DOCKET NO. UM 1688

Cover Sheet for Submission of 2014 Annual ETC Certification Reports

Name of Eligible Telecommunications Carrier: Citizens Telecommunications Company of Oregon, Inc. d/b/a Frontier Communications of Oregon

Filing date: September 15, 2014

Is this: Original submission? _____
OR
Revised submission? ____X_____

Person to contact for questions:

Name Kim Douglass

Phone number 972-908-4415

E-mail address kimberly.a.douglass@ftr.com

Documents included in this filing (please check applicable items):

_____ CAF/ICC Support (47 CFR § 54.304)

_____ Rate Floor Data (47 CFR § 54.313(h))

_____ Form 481 (High-cost per 47 CFR § 54.313, Low-income per 54.422)[1]

_____ Form 690 (Mobility Fund per 47 CFR § 54.1009)

_____ Affidavit for High-Cost Support

__X___ Additional Documentation for Form 481

Filing deadlines: The deadlines for filing items required by 47 CFR § 54 are the same as the deadlines for filing with the FCC. The notarized affidavit for high-cost support must be filed no later than the due date for the FCC Form 481. Based on current information, it appears that all items other than CAF/ICC support data are due by July 1, 2014. The CAF/ICC support data are due the same day as the ETC's interstate access tariff filing. If revisions to an original submission are filed with the FCC or USAC, a copy of the revisions must be filed with the Oregon Commission no later than five business days following submission to the FCC or USAC.

[1] Lifeline-only ETCs must provide all information specified in 47 CFR § 54.422(b) even if the ETC does not submit this information to the FCC.

Line 510 – Description of Compliance with Service Quality Standards and Consumer Protection:

The Frontier ILEC companies certify that they comply with applicable state and FCC service quality standards. Service quality metrics are monitored and reported on a monthly basis. Frontier has implemented numerous Consumer Protection measures to protect customer information from improper use and disclosure as well as to protect against fraud. For example, Frontier has implemented Customer Proprietary Network Information (policies and procedures) that are consistent with the FCC's regulations. Frontier regularly trains employees who have access to CPNI on the rules and our procedures for securing accounts and authenticating callers. Frontier also has a comprehensive Identity Theft Protection Program (or Red Flag program) which is consistent with the FTC's guidance on measures to detect and prevent identity theft. All employees are trained on Frontier's Code of Business Conduct and Ethics, which requires employees to protect sensitive customer information from improper use and disclosure. Frontier also has a Data Privacy and Security policy which applies to all employees. Further, Frontier also has implemented a strict third-party qualification protocol to prevent unauthorized charges ("Cramming") from appearing on customer's bills. Frontier also follows a "First Call" resolution policy, which aims to resolve customer complaints about unauthorized charges in one call, without referral to any third party. In addition to the foregoing, Frontier, has implemented customary IT security measures to protect our network and customer information.

Frontier certifies compliance with Oregon state consumer protection rules; Oregon OAR Division 34 – Small Telecommunications Utilities and Cooperatives.

The Oregon state consumer protection rules are available at:

http://arcweb.sos.state.or.us/pages/rules/oars_800/oar_860/860_034.html

Row 610 - Description of Functionality in Emergency Situations

In December 2013, the FCC adopted new rules to promote 911 resiliency. Frontier is currently reviewing its back-up power, circuit auditing and network monitoring practices to ensure compliance with the FCC's direction. Frontier's procedures are described below; to the extent that there is any conflict between the FCC's new 911 resiliency rules and Frontier's existing procedures, the existing procedures will be updated to conform to FCC standards within the timeframe specified by the FCC.

The Frontier ILEC companies certify that they follow best practices that are designed to allow them to remain functional in an emergency situation through the use of back-up power to ensure functionality in the event of a limited commercial power failure. Frontier's policy is that at sites where there is a generator, it will also have batteries capable of providing three-to-four hours of backup power. Sites that are provisioned to allow portable generators typically have up to eight hours of battery backup power available. Frontier adheres to formal maintenance and testing schedules of batteries and generators based on the GTE practices, the Bell standard and manufacturer standards. Batteries are load tested routinely. On site generators are tested monthly with an annual "blackout" test also incorporated. Routine maintenance occurs regularly throughout the year. Portable generators are load tested once a year along with performing the manufacturer recommended maintenance.

The companies' network is engineered to provide maximum capacity in order to handle excess traffic in the event of traffic spikes resulting from emergency situations. Carrier audits its circuits in order to provide redundancy in its network where feasible for use in re-rerouting traffic when facilities are damaged.

Line 510 – Description of Compliance with Service Quality Standards and Consumer Protection:

The Frontier ILEC companies certify that they comply with applicable state and FCC service quality standards. Service quality metrics are monitored and reported on a monthly basis. Frontier has implemented numerous Consumer Protection measures to protect customer information from improper use and disclosure as well as to protect against fraud. For example, Frontier has implemented Customer Proprietary Network Information (policies and procedures) that are consistent with the FCC's regulations. Frontier regularly trains employees who have access to CPNI on the rules and our procedures for securing accounts and authenticating callers. Frontier also has a comprehensive Identity Theft Protection Program (or Red Flag program) which is consistent with the FTC's guidance on measures to detect and prevent identity theft. All employees are trained on Frontier's Code of Business Conduct and Ethics, which requires employees to protect sensitive customer information from improper use and disclosure. Frontier also has a Data Privacy and Security policy which applies to all employees. Further, Frontier also has implemented a strict third-party qualification protocol to prevent unauthorized charges ("Cramming") from appearing on customer's bills. Frontier also follows a "First Call" resolution policy, which aims to resolve customer complaints about unauthorized charges in one call, without referral to any third party. In addition to the foregoing, Frontier, has implemented customary IT security measures to protect our network and customer information.

Frontier certifies compliance with Oregon state consumer protection rules; Oregon OAR Division 34 – Small Telecommunications Utilities and Cooperatives.

The Oregon state consumer protection rules are available at:

http://arcweb.sos.state.or.us/pages/rules/oars_800/oar_860/860_034.html

Row 610 - Description of Functionality in Emergency Situations

In December 2013, the FCC adopted new rules to promote 911 resiliency. Frontier is currently reviewing its back-up power, circuit auditing and network monitoring practices to ensure compliance with the FCC's direction. Frontier's procedures are described below; to the extent that there is any conflict between the FCC's new 911 resiliency rules and Frontier's existing procedures, the existing procedures will be updated to conform to FCC standards within the timeframe specified by the FCC.

The Frontier ILEC companies certify that they follow best practices that are designed to allow them to remain functional in an emergency situation through the use of back-up power to ensure functionality in the event of a limited commercial power failure. Frontier's policy is that at sites where there is a generator, it will also have batteries capable of providing three-to-four hours of backup power. Sites that are provisioned to allow portable generators typically have up to eight hours of battery backup power available. Frontier adheres to formal maintenance and testing schedules of batteries and generators based on the GTE practices, the Bell standard and manufacturer standards. Batteries are load tested routinely. On site generators are tested monthly with an annual "blackout" test also incorporated. Routine maintenance occurs regularly throughout the year. Portable generators are load tested once a year along with performing the manufacturer recommended maintenance.

The companies' network is engineered to provide maximum capacity in order to handle excess traffic in the event of traffic spikes resulting from emergency situations. Carrier audits its circuits in order to provide redundancy in its network where feasible for use in re-rerouting traffic when facilities are damaged.