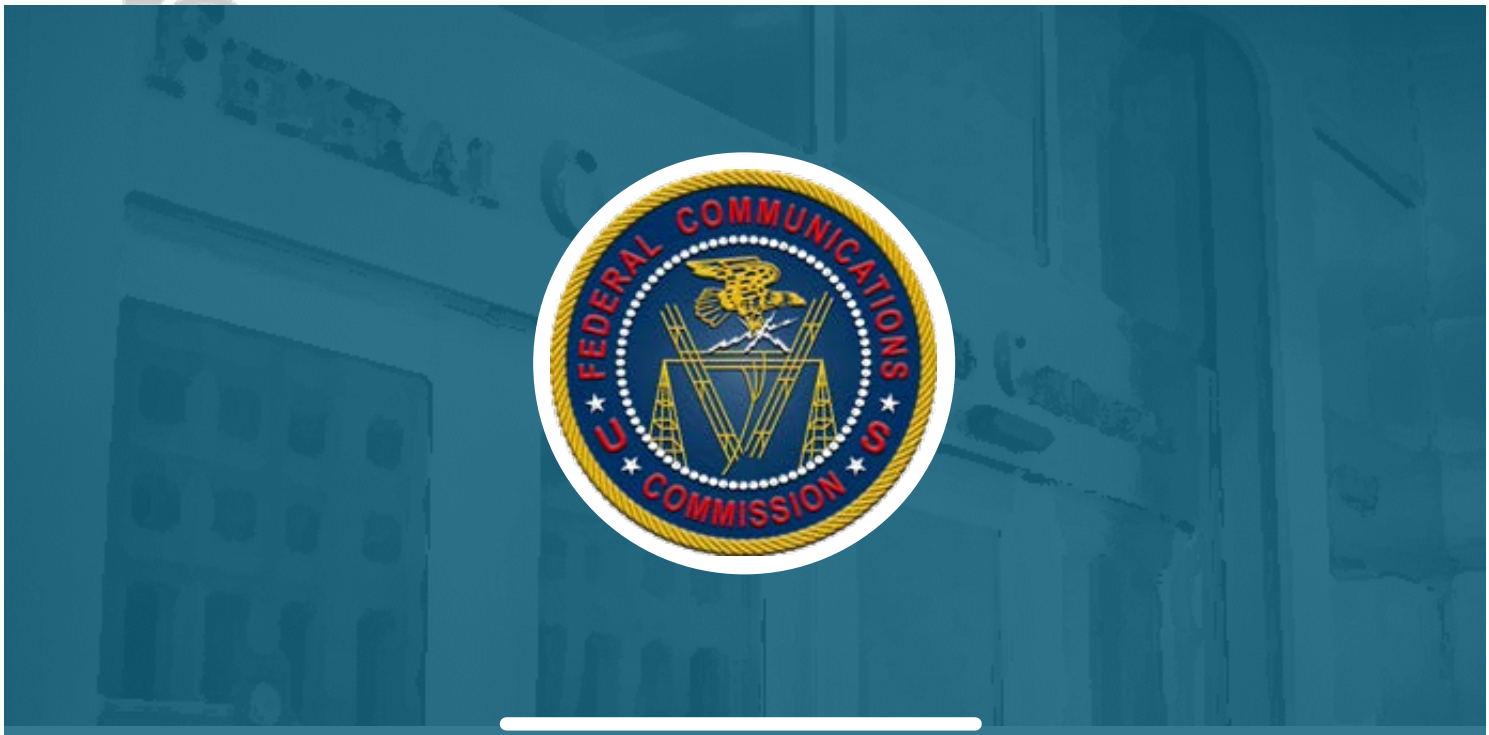

UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

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

November 10, 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 E Drake Digitally signed by Margaret E Drake DN: cn=Margaret E Drake, o=Federal Communications Commission, ou=Privacy, email=margaret.drake@fcc.gov, c=US Date: 2020.11.10 09:49:06 -05'00'	**Date** 11/10/2020	

Record of Approval

Date	Description	Author

Table of Contents

CORES

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 Commission Registration System (CORES)
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Name, contact information, financial information, and various identification numbers.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? FCC/OMD-25 Financial Operations Information System, 81 Fed. Reg. 69522 (Oct. 6, 2016).
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? Executive Order 9397, as amended by Executive Order 13478 (2008); the Communications Act of 1934, as amended, 47 U.S.C.; 44 U.S.C. §§ 3101, 3102, 3309; the Debt Collection Act as amended by the Debt Collection Improvement Act of 1996; the Federal Managers Financial Integrity Act of 1982; Accountability of Tax Dollars Act, P.L. 107-289 ; and other government-wide federal financial statutes addressing debt collection, budget control, financial controls, fraud, waste and abuse, and internal controls codified in Title 31 United States Code.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? YES

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)]

CORES resides on the FCC's network and uses Amazon Web Services cloud-based infrastructure for Username and FCC Registration Number (FRN) authentication. A portion of the FCC network database, such as username, password, and FRN, is duplicated in Amazon Web Services for authentication purposes.

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

AWS, which is used for Username and FRN authentication, 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 in the course

[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.

of 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 of registrants through a registration page on the CORES website. FCC staff and contractors also upload data, e.g. from Forms 160 and 161, that has been created or obtained in connection with the Commission's regulatory, licensing, and other activities.

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 FCC Registration Number. To limit the collection of PII, both the paper Form 160 and Electronic Form 160 for FRN registration require only those fields that are set forth in the FCC rules. Any other input fields for FRN registration are optional for the registrant. Further, CORES allows users to select exemptions in place of entering a Social Security Number (SSN) or Tax Identification Number (TIN) upon registering or updating their FRN. A SSN or TIN may later need to be added to the FRN in CORES if required by another FCC system to complete a transaction for the FRN owner, but not required by CORES itself.

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 created. PII stored in CORES is accessible to users via their online accounts where 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 particular 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).

[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?

CORES ingests information directly from users who set up accounts to establish FRNs in order to do business with the FCC. CORES interfaces directly with other FCC systems as a means of authenticating users with FRNs. See 1.4.B. for more details.

All internal connections are reflected within the CORES Systems Security Plan (SSP) and the CORES FIPS 199. The aforementioned documents are stored in CSAM.

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")?

Authorized FCC contractors have access to information in CORES, when necessary. 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). All FCC contractors are required to complete security and privacy training prior to obtaining access to any FCC systems, and complete annual security and privacy training to maintain network access and access to those systems. Contractors who access CORES are subject to the same rules and policies as FCC staff. Contractors must also follow the reporting and other procedures in the FCC's Breach Notification Policy.

Additionally, CORES interfaces directly with other FCC systems as a means of authenticating users with FRNs. In the course of authentication, individuals' contact and FRN information is shared with these APIs, if necessary. Other FCC systems using CORES as a means of authenticating users must be vetted for privacy and security purposes and have authority to operate at the FCC.

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

CORES has a specific records schedule: N1-173-00-1 (03/01/2000).
Records may be retained (1) only until the output/reports are verified; (2) 3 months for paper and electronic forms (FCC Forms 160 series); (3) permanent retention for the Master Data Files and system and file specifications with instructions:

- Paper Forms (temporary records) – Destroy three (3) months after data are entered into the system and verified.

- Electronic Forms (temporary records) – Destroy three (3) months after data are entered into the system and verified.

- Master Data File (permanent records) – Download a copy of the data annually at the end of the calendar year. Transfer immediately to the National Archives.

- Output/Reports – Textual records needed for verification purposes.

    - Temporary records – Destroy when report(s) are verified.

- Documentation – Includes system specifications and file specifications with corresponding instructions.
    - Permanent records – Transfer annually to the National Archives with the Master Data File.

1.5. Data Security and Privacy

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

Confidentiality	**__High**	**XX Moderate**	**___Low**
Integrity	**__High**	**XX Moderate**	**___Low**
Availability	**__High**	**XX 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 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 staff and contractors in the Office of Managing Director (OMD), Financial Operations and Information Technology centers. Under appropriate circumstances, data showed within CORES or CORES log data may be provided to the OIG 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 System Security Plan (SSP). Any users requiring administrative privileges on the CORES system accounts must be approved by the System Owner.

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

Yes

The Privacy Manager keeps an accurate accounting of disclosures of information.