

Comments presented by Paul Kjellander, President of the Idaho Public Utilities Commission on 03/28/2019 as part of the FERC Technical hearing on Cost Recovery of Cyber Security expenses.

Intro

I want to thank the FERC and Chairman Chatterjee for the opportunity to participate in today's technical hearing.

In my comments, I will address several types of rate recovery methods that are available at the state level for cybersecurity cost recovery. I'll touch on Base Rates, Annual Cost Adjustments, Single Issue Rate Cases, and Regulatory Preapproval Processes.

My main point today is that as state regulators, we don't have to invent new rate recovery tools to recover cyber security costs. We just need to be willing to utilize the ones we have if the situation warrants.

Base Rates

Building cyber security costs into base rates is one of the most preferred approaches. But there can be some concerns in a Rate Base environment that might represent a disincentive for investment.

An obvious concern is that in an evolving world of cyber threats...the amount in rate base might not be enough to cover expenses. And if cyber security costs are one of the only items that are potentially out of line...the cost to put on a full-blown rate case to recover extraordinary costs might serve as a huge deterrent to appropriate investment. Another perceived risk of opening up a full blown rate case to address cybersecurity costs is the risk that in an effort to keep overall rates low...the amount of recovery in other areas of a utility's operations could be lowered to find the money for increased cyber costs. This type of trade-off could create problems elsewhere for a utility...and the outcome for the utility might be one they don't want to risk.

A final perceived concern with a rate base approach is the potential disincentive that depreciation schedules might have on investment...especially if there is a huge gap in time between rate cases. One way to address this concern is to establish deferral accounts. This type of accounting treatment helps reduce the perceived risk that appropriate costs won't be recovered.

Annual Cost Adjustment

Annual cost adjustments aren't a new concept for state regulators. Many of us across the country have adopted them as tools to recovery costs associated with energy efficiency measures and fuel cost adjustments. Typically, annual adjustments are established to recover costs that can be volatile and vary dramatically from year-to-year...such as fuel costs.

While I'm not one to rule out the idea of an annual cost adjustment mechanism for cyber security expenses...our historic utilization of such a mechanism is tied to the potential of huge cost swings from year-to-year...and so far we just haven't seen this present itself in the area of cyber security. But that doesn't mean we won't see it in the future.

As software companies move to subscription models and cloud-based resources, regulated utilities will be confronted with the issue of cyber security costs migrating from capital purchases to operating and maintenance (O&M) expenses. This might prompt requests for regulators to examine the role an annual cost adjustment mechanism.

Single Issue Rate Case

This has some merit from my perspective. If an emerging issue or some other extraordinary concern creates a need for significant expenses beyond what might already be in rate base...a single issue rate case has merit. A case meeting the right criteria could be filed and put on a fast track (examples of what might drive this could be emergency considerations or some new resolution to a security threat). And since it is a single issue case, you wouldn't have a lot of other parties in the case who have interests not associated with cyber-security. That means it is easier to manage the case...especially if you have sensitive information that needs to be provided in an effort to justify potential costs. It is much easier to manage a case if you are not forced to constantly clear the room of those who for whatever reason shouldn't be privy to the information being presented.

As a thought, if we utilized a single issue rate case option for cyber security recovery and saw a trend of new case filings every year...this might serve as an indicator that an annual cost adjustment mechanism is worth considering

Regulatory Preapproval Process

In my state we have a regulatory preapproval process where a utility can open a case to get approval of large capital expenditures before the investment is made. This mitigates the risk associated with large investments and it gives lenders more confidence that cost recovery will occur.

Final Thoughts to Consider

When FERC, NERC, or WECC issue substantial penalties for Critical Infrastructure Protection (CIP) violations...could an emphasis be placed on negotiated settlements that would divert the fine for the purpose of investing in technology/solutions that would bring the utility into compliance? As it stands today, when fines are issued to utilities, state regulators pass those costs directly to shareholders. This impacts revenue and ROE. Since none of those fines are recoverable in rates it could represent a disincentive to future investment. Additionally, if money that otherwise would have been a fine could be used to fund improvements related to CIP, there is a chance that those expenses could ultimately be recoverable in a future rate proceeding.

The last item I want to mention relates to comments made earlier today about the important role that telecommunications providers play in the cyber security discussion. The point that needs to be made regarding state regulators is that many states have little or no authority over the telecommunications sector. This means that as state regulators we can't force telecommunications providers to disclose information related to cyber security issues that they do not want to provide. I'm not suggesting that there are any bad actors among the

telecommunication's providers, I'm simply pointing out a scenario that makes it more difficult for state regulators to know what is actually happening on the telecom front.

Again, thank you for the opportunity to address you on this important topic.