Universal Service
Administrative Co.

PRIVACY IMPACT ASSESSMENT FOR USAC FINANCIAL SYSTEM (UNIFI)

July 19, 2024

Record of Approval

Document Approval		
USAC PRIVACY POC		
Laurence H. Schecker		**Senior Advisor - Associate General Counsel and Privacy Officer**
Signature DocuSigned by: Laurence Schecker 2AFA2492613041F...	**Date** 7/23/2024	
Accepted by:		
Elliot S. Tarloff		**FCC Senior Agency Official for Privacy**
Signature DocuSigned by: Elliot S. Tarloff 9000F2444A314E2...	**Date** 7/23/2024	

Version History

Date	Description	Author
10/10/2023	Draft	P.Gray
12/02/2023	Initial Draft Revision	IT Security ISSO
1/29/2024	Initial Draft Revision updates	OGC, ISSO
04/02/2024	Clerical and formatting edits and revisions to Section 1.2, 1.3B-D, 1.4A, 1.6C	Privacy Advisor – Katherine Morehead Senior Agency Official for Privacy (SAOP) – Elliot S. Tarloff
06/25/2024	Further clarifying edits to Sections 1.3A-C, 1.4A-B	SAOP – Elliot S. Tarloff
07/05/2024	Further edits and comments to 1.4D to unpack data transfers to third parties, including via API.	IT Security, ISSO

UNIFi

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 USAC Privacy Officer, in consultation with 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 of the E-Government Act, including a PIA. A PIA should not be completed until an IPA is completed and the SAOP makes a determination that a PIA is necessary.

If you have any questions, please contact the USAC Privacy Officer at privacy@USAC.org or the FCC 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).

INFORMATION ABOUT THE SYSTEM
NAME OF THE SYSTEM APPLICATION USAC Financial System (UNIFi)
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The UNIFi functionality requires USAC to use and store business (including sole proprietorship) information, including contact information, identification information, and financial information. Records are not retrievable from the front end of UNIFi by personal identifier.
IN WHAT SYSTEM OF RECORDS (SORN) IS THE INFORMATION CONTAINED (IF APPLICABLE)? FCC-2 Business Contacts and Certifications
WHAT ARE THE LEGAL AUTHORITIES FOR THE COLLECTION OF THIS PII? 47 U.S.C. 254; 47 CFR Part 54, Subpart H.
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? Yes. UNIFi data are shared with the FCC and the U.S. Treasury (via to Treasury/Pay.Gov) as part of confirming an entity's eligibility (including Red Light and Do-Not-Pay checks) to receive Universal Service Fund (USF) payments.

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 USAC receives/will receive from the cloud computing provider:

☐ USAC uses provider-supported application/s on the provider's cloud network (Software as a Service or SaaS)

☒ USAC has deployed application/s on the provider's cloud network and the provider supports the applications (Platform as a Service (PaaS) – Oracle Cloud Infrastructure

☐ USAC 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)

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.

UNIFi is the USAC financial accounting system used to handle operating expenses and payments for the Universal Service Fund (USF). It is used to support the USF support mechanisms by processing disbursements for all four USF programs (Rural Health Care, High Cost, Low Income, and Schools & Libraries) and congressionally appropriated funds (Affordable Connectivity Program and Emergency Connectivity Fund). UNIFi also collects USF contributions and other payments owed to the USF, and disburses payments to USAC vendors, USF program participants, and appropriated program participants. The information collected, maintained, and used in UNIFi permits USAC to process receipts and disbursements and administer the USF and appropriated programs.

[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 Notice[4] for each system that is included with the online or paper form the system(s) use(s) to collect the PII.

UNIFi does not collect information directly from outside groups but processes the information from USAC's E-File and Enterprise Data Warehouse (EDW) systems. The UNIFi functionality requires USAC to use and store business (including sole proprietorship) information, including contact information, identification information, and financial information. The UNIFi itself is not a designated federal system of records under the Privacy Act and thus, does not provide the specific privacy notice required by the Act. However, USAC has a privacy notice covering the collection of PII on its public facing website: https://www.usac.org/about/privacy-policies/

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

USAC collects PII only as directed by the FCC and as needed to perform the administration of USF and appropriated programs. Third parties are notified when they provide information using USAC systems that certain business information provided to USAC may become publicly available in connection with USAC's reporting obligations. Additionally, the UNIFi receives data from E-file and E-Rate Productivity Center (EPC). E-file and EPC use Data Universal Numbering Systems (DUNS) numbers as identifiers; these numbers are available only to entities with Employee Identification Numbers (EINs)—thereby reducing (but likely not eliminating) the frequency with which entities will need to share Social Security Numbers (SSNs) for identification purposes.

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

The information in the UNIFi is collected from USF contributors, program participants, or USAC vendors. These entities provide their own information and are responsible for ensuring that it is accurate, complete, reliable, and current. In addition, these entities can update their information as part of the annual and quarterly reporting requirements via FCC Form 498 (Service Providers) and FCC Form 499 (Contributors).

[4] A Privacy Act Notice 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.

UNIFi ingests PII from other systems. The E-File and EPC systems provide all users with warnings that PII is not to be entered beyond the minimal amount required. These data flow from these systems into UNIFi and are shared with the USAC Enterprise Data Services (EDS) which stores UNIFi data in the Enterprise Data Warehouse (EDW).

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. UNIFi data is initially transferred internally between the EDW database schemas, UNIFi_ODS and ERP schemas. Data is then transferred from the ERP schema via an API, using the Oracle Integration Cloud (OIC), to the UNIFi Oracle E-Business Suite (EBS) production database. Once the data is processed by the UNIFi application, it is encrypted at rest and transferred via the OIC Secure File Transfer Protocol (SFTP)—i.e., encrypted in transit—to the Department of Treasury.

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

The USF related records will be retained in accordance with the National Archives and Records Administration (NARA) Records Schedule Number DAA-0173-2017-001. The record retention period for USF records generally is 10 years or longer if needed for business or audit purposes. USAC corporate records are governed by USAC's record retention policy. USAC disposes of paper documents by shredding. Electronic data, files, and records are destroyed by electronic erasure in compliance with National Institute of Standards and Technology (NIST) guidelines.

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.

UNIFi implements controls in accordance with the USAC baseline for Moderate systems with PII. The UNIFi system is hosted in the Oracle Cloud Infrastructure (OCI) Government Cloud. UNIFi inherits platform encryption methodologies from OCI. To prevent unauthorized disclosure of data, data are encrypted at rest, utilizing a FIPS 140-3 compliant industry-standard AES-256 or higher robust encryption algorithm. Data in transit are encrypted using TLS 1.2 or greater.

Auditing is performed for alter database statements and modifications to database user accounts and privileges. This is enabled within the database in real time. Additionally, in compliance with USAC's Information Security and Privacy Policy, auditing is conducted for high-privileged users, local direct access to the database, actions by users that have database access, data-security events, and database-management events. Monitoring of sensitive data access and updates are performed.

All logs are aggregated and ingested into a security information and event management tool for monitoring and reporting.

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.

The UNIFi system security controls are partially inherited from USAC General Support Systems (GSS) security controls, USAC enterprise common controls (ECC), Oracle Cloud Infrastructure, and IBM Smart Cloud for Government (SCG).

1.6. Access to the Information

A. Which types of users will have access to the PII in this information system?

Access to PII in UNIFi is limited to USAC and FCC staff on a least-privilege and need-to-know basis. Reports regarding UNIFi activities may potentially include information about specific business entities and contact information. USAC may also generate and provide UNIFi reports pursuant to inquiries received under applicable laws.

B. Does this system leverage Enterprise Common Controls (ECC)?

Yes, the UNIFi system security controls partially inherit from USAC GSS security controls, USAC enterprise common controls (ECC), OCI, and SCG. OCI and SCG are both FedRAMP authorized.

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

Yes