UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT FOR THE UNIVERSAL LICENSING SYSTEM 2.0 (ULS2)

JULY 2021

OFFICE OF THE GENERAL COUNSEL

WASHINGTON, DC 20554

Record of Approval

Document Approval		
Drafter Name: Olutoni Iyiola		**Bureau/Office: OMD/IR**
SAOP Approval		
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: 2021.07.23 12:21:23 -04'00'	**Date** 7/23/21	

Record of Approval

Date	Description	Name
7/6/2021	Validation of information – System Owner	Mary Deatrick
7/8/2021	Validation of completeness – IT Compliance Lead	Liem Nguyen

Universal Licensing System 2.0 (ULS2)

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 Universal Licensing System 2.0 (ULS2)
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Full Name, Date of Birth*, Home Address, Phone Number, Race/Ethnicity, Sex, Email Address, Work Address, Geolocation Information, and User ID. ***Note: Race, ethnicity and sex is voluntary provided by applicants. Individual applicants may provide a Home Address if they have no Work Address. Date of Birth is only required for specific, not all, radio service applicants.. *In the initial release, date of birth will not be collected for the market-based services. It will be collected at a later date.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? WTB- 1, Wireless Services Licensing Records
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 31 U.S.C. 7701; and 47 U.S.C. 301, 303, 309, 312, 362, 386, 507, and 510.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes, User ID, Email address/FRN will be shared with CORES – Financial Operation API which interfaces with Genesis.

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)]

Amazon Web Services (AWS)

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

Universal Licensing System 2.0 (ULS2) is hosted on FedRAMP Amazon Web Services (AWS).

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 collected PII data in ULS2 enables participants to research applications and licenses. This also provides the ability to search for applications and licenses by information such as a applicant/licensee name and address. It is also used to identify the point of contact for applications and licenses.

[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.

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.

PII will be collected from Individuals. In later releases, PII will be collected from third-party frequency coordinators for Market-Based services once the modernization moves to site-based services.

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

PII is only collected as part of the electronic application filing process. The FCC reviews the PII collected routinely to ensure we are only collecting the PII necessary to process applications and facilitate research.

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 and accuracy of the data at the time it is entered into the system. When an applicant files and application against the license (e.g., modification, renewal, administrative update), they ust certify that the information in the system is correct.

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?

User ID, Email address/FRN will be shared with CORES – Financial Operation API which also interfaces with Genesis. All internal connections are reflected within the Cyber Security Asset Management tool (CSAM).

[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.

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

C. How long will the PII be retained and how will it be disposed of?
PII will be retained and disposed of in accordance with FCC policy and the National Archives and Records Administration (NARA) General Records Schedule 6.4 (GRS 6.4). Which indicates to destroy when 3 years old, but longer retention is authorized if required for business use.

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. 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), ttps://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.

Universal Licensing System 2.0 (ULS2) does not inherit privacy controls from an external provider.

1.6. Access to the Information

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

FCC employees and contractors will have access to the PII in Universal Licensing System 2.0 (ULS2).

B. Does this system leverage Enterprise Access Controls?

Yes

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

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