UNITED STATES

FEDERAL COMMUNICATIONS COMMISSION

PRIVACY IMPACT ASSESSMENT (PIA) FOR THE UNIVERSAL LICENSING SYSTEM (ULS) 1.0 BOUNDARY

November 2023
Annual Review Date

OFFICE OF GENERAL COUNSEL

Washington DC, 20554

Next Review Cycle: September 2024

Record of Approval

Document Approval	
Drafter Name: Shannon Kendall (Contractor)	**Bureau/Office: Office of Managing Director (OMD), Information Resiliency (IR)**
SAOP Approval	
Printed Name: Elliot Tarloff	**Senior Agency Official for Privacy**
X ELLIOT TARLOFF Digitally signed by ELLIOT TARLOFF Date: 2023.11.01 14:39:33 -04'00' **Signature & Date**	

Record of Approval

Date	Description	Author
9/28/2023	Validation of information – System Owner	Diane Dupert
9/21/2023	Validation of Compliance	Liem Nguyen

Revision History

Date	Description	Name
6/1/2021	Validation of Information – System Owner	Diane Dupert
6/2/2021	Validation of Completeness	Liem Nguyen
4/28/2023	Template Update	ISSO – Shannon Kendall
6/5/2023	Review and Edits. Payfees FOSS removed and replaced with CORES 2 in Sections 4 (A).	ISSO System Owner – Diane Dupert
08/01/2023	Clerical edits and revisions to Sections 2, 3A-3C,	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff
08/10/2023	Requested edits to Sections 2, 3B, 4A-4B	SAOP ISSO
09/22/2023	Clerical edits and revisions to Sections 1.2, 1.3B-C, 1.4A-B,	SAOP
09/28/2023	Clerical edits reviewed and accepted	ISSO

Boundary for the Auction Bidding System & Flexible Auction Bidding System

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 is 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/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.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).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM Universal Licensing System (ULS)
NAME OF BUREAU Wireless Telecommunications Bureau (WTB) and Public Safety and Homeland Security Bureau (PSHSB)
DOES THE SYSTEM CONTAIN PII? Yes. Records in this system are retrievable by various identifiers, including those associated with individuals.
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) Contact information, voluntary demographic information, other personal information (for certain radio service applicants), and User ID.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPPLICABLE)? WTB- 1, Wireless Services Licensing Records FCC-2, Business Contact and Certification Information
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, 364, 386, 507, and 510.
DOES THE COMMISSION KEEP AN ACCURATE ACCOUNTING OF DISCLOSURES FROM THE SYSTEM AS REQUIRED BY SUBSECTION © OF THE PRIVACY ACT? Yes. The Privacy Team keeps an accounting of disclosures.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes, ULS 1 shares PII with FCC CORES 2 for applicant payment support and 3.5Ghz API for FSS Earth Station Antenna Site Data, FSS Call Sign Data

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 a cloud network specifically established for the boundary of the ULS systems and under the responsibility of the provider (Software as a Service or SaaS)

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

☐ 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)

☒ Not applicable, ATO boundary does not consist of cloud-based computing systems

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.

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 PII that is collected on a mandatory basis in ULS is required for entities to apply for and receive licenses, and for WTB and PSHSB to review and make decisions regarding those applications. The system also collects voluntary demographic data consistent with the provisions of the Communications Act, and certain other PII from a sub-set of radio service licenses. Public users and FCC internal users can search applications, licenses, and antenna structures using certain PII elements or other criteria such as a file number, applicant name, application purpose, call sign, licensee name, or radio service.

[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 is collected directly from applicants and licensees in certain frequency bands. For these frequency bands, Privacy Act Statements are provided in the relevant ULS Form Instructions and via a Privacy Act link in the online form.

In other frequency bands, PII is collected by third-party filers who do not require FRN accounts but manage application filings for other entities using their FRNs. Third party filers include certified Land Mobile and Microwave frequency coordinators, Commercial Operator License Examinations Managers (COLEMs), Volunteer Examiner Coordinators (VECs), and Spectrum Access Systems (or SASs). They establish their own systems to create tab delimited files with the required application data. Third party filers then use a GUI to upload to an EBF server, allowing ULS to ingest the data and create application forms.

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

PII is collected only as part of the application filing process. The FCC reviews the PII collected routinely to ensure the collection of only the PII necessary to process applications and coordinate licenses.

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 and accuracy of the data at the time it is entered into the system.

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?

PII is ingested directly from users (licensees and applicants) or indirectly from frequency coordinators on behalf of entities. PII from ULS is shared with the FCC CORES boundary.

[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.

All internal connections are reflected within the Cyber Security Asset Management tool (CSAM).

The FCC utilizes a specific application programming interface (API) for the 3.5Ghz band for applicants who wish to lease spectrum. Frequency coordinators use this API to file the requests for external applicants.

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")?

Yes, frequency coordinators utilize the 3.5Ghz API to file lease applications on behalf of applicants.

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.

Universal Licensing System (ULS) 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 within the Wireless Telecommunications Bureau and the Public Safety Homeland Security Bureau will have access to the PII in Universal Licensing System (ULS).

B. Does this system leverage Enterprise Access Controls?

Yes, all FCC common controls as they relate to FCC policy, e.g. AC-1.