

Attachment 1

CenturyLink's Comments

Docket No. 16-R100-01

Docket No. 16-R100-02

October 24, 2016

CenturyLink's questions overlaying the questions of Rocky Mountain Power:

- What type of authentication mechanism will be used? (e.g., SSH keys, User id/password, or Certificate?)

CenturyLink's additions:

- Will 2-Factor authentication be implemented (could be a customer selectable option) to strengthen the authentication into the SFTP connection? (The concern is to control the establishment of the encrypted SFTP session with another level of authentication prior to establishing the SFTP connection and transporting data across the connection.)
- Will accounts on the SFTP server map to individuals, or to companies? If individuals, will group permissions be configured to support team functions? (so user A at company X can see what user B also at company X has already contributed)
- Will it be possible for contributors to use a program such as WinSCP to "drag-and-drop" files onto the SFTP server?

CenturyLink's additions:

- If allowing the use of a tool like WinSCP, will the 2-Factor authentication capability be included?
- To alleviate concerns about storing files on an internet-accessible server, will the Commission allow the Company to bundle and encrypt the contributed files with a user friendly industry standard tool such as 7-zip?
- Will statutory protections for confidential information between the Company and the Commission be applicable to the state run web portal?

CenturyLink's additions:

- Will any customer data reside on the customer facing web portal or will all SFTP transmitted data reside only on the state run SFTP server and then be moved onto the standard file servers as currently done when customer submitted files are received via email, for example? If customer data may reside on the internet facing web portal, how will this data be protected? What administrative, physical and technical controls will be employed?