Docket No. DE 17-189
Exhibit 21

EXHIBIT
tabbies
#21
DE 17-189

Liberty Utilities (Granite State Electric) Corp. d/b/a Liberty Utilities

Docket No.DE 17-189

Petition to Approve Battery Storage Pilot Program

Record Request

Record Request Received: November 29, 2018

Date of Response: December 13, 2018
Respondent: Shawn Eck

REQUEST:

"[Has] the cybersecurity officer at Liberty … applied the NERC CIP Standards … to the equipment that is going to be installed in this pilot"? (November 29, 2018, Transcript at 160)

RESPONSE:

I am the Senior Manager, IT Security, Risk and Compliance, and work for an affiliate that provides IT and other services to both Algonquin Power & Utilities Corp. (APUC) and the regulated Liberty Utilities entities. Three IT professionals report to me, one holding the title Supervisor, IT Security, Risk and Compliance, and two with the title of Senior Analyst, IT Security and Controls. I report to the Vice President of Transitional Management and IT who, in turn, reports to the president Liberty Utilities Co., which the parent of all the regulated Liberty Utilities companies, including Granite State Electric.

The APUC Board of Directors delegated to the APUC executive management team the authority to enforce and monitor compliance with the Cybersecurity Policy that governs all APUC and Liberty Utilities entities. Management, in turn, established a Cybersecurity Working Group ("CWG"), which is responsible for interpreting, enforcing, overseeing the implementation of, and recommending improvements to this policy. I am a member of the CWG along with members of the IT Security team listed above, and others. The Cybersecurity Plan was filed on behalf of Granite State Electric with the Commission at the end of 2017, and the Company will be filing an updated version of the plan pursuant to Puc 306.10 by year end.

NERC Critical Infrastructure Protection Standards (CIPS), comprising of 12 different standards, were created by identifying security controls from National Institute of Standards and Technology (NIST) SP800-53 and International Organization for Standardization (ISO) 27001 controls frameworks, which the electric industry felt should be applied to the critical transmission and generation assets governed by FERC. Each of the 12 standards addresses a security focus or area. The first standard, CIP-002, states that CIPS apply to the Bulk Electric System (BES), generally defined as electric transmission assets over 100 kV, generation assets over 75 MVA, associated control centers, and some limited and specialized distribution assets related to the BES. These assets are then assigned an impact rating. The remaining CIPS identify security requirements that must be applied based on the impact of each asset as identified in CIP-002. None of Granite State Electric's assets fall within the CIPS' definition of BES, so the CIPS are not applicable to Granite State Electric.

However, APUC and the Liberty Utilities companies nationwide have a comprehensive cybersecurity plan which covers the security objectives identified in the CIPS standards, but which are not specific to electrical transmission, generations, and control center assets. The APUC/Liberty plan leverages the same standard security frameworks which were the sources of identifying the NERC CIPS requirements, such as NIST and ISO, but the APUC/Liberty plan allows for additional security considerations not addressed by the limited scope of NERC CIPS. In creating the APUC/Liberty plan, we have identified the NIST Cyber Security Framework (CSF), https://www.nist.gov/cyberframework, and the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2) framework, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0 for program assessment and reporting. These frameworks and models are created specifically to provide security assurance of critical infrastructure assets. Liberty follows a risk based approach to program implementation and continuous improvement. All security areas identified in the NERC CIPS are included in our security program.

My team performs the risk advisory role and works with each business area to provide guidance and recommendations to ensure cybersecurity needs and objectives are addressed. We work closely with Enterprise Risk Management to monitor and manage enterprise cybersecurity related risk.

The steps taken to address a cyber risk assessment for new initiatives begin with an assessment of the business functions and objectives. This provides insight into what type of data we will be processing and the impact should something go wrong. We then work with the business and associated vendors to get an understanding of the solution and technology being proposed. We identify risk areas which may be compromised to cause harm or interrupt the services/solution. We work with the vendor to get an understanding and assurance that their security programs are also adequate and cover all aspects of the proposed solution. The security review scope and approach depends what services are being provided and how the solution is delivered.

The actions taken specific to the Granite State Electric/Tesla Pilot initiative followed the above process. We met with Heather Tebbetts and other business stakeholders (including IT, Customer Service, and Operations) to get a sense of what the business function and solution objectives were. We had conversations with Tesla to get an understanding of technology and solutions used to deliver the service. And we reviewed their security program and controls in place to ensure the various components of the solutions were covered by an acceptable security program.

The process is not yet finished as the final agreement has not yet been signed and there were some business processes and decisions still being worked through over the recent months. I understand all the processes have now been resolved and decisions made, so our team will conduct another security review of the overall solution and program to identify any risk that we feel still needs to be addressed before we give authority for the program to go live. We will review the final contracts and any additional security reports from Tesla to determine if the security controls and objectives are adequate.

My current understanding is that Granite State Electric will only need to have access to the Tesla-managed web-based SaaS solution and thus the security of that environment will rely on the security controls implemented by Tesla. Tesla will not have access to any of Granite State Electric's systems.

Finally, I have the authority to prevent the program from going forward unless and until our team is satisfied.