 69522

WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII?

The Communications Act of 1934, as amended, 47 U.S.C.; 44 U.S.C. §§ 3101, 3102, 3309; Section 7701 of the Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c)(1); Federal Financial Management Improvement Act of 1996; Financial Officers Act of 1990; the Federal Managers Financial Integrity Act of 1982; Executive Order 9397.

DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT?

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

DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS?

Yes. The services authenticate usernames (i.e., email addresses) and passwords and retrieves associated usernames (emails) for a given FRN for CORES and other systems.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Financial Office Admin (FO Admin)
NAME OF BUREAU Office of the Managing Director (OMD)
DOES THE SYSTEM CONTAIN PII? Yes. The system allows for the retrieval by FCC admin users of PII by unique identifiers.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) PII includes individual and non-individual FRN data such as contact information, financial information, and authentication and security information.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/OMD-25 Financial Operations Information System, 81 Fed. Reg. 69522
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? The Communications Act of 1934, as amended, 47 U.S.C.; 44 U.S.C. §§ 3101, 3102, 3309; Section 7701 of the Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c)(1); Federal Financial Management Improvement Act of 1996; Financial Officers Act of 1990; the Federal Managers Financial Integrity Act of 1982; Executive Order 9397.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accurate accounting of disclosures of information.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. The Financial Operations Administration System (FO Admin) is an internally accessible web application that grants Financial and other FCC staff with a business need access to various financial modules and features. FO Admin is interconnected and exchanges information with CORES, FCC User Registration, and GENESIS.

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM User Registration
NAME OF BUREAU Office of the Managing Director (OMD)

DOES THE SYSTEM CONTAIN PII?
Yes. PII is retrievable from User Registration by unique identifier.

PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE)
A user registers an FCC username in the form of an email address, and provide name, and contact information (phone number), as well as alternative emails (optional).

IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)?
FCC/OMD-25 Financial Operations Information System, 81 Fed. Reg. 69522

WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII?
The Communications Act of 1934, as amended, 47 U.S.C.; 44 U.S.C. §§ 3101, 3102, 3309; Section 7701 of the Debt Collection Improvement Act of 1996, 31 U.S.C. § 7701(c)(1); Federal Financial Management Improvement Act of 1996; Financial Officers Act of 1990; the Federal Managers Financial Integrity Act of 1982; Executive Order 9397.

DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION (c) OF THE PRIVACY ACT?
Yes. The Privacy Team keeps an accurate accounting of disclosures of information.

DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS?
Yes. User Registration shares PII with CORES, FO Admin, FO-API, and FCC's OKTA system.

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 on the cloud network and controls how these applications are configured and operate (Infrastructure as a Service or IaaS).

[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.

Most CORES systems reside on the FCC's network hosted at Allegany Ballistics Laboratory (ABL) which is leased from IBM, but FO API Cloud uses Amazon Web Services (AWS) a cloud-based infrastructure for Username or FCC Registration Number (FRN) authentication and an extension of the FO API 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.

☐ Not applicable, ATO boundary is not Cloud based.

*Note: AWS, which is utilized for CORES Username and FRN authentication and for FO APICL services, is the only cloud-based system that is part of the boundary and is 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.

Information in CORES is collected, used, disseminated, and maintained for the FCC to perform its regulatory, licensing, enforcement, policy, financial management, and other activities. Personal information is necessary to authenticate registrants while issuing, renewing, reviewing licenses, accepting payments, authorizing service, and enforcing regulations or statutes.

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.

CORES collects and stores business and individual information, including PII, of registrants through a registration page on the CORES website. The FCC Registration webpage currently links to the FCC's Privacy Policy.

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

CORES collects PII based on FCC rules for obtaining an FRN. To limit the collection of PII, Electronic Form 160 for FRN registration requires only those fields that are set forth in the FCC rules. Further, CORES allows users to select exemptions in place of entering a Social Security Number (SSN) or Tax Identification Number (TIN) upon registering or

[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.

updating their FRNs. An SSN or TIN may later need to be added if required by another FCC system to complete a transaction for the FRN owner, but its collection is not required by CORES itself.

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

It is the responsibility of the parties providing the data to ensure the completeness, accuracy, and currency of data at the time it is provided. PII stored in CORES is accessible to users via their online accounts, and they can make updates as necessary. Information that is used by the FCC as part of its regulatory, enforcement, and other activities will be reviewed for accuracy and timeliness as required by the activity and the laws and authorities, if any, applicable at the time the agency compiles the records (e.g., Communications Act, administrative or court evidentiary rules and procedures).

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?

CORES ingests data, including PII, directly from users. CORES also interfaces directly with other FCC systems as a means of authenticating users with FRNs. When users authenticate via CORES, an individual's, or entity's contact and FRN information is shared from CORES to the relevant system via Application Programming Interfaces (APIs). Other FCC systems using CORES as a means of authenticating users must be vetted for privacy and security purposes and must have an authority to operate at the FCC.

All internal connections are reflected within the CORES SSP, and documents are stored in CSAM.

CORES, FO Admin, and FO API connect to GENESIS, which is a product of CGI Federal (CGI). The GENESIS system is comprised of Momentum, a commercial off-the-shelf (COTS) software solution that is built and maintained by the CGI. Further, the FO API services may be used by partner agencies if an agreement is reached between agencies. FO Admin also uses "Alfresco" for some file upload/download services. Alfresco is a COTS Enterprise Content Management (ECM) system. Alfresco includes a collaboration environment - Alfresco Share - and an out-of-the-box web portal framework for managing and using content. Alfresco is in use by FCC's Office of the Inspector General (OIG); it is classified as a Minor Application (aka Child System) within FCC's instance of Amazon Web Services (AWS).

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. Data are shared from the CORES boundary via API with other internal FCC and contractor systems, but information exchanges with third parties are through non-API mechanisms.

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

Information in the systems 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	☒ Moderate	☐ Low
Integrity	☐ High	☒ Moderate	☐ Low
Availability	☐ High	☒ 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. 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?

FCC staff and contractors in the Office of Managing Director (OMD), Financial Operations, and Information Technology centers have access to the PII in the CORES boundary. For example, some authorized FCC contractors have access to certain administrative functions in CORES to ensure the system is functioning properly and to respond to public user inquiries (for example, inquiries regarding password resets, or login issues). Contractors who access CORES are subject to the same rules and policies as FCC staff. Under appropriate circumstances, data within CORES or CORES log data may be provided to other Bureaus and Offices or law enforcement agencies for auditing or law enforcement purposes.

B. Does this system leverage Enterprise Access Controls?

Yes. The identification of authorized users of the CORES system and the specification of access privileges is consistent with the requirements in associated security controls that are depicted within the CORES SSP. Any users requiring administrative privileges on the CORES system accounts must be approved and then received additional scrutiny by the System Owner and FCC official responsible for approving access to the CORES system, accounts and obtain temporary privileged access through the FCC’s Enterprise Access Controls.