



State Staff Information Sharing “Surge” Call Summary

“IT Expenditures - The Newest Big Investment”

September 9th, 2016

On September 9th, 2016 the NARUC Research Lab convened state public utility commission staffers on a "surge" technical assistance call to learn from one another about utility information technology (IT) expenditures.

As a group, we sought to explore how much spending on IT by utility companies is prudent. During the call we sought to explore the categories of IT investments made by utilities; IT cost recovery requests embedded in utility rate cases; IT solutions by state; how much commissions are approving for cost recovery on IT investments by utilities; as well as questions regulators can ask utilities in an effort to understand utility IT expenditures (including cybersecurity IT costs).

We learned that U.S. companies in general (not just utilities), ranging from small to large, are spending between 4% and 6% of their revenue on IT-related expenditures. (Source: CIO Magazine 2016).

In 2014, IT spending by utilities worldwide was \$149.38 billion, which is more than education, and healthcare providers, but less than banking, finance, manufacturing, and government sector spending (the financial sector spends more on IT than any other sector).

Next, we looked the types of IT items that companies across sectors are spending money on. Call participants noted that non-staff spending broke down into two major cost components. Communications services and IT services – money spent outside the company - comprised slightly more than half of total spending on IT. Software and hardware – capital expenditures - tended to be a little less than half of total spending on IT. It would be helpful for commissions to know how much individual utility companies spend on IT, however, state call participants agreed that getting such information is difficult to obtain.

Call participants and NARUC staff came

up with the following consolidated list of IT expenditures:

Internal Communications

External communications

Networks and Management Systems

- Performance Management
- Accounting Management (billing, payroll)
- Fault Management (detects, logs, and reports network and system problems)
- Security Management (controls access to network/system resources per security guidelines)
- Network Configuration Management

Customer Data Management

Business Processes

Employee IT training

Business Analytics; and

Application Development

Operations technology (OT), however, is not included in the list above, and OT expenditures are a significant expense for utilities since it includes everything that is associated with making the grid smarter. In 2014, Navigant Consulting predicted that \$600 billion will be spent worldwide on smart grid expenses between 2014 and 2023, with much of these expenses being incurred in Europe and Asia.

Next, we discussed where IT spending is heading. We will continue to see more spending in the following areas: Cloud computing, mobile technologies, and virtualization of business processes, and OT systems.

We discussed these questions as well:

- **Q:** What kinds of IT spending have you seen? **A:** MI gave some very specific examples (see below).

- **Q:** Is it hard to identify? **A:** It can be hard since it's sometimes not separated from cyber expenses.
- **Q:** Is it hard to gauge prudence? **A:** Yes, it seems many states aren't sure when something is gold-plating or not.
- **Q:** What matters to you – what values do you want to see reflected in utility spending? (This question varied too much by state to provide a summary)
- **Q:** Do you have a good sense of what's a good number? **A:** A Midwestern state described their struggle with this, and so they have sought help from a consultant.

States on the call shared their experiences with IT expenditures they have seen utilities make:

Michigan shared specific challenges they are faced with such as: how to figure out what IT expenditures utilities want versus what they actually need; understanding why utilities choose to include or not include certain items in a rate case; how utilities came to conclusions about the options they eliminated; what is gold plating and what is not; and what is really at stake if certain investments are not made?

Michigan recently hired a consultant who has a lot of experience with IT expenditures made by utilities, to help them do a deeper dive into these issues as the commission is deals with audit and discovery questions in rate cases.

The contractor will aid the commission for approximately a three month period beginning in the fall of 2016.

In Michigan rate cases, IT costs have been increasing in the last five years. In an average rate case, there are between \$40 and \$70 million in IT expense requests, and this is split between capital costs and O&M costs. Much of these costs are needed for making the grid smarter, where the more smart grid software that utilities acquire, the more customer data there will be to process. The other large expense utilities have is the integration of their IT business units with their OT business units, in order to enable data to be transferred more easily throughout the organization, and to achieve greater efficiencies overall. It was noted that some utilities in the state separate cybersecurity costs from IT ones, while others have IT and cybersecurity costs included in nearly every line item, which makes analyzing each one individually a challenge.

In Massachusetts, cybersecurity costs are looked at separately from other expenses. Utility companies in the state have been working well with regulators, who meet annually with all electric and gas companies. They have noticed that IT costs vary to a large extent from one utility to another one. The PUC acknowledged that it lacks the IT expertise in-house to help determine prudence of costs more thoroughly, however, it also noted that retaining such in-house expertise would be unaffordable for the commission. Five years ago, the state commission hired a consultant to provide some training on IT expenditures, and thereafter,

Massachusetts has been having semi-official discussions with its utilities annually about cybersecurity expenditures specifically.

The state of Washington is working to understand more about both cybersecurity and IT investments that are made at small and medium size utilities. Washington asks its utility companies for specifics about their participation (if any) in regional or national tabletop exercises, or other events related to critical infrastructure security. The state also asks questions about which organizations have been notified in emergencies, if there are plans in place to handle emergencies, and they informally discuss what the cost of these efforts are. Specific questions about the details of these plans are not asked due to public disclosure laws. In the last year, Washington has met with every utility CEO in the state, communicating the importance of cybersecurity being a board level interest. Washington has also met with some of its energy public utility districts (PUDs), to create an education primer for the smaller PUDs that are not regulated so they can stay abreast of these issues. The state does not have in-house cyber or IT specialists, but have been able to rely on the in-house engineers and also have other staff who came from industry, to help with these topics.

Washington expressed a desire to know more about how IT and cyber costs are broken out, but this effort is still a work in progress. Washington continues to develop procedures for looking at how companies are protecting their critical infrastructure. The state has an internal team of six people – one from each division - who meet approximately once every six weeks, to discuss and compare company and industry information. The state has an internal team of six people – one from each division - who meet approximately once every six weeks, to discuss and compare company and industry information.

Finally, NARUC staff shared examples of cost questions that regulators could ask their utilities to learn more about their IT expenditures. These cost questions break down into several categories:

- Are there initial costs, like hardware and software, and training?
- What are the ongoing costs — maintaining systems, including licenses for proprietary software, hosting, and support?
- Are there upgrade costs (cost of upgrades, and expected lifespan of systems/frequency of upgrades?)
- Is there value proposition that goes into both the cost and benefit side of this? How much employee time will the system save? How much new business could the system generate?
- Is there an opportunity cost of either doing an alternative or not doing this?
- What are the risks and potential downsides? What does it cost to mitigate those risks?

The call concluded with the following ideas about what else NARUC can do to help states get more of the resources they need: (1) A summary of the outcomes of this surge call; (2) A community of folks to turn to – we’ll include the list of participants in the summary for all the participants. Additional possible follow-up items include: (3) Some sort of benchmarking or survey of what states are seeing (this one may prove challenging to do, but perhaps another organization can do this for us); and/or (4) a broader primer on the issue with sample questions to ask.



This “Surge Summary” represents the synthesis of a policy conversation among state PUC staff aimed at interstate collaboration, technical assistance, and information sharing.

Please address questions to NARUC’s Research Lab staff, whose details are online at www.naruc.org/lab

Have a question you’d like to convene state staff from around the country to explore? Please contact Miles Keogh, NARUC’s Lab Director, 202-898-2217 mkeogh@naruc.org