Universal Service Administration Company

Privacy Impact Assessment (PIA) for the
National Verifier Lifeline Eligibility Database

October 17, 2017

Submitted to:
Johnnay Schrieber
Director of Privacy
Telephone Number: 202-423-2604
Email address: Johnnay.Schrieber@usac.org

Prepared by:
James Lee
Director of Lifeline
Telephone Number: 202-772-4520
Email address: James.Lee@usac.org

The *Privacy Act of 1974*, as amended, 5 U.S.C. § 552a, requires Federal agencies to take special measures to protect personal information about individuals when the agencies collect, maintain, and use such personal information.

The Privacy Impact Assessment's[1] purpose is to help USAC to evaluate the changes in the information in the system and to make the appropriate determination(s) about how to treat this information, as required by the Privacy Act's regulations.

Section 1.0 Information System Status:

1.1 Status of the Information System:[2]

☒ New information system—Implementation date: December 5, 2017
☐ Revised or upgraded information system -

If this system is being revised—what will be done with the newly derived information:

☐ Placed in existing information system—Implementation Date:
☐ Placed in new auxiliary/ancillary information system—Date:
☒ Other use(s)—Implementation Date:

Please explain your response:

The Lifeline Eligibility Database (LED) is the system of record for the National Verifier, which will be used to verify eligibility for Lifeline subscribers. Its primary objectives are to verify eligibility of new applicants and existing Lifeline subscribers and to prevent duplicate Lifeline benefit claims.

1.2 What changes are being made to the information system:

☐ Changes to the operating system:
☐ Changes to the categories of information being collected:
☐ Changes to the categories of individuals affected:
☐ Other changes:

Explain your response:

1.3 Has a Privacy Threshold Assessment (PTA) been done?

☒ Yes
Date: October 13, 2017

☐ No

If a PTA has not been done, please explain why not:

SECTION 2: PERSONALLY IDENTIFIABLE INFORMATION (PII) IN SYSTEM

2.1 What are the categories of individuals from whom the PII is collected?

[1] This questionnaire is used to analyze the impacts on the privacy and security of the personally identifiable information (PII) that is being maintained in these records and files.
[2] "Information system" is a general term that refers to electronic databases, licensing, and records systems and formats and also to paper based records and filing systems.

The categories of individuals in this system include those individuals (residing in a single household) who are applying for or have applied for federal universal service Lifeline program benefits; are currently receiving Lifeline benefits; are minors whose status qualifies a parent or guardian for Lifeline benefits; or who have received benefits under the Lifeline Program, which serves low-income individuals by providing these qualifying individuals with federal universal service discounts on telephone and/or broadband service for their household.

The LED will collect, use, and maintain PII in its databases and files that includes, but is not limited to: individual applicant's first and last name; residential address; information on whether the individual resides on Tribal lands; information on whether the address is temporary and/or descriptive and whether it includes coordinates; mailing address (if different); date of birth; last four digits of social security number (SSN) or Tribal identification number; telephone number; full name of the qualifying person (if different from the individual applicant); qualifying person's date of birth; the last four digits of the qualifying person's SSN or their Tribal identification number; information on whether the qualifying person resides on Tribal lands; means of qualification for Lifeline (i.e., income or relevant program participation); documents demonstrating eligibility; individual contact information; Lifeline subscriber identification number; security questions; answer to security questions; user name; password; agent identification information (if an agent is assisting in completing the application); individual applicant's eligibility certifications; individual applicant's signature and date of application; Lifeline service initiation date and termination date.

In addition, users in LED include service provider users who may use the LED to assist their subscribers confirm eligibility for the Lifeline program. Limited information regarding service provider users will be collected by LED, including name and email address of the sale agent which are needed to provide access to the LED.

2.2 What are the categories of PII that are being collected?

The categories of records in the LED include: The individual's first and last names; residential address; mailing address; date of birth; last four digits of SSN; information on whether the address is temporary and/or descriptive and whether it includes coordinates; mailing address (if different); Tribal identification number; telephone number; means of qualification and eligibility for Lifeline (i.e., income or relevant program participation); full name of the qualifying person (if different from the individual applicant); qualifying person's date of birth; the last four digits of the qualifying person's SSN or their Tribal identification number; information on whether the qualifying person resides on Tribal lands; means of qualification for Lifeline (i.e., income or relevant program participation); documents demonstrating eligibility; individual contact information; Lifeline subscriber identification number; security questions; answer to security questions; user name; password; agent identification information (if an agent is assisting in completing the application); individual applicant's eligibility certifications; individual applicant's signature and date of application; Lifeline service initiation date and termination date..

and current enrollment status in the National Lifeline Accountability Database (NLAD).

In addition, LED collects limited information regarding service providers who are users of the system, including first and last name and email address of the sales agent, which are necessary to establish account access for LED. The LED also collects and stores the IP address of all users who attempt or has logged into the LED.

2.3 What is being done to limit or eliminate the collection of PII?

Only the PII elements mandated for collection by the Federal Communication Commission (FCC) rules (i.e., 47 C.F.R. §§ 54.407, 54.410(d)), or absolutely necessary to manage the Lifeline program are collected by the LED system. In addition, LED utilizes role-based permissions so that only authorized users have access to PII as necessary. Sensitive PII such as date of birth or the last four digits of SSNs is not displayed or available via reports to external users of LED. Only a limited number of authorized USAC Lifeline program staff have access to view reports of sensitive PII such as date of birth or last four digits of SSN that is stored in LED, which is necessary to support data requests for audits or program reviews by USAC and/or the FCC. No other users will have access to sensitive PII data reports within LED. USAC's business process outsource (BPO) contractor staff who process manual documents submitted for review (i.e., identity proof documents submitted by a Lifeline applicant where the automated verification check cannot confirm a person's identity) will only have access to review the document submitted one by one as the documents are processed, but will not have report access that enables a user to view multiple records within LED that contain sensitive PII.

2.4 If applicable, what is being done to limit the collection of Social Security Numbers?

Only the last four digits of SSNs are ever collected or stored in LED for the purpose of automated verification. The collection of the last four digits of SSN is necessary for the system to perform an identity verification check for Lifeline subscribers and to verify that the individual not receiving Lifeline support from multiple service providers. The FCC rules limit Lifeline program support to one benefit per a household. System programming ensures that for the input field for SSN in LED, that only four digits are accepted, and entry greater than four digits is prevented. In addition, any external reports from LED will not include the last four digits of the SSN or data of birth data elements. In the event that an applicant submits a copy of a Social Security Card to verify their identity in a dispute process for a failed identity check, such documents are first redacted by the National Verifier staff prior to storage in LED so that it only displays the last four digits. Access to manually processed documents are restricted to certain USAC staff or its BPO contractor staff on a role-based permission basis and only to the degree necessary to perform their job functions (e.g., for only the time period required to review and make a determination to accept or deny proof documents for eligibility or identity).

2.5 What are the purposes for collecting, maintaining, and using the PII?

The Lifeline Program provides federal universal service discounts for voice telephony and/or broadband service, and the initial connection charge in Tribal areas to support

such service, to qualifying low-income individuals (i.e., one Lifeline telephone service per household). Individuals may qualify for Lifeline through proof of income or proof of participation in a qualifying program (i.e., Medicaid, Supplemental Nutritional Assistance Program (SNAP), etc.). The Lifeline Program system of records notification (SORN)[3] covers the PII that the eligible telecommunications carriers (ETCs) or individual Lifeline applicant must provide to confirm the subscriber's eligibility for the Lifeline program and to prevent the individuals in a single household from receiving more than one Lifeline Program benefit, as required by 47 C.F.R. §§ 54.404 and 54.410. The Lifeline Program SORN also covers the PII that enables USAC to recertify the eligibility of current Lifeline Program subscribers for subscribers residing in states where the National Verifier function as been established, as required by 47 C.F.R. § 54.410. The PII in WCB-1/Lifeline Program SORN will include:

1. The information that is used to verify an individual's identity and eligibility to participate in the Lifeline Program by the National Verifier functions administered by USAC.
2. The information used by USAC to recertify Lifeline subscribers in those areas where the National Verifier is responsible for recertification of a subscriber's Lifeline eligibility.
3. The information that is used to recertify an individual's continued eligibility to participate in the Lifeline Program and to be recertified using the National Verifier in areas where the National Verifier is responsible for recertification of a subscriber's Lifeline eligibility.
4. The information that is used to determine whether an individual in a household, who is applying for a Lifeline Program benefit, is already receiving a Lifeline Program benefit from one or more providers. In order to determine if this information is in fact accurate, the information is confirmed with a third-party verification service not in the control of USAC or the Commission;
5. The information that is contained in the records of the inquiries that the ETCs will make to the Lifeline Program contractor's call center to verify that an individual is eligible to participate in the Lifeline Program.
6. USAC will designate a third party contractor to establish this call center as part of USAC's "exception management practices." The contractor will operate this call center, which individuals may use who are seeking to participate in or are already participating in the Lifeline Program. These individuals may call the center to ensure that they have not been improperly denied access to Lifeline Program benefits through the verification process. Any information generated by these inquiries will constitute a separate, distinct database, which will include, but is not limited to, recordings of live agent calls to be stored for 30 days from the date of the call, identity of the user initiating the request, brief description of the request, type of request, identification of the USAC-approved script used in responding to the request, resolution status, and whether the request was escalated (i.e., if the agents escalates the issue to the agent's manager or USAC program personnel). This information will be used, among other things, to verify the accuracy of the information stored in the Lifeline system *(*i.e., to determine the accuracy of the PII provided by the ETC or individual Lifeline applicant). Records in the Lifeline system are available for public

[3] The SORN for LED known as "FCC/WCB-1, Lifeline Program," published in the Federal Register on August 15, 2017. (82 Fed. Reg. 38686).

inspection after redaction of information that could identify the individual participant, such as the individual's name(s), date of birth, last four digits of social security number, tribal ID number, telephone number, or other PII.

8. USAC will designate a third-party contractor to develop, test, and operate the database and system network. The contractor will establish the core database and automated connections to other databases. This information will be used, among other things, to develop technical parameters for database connections and matching criteria.
9. USAC will designate a third-party business process outsourcing (BPO) contractor to perform and review eligibility determinations where the National Verifier is responsible for such processes for the purpose of performing manual eligibility verification (when needed) and to assist in dispute resolution. The BPO may collect copies of documentation that support an individual's eligibility to receive federal Lifeline program benefits.

2.6 What does this information system do with the PII:

☐ The system collects PII, but it will not perform any analyses or manipulation of the PII.
☒ The system will derive new or create previously unavailable information through manipulation, aggregation, consolidation, and/or analysis of this PII.

2.7 What are the potential privacy impacts on the individuals whose PII is manipulated and/or analyze by the information system:

☒ The PII will be used to produce reports on the individuals;
☒ The PII will be included in the individual's records;
☒ The PII will be used to make a determination about an individual;
☐ The PII will be used for other purposes that have few or no impacts on the individuals.

Please explain your response (including the magnitude of any impacts):

The PII information that is collected regarding Lifeline subscribers is used to determine whether an individual within a household, who is applying for a Lifeline Program benefit, is eligible to receive Lifeline program support and whether that individual is already receiving a Lifeline Program benefit from one or more providers, verify the identity of the individual, and to confirm the validity of address information submitted. If a subscriber is eligible for support because of qualifying beneficiary, the qualifying beneficiary's PII will be collected and used to determine whether the individual is eligible to receive Lifeline program support and whether the individual is already to receiving a Lifeline program benefit from one or more providers, verify the identity of the qualifying beneficiary, and to confirm the validity of the address information submitted. Automated eligibility verifications are confirmed by LED when it receive a "yes" or "no" response in regards to whether the individual is eligible via a qualifying program by querying external data sources (i.e., federal and/or state eligibility program eligibility data sources). LED utilizes role-based permissions so that only authorized users have access to PII on a strict "need to know basis." Sensitive PII such as date of birth or the last four digits of SSN is not displayed or available via reports to external users of LED. Only a limited number of authorized USAC Lifeline program staff have access to view sensitive PII such as date of birth or last four digits of SSNs that is stored

in LED, which is necessary to support data requests for audits or program reviews by USAC and/or the FCC. LED is only utilized for its intended use in support of verifying and managing subscribers for the Lifeline program and the routine uses described in the SORN.

2.7 Who will have access to the PII in the reports?

LED utilizes role-based permissions so that only authorized users have access to PII as necessary. Sensitive PII such as date of birth or the last four digits of SSNs is not displayed or available via reports to external users of LED. Only a limited number of authorized USAC Lifeline program staff have access to view sensitive PII such as date of birth or last four digits of SSNs that is stored in LED, which is necessary to support data requests for audits or program reviews by USAC and/or the FCC.

In addition, service provider users (i.e., a single sales agent) can access reports regarding his/her own subscribers that they have assisted in the submission of an eligibility verification request in LED only if he/she had previously submitted this PII into LED. (However, sensitive PII such as date of birth or last four digits of SSN are not contained in reports available to service providers). The service providers will only be able to review information for applications that they submitted into LED, but the access will not include the subscriber's sensitive PII, such a DOB and SSN. The access is limited to a per user level.

2.8 What are the sources (individuals) for the PII:

PII is entered by individual Lifeline subscriber (i.e., Lifeline program applicant) and service providers assisting subscribers as part of the requirement to have the subscriber's eligibility confirmed by the National Verifier (via automated verification processes enabled by the LED) for the Lifeline program prior to enrolling a subscriber for Lifeline supported service. The PII is collected from the individual Lifeline subscriber as part of the application process for receiving the federal Lifeline program benefit. Individual Lifeline subscriber must provide their affirmative consent to the collection, use, and retention of their PII as part of the application process and as part of the eligibility verification process within LED.

2.9 What are the legal authority(s) for collecting and maintaining the information?

47 U.S.C. §§ 151-154, 201-205, 214, 254, 403. 47 C.F.R. §§ 54.404-54.410.

SECTION 3: RECORDS RETENTION AND DISPOSAL

3.1 How is the information retrieved or accessed?

Individual subscribers and service providers will enter information through the publicly available web portal for the LED. Individual subscribers will be able to access LED by creating user accounts with username and password credentials that are entered within the

LED. USAC and BPO contractor staff will access and retrieve data from LED through role-based permissions based on "least privilege."

3.2 What are the policies for the storage and maintenance of the information?

Per USAC IT Security Policy, storage and maintenance of information is to adhere to guidance in accordance with NIST guidance, SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." All of the PII within LED is stored encrypted and can only be access through role-based permissions.

3.3 Does this information system have a records retention and disposition schedule approved by the National Archives and Records Administration (NARA)?[4]

The National Archives and Records Administration (NARA) has not established a records schedule for the information in the Lifeline Program system of records. Consequently, until NARA has approved a records schedule, USAC will maintain all information in the Lifeline Program system of records in accordance with NARA records management directives. The 2012 *Lifeline Reform Order* states that information in the Lifeline Program is maintained for ten years after the consumer de-enrolls from the Lifeline Program. *See Lifeline and Link Up Reform and Modernization, et al.*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6740, para. 195 (2012).

If so, how long, and for what reason(s) does USAC retain the information?

Until NARA has approved a records schedule, USAC will maintain all information in the Lifeline Program system of records in accordance with NARA records management directives. The 2012 *Lifeline Reform Order* states that information in the Lifeline Program is maintained for ten years after the consumer de-enrolls from the Lifeline Program. *See Lifeline* R*eform Order,* FCC Rcd at 6740, para. 195.

How is the information destroyed when it is no longer needed?

Disposal of obsolete or out-of-date paper documents and files is by shredding only. Electronic data, files, and records are destroyed by electronic erasure.

3.4 Has a system of records been created to cover this PII, and if so please provide the name and Federal Register citation and publication date:

The system of records notification (SORN) for this system was published on August 15, 2017, and became effective on September 14, 2017. *See* 82 Fed. Reg. 38686.

If the system is being upgraded, will the SORN require modification?

[4] Has this records retention and disposal schedule been approved by the National Archives and Records Administration (NARA)?

LED is not being updated. Any future changes will be assessed to determine if the SORN may require modification.

SECTION 4: CORRECTION AND REDRESS

4.1 How do individuals inquire whether this information system contains their PII?

Individuals wishing to determine whether LED contains information about them may do so by writing to the Universal Service Administrative Company (USAC), 700 12th Street NW., Suite 900, Washington, DC 20005; or Wireline Competition Bureau (WCB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554; or Leslie F. Smith, Privacy Manager, Information Technology (IT), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554, or email Leslie.Smith@fcc.gov. Individuals must furnish reasonable identification by showing any two of the following: Social security card; driver's license; employee identification card; Medicare card; birth certificate; bank credit card; or other positive means of identification, or by signing an identity statement stipulating that knowingly or willfully seeking or obtaining access to records about another person under false pretenses is punishable by a fine of up to $5,000.

Individuals requesting access must also comply with the FCC's Privacy Act regulations regarding verification of identity and access to records (47 C.F.R. Part 0, Subpart E).

4.2 How do individuals gain access to their PII in this information system's records?

Individuals wishing to determine whether LED contains information about them may do so by writing to the Universal Service Administrative Company (USAC), 700 12th Street NW., Suite 900, Washington, DC 20005; or Wireline Competition Bureau (WCB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554; or Leslie F. Smith, Privacy Manager, Information Technology (IT), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554, or email Leslie.Smith@fcc.gov. Individuals must furnish reasonable identification by showing any two of the following: Social security card; driver's license; employee identification card; Medicare card; birth certificate; bank credit card; or other positive means of identification, or by signing an identity statement stipulating that knowingly or willfully seeking or obtaining access to records about another person under false pretenses is punishable by a fine of up to $5,000.

4.3 How can individuals seek to correct or to amend their PII this information system?

Individuals wishing to correct or amend their PII in LED may do so by writing to the Universal Service Administrative Company (USAC), 700 12th Street NW., Suite 900, Washington, DC 20005; or Wireline Competition Bureau (WCB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554; or Leslie F. Smith, Privacy Manager, Information Technology (IT), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554, or email Leslie.Smith@fcc.gov. Individuals must furnish reasonable identification by showing any two of the following: Social security card; driver's license; employee identification card; Medicare card; birth certificate; bank credit card; or other positive

means of identification, or by signing an identity statement stipulating that knowingly or willfully seeking or obtaining access to records about another person under false pretenses is punishable by a fine of up to $5,000.

Individuals requesting access must also comply with the FCC's Privacy Act regulations regarding verification of identity and access to records (47 C.F.R. Part 0, Subpart E).

4.4 How does USAC provide redress for individuals to seeking to amend or correct their PII in this system?

Individuals wishing to amend or correct their PII in LED may do so by writing to the Universal Service Administrative Company (USAC), 700 12th Street NW., Suite 900, Washington, DC 20005; or Wireline Competition Bureau (WCB), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554; or Leslie F. Smith, Privacy Manager, Information Technology (IT), Federal Communications Commission (FCC), 445 12th Street SW., Washington, DC 20554, or email Leslie.Smith@fcc.gov. Individuals must furnish reasonable identification by showing any two of the following: Social security card; driver's license; employee identification card; Medicare card; birth certificate; bank credit card; or other positive means of identification, or by signing an identity statement stipulating that knowingly or willfully seeking or obtaining access to records about another person under false pretenses is punishable by a fine of up to $5,000.

Individuals requesting access must also comply with the FCC's Privacy Act regulations regarding verification of identity and access to records (47 C.F.R. Part 0, Subpart E).

4.5 Are there any exemptions to the notification, access, and correction, and/or amendment procedures for individuals seeking information about themselves?

No.

SECTION 5: MANAGEMENT AND TRAINING

5.1 What policies determine who is authorized and granted access to the system's information?

The electronic records maintained in LED are protected by USAC's IT privacy safeguards and policies, which comprise a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal IT privacy standards, including those required by the National Institute of Standard and Technology (NIST) and the Federal Information Security Management System (FISMA). In addition, access to the electronic files is restricted to authorized USAC and contractors' staff who use or maintain LED on a "need to know" basis and for an authorized purpose.

If contractors do not have access to the system's information, please skip to Question 6.1.

5.2 How does USAC ensure that the employees and contractors with access to the system's PII comply with their duties and responsibilities under the Privacy Act?

USAC employee and contractor access to electronic records maintained in LED are controlled through USAC's IT privacy safeguards, policies, and procedures which comprise a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal IT privacy standards, including those required by NIST and FISMA. The contracts with the Business Process Outsource (BPO) vendor includes the Privacy Act contractual requirements and the BPO will implement a Privacy Program Compliance Plan for its employees and any subcontractors that will be collecting, processing, handling, and retaining PII from Lifeline subscribers. In addition, all USAC staff and contractors with access to LED will receive and certify receipt of role-based privacy training.

5.3 What specialized training is provided to employees and contractors who have access to the PII?

USAC employees and USAC contractors must take security and privacy awareness training prior to be given access to PII within LED or to USAC information systems. USAC will be rolling out additional role-based privacy training for employees and contractors who collect, process, handle and manage PII in third quarter 2017. In addition the BPO vendor will implement a Privacy Program Compliance Plan for its employees and any subcontractors that will be collecting, processing, handling, and retaining PII from Lifeline subscriber. The Privacy Program Compliance Plan will include all required mandatory security and privacy training, including role-based training.

5.4 How often do these employees and contractors receive re-training?

Privacy awareness training and any required role-based privacy training is provided on an annual basis. The training requirements flow down to all contractors and subcontractors with direct access to PII via contractual requirements.

5.5 Do the training requirements meet Federal Information Security Management Act (FISMA) standards?

Yes.

SECTION 6: COLLECTING AND SECURITY THE INFORMATION

6.1 How will the information system collect an individual's PII: (Choose all the apply.)

☒ The information system has a link to the USAC's Internet address at www.checklifeline.org or www.usac.org, or other customer-facing URL
☒ The information system has a customer-facing web site via the USAC Intranet for USAC employees;
☐ The PII is collected by e-mail;
☐ The PII is collected by social media website(s);
☒ The PII is collected from a FCC form, license, or other document:
☒ The PII is collected by regular mail; and/or
☒ The PII is collected by orally via telephone or visually (VRS) notification:

Please explain your response: The LED will have a public URL and can be accessed by USAC staff, USAC contractors, individual subscribers or ETCs for the express purpose included in the Lifeline SORN. Eligibility and identity documents may also be physically mailed to USAC's National Verifier BPO for processing. The BPO call center may also collect PII information from subscribers over the phone such as name, date of birth, and only the last four digits of SSN to support Lifeline subscribers in the eligibility verification process. The individual subscriber must provide his/her affirmative consent to collect, use, and store his/her PII when they apply for, inquire about their own service, or to recertify for Lifeline benefits. The individual subscriber will also provide his/her affirmative consent to the collection, use, sharing, and retention of their PII when they confirm eligibility through the LED. Information regarding Lifeline subscribers will not be provided to service providers over the phone without first receiving affirmative consent from the subscriber.

6.2 How are individuals advised of their privacy rights when they provide their PII?

- ☒ There is a link to the Privacy Notice at www.checklifeline.org:
- ☐ A Privacy Notice is displayed on the social media webpage:
- ☒ A Privacy Notice is printed at the end of the form(s), license(s), and/or other document(s):
- ☐ The USAC Intranet site displays a Privacy Notice:
- ☒ The collection or input mechanism uses another method to provide individuals with the Privacy Notice such as an oral (telephone) or visual (VRS) notification:
- ☐ No Privacy Notice is provided:

6.3 If a Privacy Notice is provided, which of the following are included?

- ☒ Proximity and timing—the privacy notice is provided at the time and point of data collection.
- ☒ Purpose—describes the principal purpose(s) for which the information will be used.
- ☒ Authority—specifies the legal authority that allows the information to be collected.
- ☒ Conditions—specifies whether providing the information is voluntary, and the effects, if any, of not providing it.
- ☒ Disclosures—specify the routine use(s) that may be made of the information.
- ☐ Not applicable, as information will not be collected in this way.

Please explain your response:

Pursuant to 47 C.F.R. §54.404(b)(9), service providers must provide disclosures and obtain consent prior to submitting PII to LED. The FCC rule specifically requires that "[a]ll eligible telecommunications carriers must obtain, from each new and existing subscriber, consent to transmit the subscriber's information. Prior to obtaining consent, the eligible telecommunications carrier must describe to the subscriber, using clear, easily understood language, the specific information being transmitted, that the information is being transmitted to the Administrator to ensure the proper administration of the Lifeline program, and that failure to provide consent will result in subscriber being denied the Lifeline service." This language is currently included on the application and

recertification forms that are completed by individuals to receive Lifeline benefits. In addition, when individual access the LED, on the first screen there is a link to the Privacy Act Statement. The individuals will have access to the Privacy Act Statement prior to entering any PII into the LED.

6.4 Do individuals have the right to decline to provide their PII?

Yes, but the failure to provide consent or the required PII would prohibit the individual from being able to qualify for, apply for and to enroll in the federal Lifeline program.

6.5 How do individuals provide consent for their PII to be used?

Consent may be provided in various formats, in writing or verbally. Consent to collect, use, share and retain the individual's PII is obtained from the individual when they access the LED to verify eligibility. Individuals also provide their consent to the collection, use, sharing and retention of their PII when they apply for or recertify for Lifeline benefits.

6.6 May individuals consent to partial and/or particular uses of their PII?

No. As provided in the FCC rules, individuals are required to provide certain information, including, name, address, phone number, DOB, and last four digits of social security number in order to apply for and receive federal Lifeline benefits.

6.7 What are the potential consequences for refusing to provide PII:

Per FCC rules, the failure to provide consent or the required PII information will result in the individual being unable to qualify for, apply for and receive federal Lifeline benefits.

SECTION 7: INFORMATION SHARING

7.1 Does this system share/transmit information with other non-USAC information systems shared?

Yes.

1. PII is also shared with a non-USAC third party identity verification provider, that is contracted to verify the identity of subscribers prior to entry into the LED system.
2. Address information is shared with the USPS's automated address verification service that is contracted to verify the validity of an address prior to entry into the LED.
3. PII (name, date of birth, and last four digits of SSN) is shared with federal and state data sources where the National verifier is implemented that provide automated yes/no responses to enrollment in a qualifying Lifeline eligibility program (e.g. SNAP or Medicaid), as available. As of the date of this PIA, the National Verifier is connected with the U.S. Department of Housing and Urban Development (HUD), Mississippi, New Mexico, Colorado, and Utah.

7.2 How is this external information sharing compatible with the purposes for collecting, using, and retaining this PII?

The external information sharing is compatible with the purpose of collecting, using, and retaining PII under the SORN's routine uses for the prevention of fraud, waste, and abuse for the Lifeline program and confirming the accuracy of information entered to LED.

7.3 Are there restrictions on the re-dissemination of this PII by the other party(s)?

Yes, re-dissemination of PII in LED can only occur under the provisions listed in the SORN and in accordance with the Computer Matching Agreements.

7.5 What security measures protect the shared/transmitted PII and prevent unauthorized access?

Access to electronic records maintained in LED are controlled through USAC's IT privacy safeguards, policies, and procedures which comprise a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal IT privacy standards, including those required by NIST (i.e., NIST SP 800-53) and FISMA. Any parties receiving access to PII data within LED are contractually required to protect and secure the data according to USAC's policies and procedures and the terms of the Computer Matching Agreements.

7.6 What kind of agreement permits this matching or data sharing arrangement?

USAC shares the data in accordance with the routine uses included in the SORN, and adheres to the Privacy Act of 1974, as amended (5 U.S.C. § 552a) requirements. USAC and the FCC have executed Computer Matching Agreements with the federal and states agencies where LED is sharing PII to confirm the individual's eligibility to receive federal Lifeline program benefits.

7.7 Is this a new or a renewed matching agreement?

☒ New matching agreement
☐ Renewed matching agreement

Please explain your response: LED is a new system and notice of the computer matching agreements are publicly posted in the Federal Register. USAC and the FCC will also post copies of the executed Computer Matching Agreements on their respective websites.

7.8 Has the FCC's Data Integrity Board (DIB) reviewed and approved the matching agreement(s)?

☒ Yes –approval data: The Computer Matching Agreements with the states (UT, NM, CO, and MS) were approved by the FCC DIB on July 27, 2017. The FCC DIB approved the Computer Matching Agreement with HUD on April 11, 2017.
☒ No

Please explain your response: The FCC Data Integrity Board did not approve the contract with the vendor to provide third-party identification verifications services to LED. However, this was not a computer matching agreement that falls within the scope

of the Privacy Act. The FCC required USAC to engage with a third-party identification verification vendor to confirm the identity of individuals who apply for and receive Lifeline benefits and approved the contract with the vendor.

SECTION 8: DATA QUALITY REQUIREMENTS

OMB regulations require Federal agencies to ensure that the information they collect and use meets the Federal Data Quality standards for Confidentiality, Integrity, and Availability of the PII.

If this information system does not collect PII from FCC sources, please skip to **Question 8.2**.

8.1 How is the PII checked to ensure it meets the Data Quality guidelines? (Please check all that apply.)

- ☐ Information is processed and maintained only for the purposes for which it is collected.
- ☐ Information is reliable for its intended use(s).
- ☐ Information is accurate.
- ☐ Information is complete.
- ☐ Information is current.
- ☐ Not applicable:

8.2 If PII is collected from non-FCC sources, how is it checked for adherence to the Data Quality guidelines? (Please check all that apply and provide an explanation)

- ☒ Information is processed and maintained only for the purposes for which it is collected:
- ☒ Information is reliable for its intended use(s):
- ☒ Information is accurate:
- ☒ Information is complete:
- ☒ Information is current:

Please explain any exceptions or clarifications:

The data found within LED is entered by prospective or current Lifeline subscribers and service providers on behalf of the individual Lifeline subscriber. Both service providers and the Lifeline subscribers certify under perjury of the law that they are providing accurate, complete, current data when it is entered into LED. Field level validation controls are used in LED to ensure that one cannot use a date for an address field or enter an age that is not possible. In addition, LED is connected to the third-party verifier service and the USPS address service to help ensure the data entered into LED is accurate, reliable, complete, and current. In addition, USAC has policies in place to ensure the data is processed and maintained only for the purposes for which it is collected.

8.3 If the PII is being manipulated and/or analyze, what policies and procedures ensure that the system adheres to the Data Quality guidelines when the PII is aggregated or consolidated?

USAC follows internal policies and procedures, and has built in system protections to verify data quality and consistency of reporting information. In addition, in December 2016, the Director of Privacy position was created to ensure that the company has policies and procedures in place to protect PII and to ensure the appropriate use of this data. The Director of Privacy is to be contacted before PII from LED is shared including in an aggregated format.

8.4 How does USAC ensure that the PII is used in accordance with the stated practices in this PIA?

USAC follows regular reviews of system and internal policies and procedures to ensure that PII is used in accordance with practices as stated in this PIA. In addition, the Director of Privacy is responsible for ensuring that USAC staff are trained and that the PII from LED is only used for its intended purposes.

8.5 How often is the system audited to ensure compliance with these policies and practices?

The LED system is audited both by internal and external auditors, and by policy at least annually to ensure it is in compliance with FISMA requirements.

8.6 What would be the consequences to the USAC's operations if this information system became dysfunctional?

There would be moderate harm to USAC's operations, and a severe impact to LED could potentially delay processing of required monthly functions, such as reimbursement to service providers for universal service Lifeline program claims.

SECTION 9: PAPERWORD REDUCTION ACT (PRA) INFORMATION COLLECTION REQUIREMENTS

9.1 Does the information system require any paperwork and/or recordkeeping requirements, including both voluntary and required compliance:

☒ Yes, the information system includes paperwork and/or recordkeeping requirements that non-FCC employees and contractors must complete.
☒ FCC forms, licenses, or other documentation.
☒ Marketing, consumer, or customer satisfaction surveys or questionnaires.
☒ Recordkeeping or related activities.
☒ Website or other Internet-related portal.

Please explain if this information system is <u>not</u> subject to the PRA:

☐ No, the information system doesn't impose any paperwork and/or recordkeeping that constitute a PRA "information collection."

9.2 Please list the OMB Control Number, Title of the collection, and Form number(s) for the PRA information collection(s) related to this information collection:

OMB Control Number: 3060-0819, Lifeline Reform and Modernization, Telecommunications Carriers Eligible for Universal Service Support, Connect America Fund, ICR Reference No: 201704-3060-017. In addition, on the first screen of the LED, there is a link to the Paperwork Reduction Act (PRA) Statement. All of the application, recertification, and on-per-household worksheet also contains the PRA statement at the end of the form.

SECTION 10: TECHNOLOGICAL IMPACTS

10.1 What impact does technology have on the privacy of the individual's whose PII is being collected?

LED will capture the IP address for every login attempt of the originating party, including individual Lifeline subscribers.

10.2 Does this information system include the use of technology to conduct electronic searches, queries, and/to monitor or track an individual whose PII is being collected and used?

Yes. Please see the above response regarding the tracking and recording of IP addresses.

10.3 If applicable, what controls, policies, and procedures does this information system have to prevent unauthorized monitoring?

USAC is only tracking the IP address for auditing purposes, but is not conducting any additional monitoring of the individual subscribers.

SECTION 11: SECURITY, RISK ASSESSMENT, AND MITIGATION

11.1 What security classification has been assigned to this information system?

Moderate security categorization.

11.2 What risk level has the USAC Director of Information Security assigned to this information system?

Moderate risk level.

11.3 What controls are in place to prevent unauthorized access to the PII?

USAC employee and contractor access to electronic records maintained in LED are controlled through USAC's IT privacy safeguards, policies, and procedures which comprise a comprehensive and dynamic set of IT safety and security protocols and features that are designed to meet all Federal IT privacy standards, including those required by NIST and FISMA.

11.4 How often are the system's safety and security controls reviewed to ensure they comply with Federal regulations?

Annually and when changes or modifications are made to the system or to the data that is being collected by the system.

11.5 What other processes are in place to monitor and to respond to potential privacy incidents like a "data breach?"

USAC systems are monitored in accordance with NIST Continuous Security Monitoring recommendations. PII is monitored for access and unauthorized changes.

11.6 What measures are used to mitigate any potential risks and vulnerabilities for the information system's PII?

Risks:	Mitigating factors:
a. Disclosure of PII to an adversary may severely impact the agency operations, agency assets, or individuals identifiable from the information.	a. Access to PII is monitored via technical controls and enforced via management policy.
b. Misuse of PII by USAC personnel, USAC contractors, or carriers would cause irreparable harm to USAC.	b. PII is stored encrypted and only accessible to limited personnel on a strict need-to-know basis and for an authorized purpose.