PRIVACY IMPACT ASSESSMENT FOR HIGH-COST LOW INCOME 2.0 (HCLI 2.0)

05/23/2024

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** 5/23/2024	
Accepted by:		
Elliot S. Tarloff		**FCC Senior Agency Official for Privacy**
Signature DocuSigned by: Elliot S. Tarloff 9000F2444A314E2...	**Date** 5/23/2024	

Version History

Date	Description	Author
5/23/2024	Final Version	Matthew Sneed, Laurence Schecker, Mitchell Calhoun, and Max Mansur

High-Cost Low Income 2.0

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 High-Cost Low Income 2.0
DOES THE SYSTEM CONTAIN PII? Yes
PLEASE PROVIDE A BRIEF DESCRIPTION OF THE PII (IF APPLICABLE) The PII collected in HCLI 2.0 includes contact information to verify HCLI 2.0 carriers.
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 C.F.R. Part 54 Subparts D, M, and O
DOES THIS SYSTEM SHARE THE PII WITH OTHER SYSTEMS? No, information and data are not shared to external systems.

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)) [Appian Cloud]

☒ 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) [AWS Commercial Cloud]

The HCLI 2.0 system boundary will operate as an internal application within USAC's existing Appian Cloud instances, as well as having the back end running in USAC's existing AWS Cloud environment.

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.

The HCLI 2.0 system processes business contact information to facilitate the identification of and communication with individuals regarding USF disbursements to their respective companies. This business contact information is crucial for the effective administration of the HCLI program because it enables appropriate coordination and communication with filing entities.

[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.

The collection of business contact information occurs through the HUBB application within USAC's High Cost Broadband Portal (HCBP) system. There is no direct collection of user data or information from non-USAC sources to the HCLI 2.0 system.

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

HCLI 2.0 exclusively gathers business contact information. This data serves the purpose of identifying appropriate points of contact for carriers to allow for necessary communication and coordination.

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

The HCLI 2.0 application receives business contact information, including full name, business email address, and business phone number, from the HUBB application within the HCBP system. This data are not stored within HCLI 2.0's Relational Database Service (RDS), as a proactive measure to ensure the accuracy and completeness of the business contact information. It is the responsibility of each carrier to ensure the accuracy, completeness, and timeliness of information provided for its point of contact. HCLI 2.0 affords carriers the opportunity to update and correct information as necessary.

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.

PII contact information is ingested via automated process from HCBP's HUBB application. No PII is shared with other systems.

[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.

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")?

HCLI 2.0 is a USAC internal system and will not be sharing any information with third parties.

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

The HCLI 2.0 application retains all data as required by the FCC's requirements and adopted in the USAC data retention schedule. HCLI 2.0 retention schedules are approved by the National Archives and Records Administration (NARA) and require retention for 10 years (or longer if there is a business need to retain the records). USAC adheres to National Institute of Standards and Technology (NIST) guidelines for the destruction of records. Please refer to NARA RECORDS NUMBER DAA-0173-2017-0001-0003, for more information.

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**	**___Moderate**	**_X_Low**

B. Discuss the physical, administrative, and technical controls in place to protect the data in the system.

The HCLI 2.0 front-end is hosted within Appian Cloud, which resides in FedRAMP authorized Appian cloud instance. USAC employee, contractor, and vendor access to Appian Cloud is controlled through USAC's IT security and privacy policies and procedures. These are a comprehensive and dynamic set of security and privacy protocols with features designed to meet applicable Federal IT security and privacy standards. A limited group of authorized USAC Appian Cloud system administrators have access to all Appian Cloud data on a need-to-know basis. All user access to the Appian Cloud is controlled via the role-based security features. Other user access to supporting files and folders is granted to individual users on an as needed basis using the least privilege principle.

The HCLI 2.0 back-end is hosted in AWS Commercial Cloud, which resides in FedRAMP authorized AWS East/West instance.). HCLI 2.0 data between USAC and non-USAC systems is protected through firewalls and secured sockets layer (SSL) encryption, and

indirect transfers of data are protected by encryption or comparable security safeguards. HCLI 2.0 will use a Relational Database Service (RDS) cluster that uses encrypted storage volumes for both primary and replica instances, as well as encrypting backups and snapshots for database. Documents stored in AWS S3 will also be encrypted. AWS Commercial Cloud user access to HCLI 2.0 is controlled via the role-based security features.

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.**

HCLI 2.0 doesn't inherit privacy controls from an external provider, other than the FedRAMP authorized hosts on which the application is built.

1.6. Access to the Information

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

USAC's internal HCLI 2.0 users can view business contact information within the system.

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

Yes, HCLI 2.0 inherits controls from USAC's ECC.

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

Yes.