National Grid/Liberty Energy NH

Petition for Authority to Transfer Ownership of Granite State Electric Company and EnergyNorth Natural Gas, Inc.

DG 11-040

Exhibit 21
Response to Record Request #2

Date of Request: April 19, 2012 Date of Response: May 1, 2012

REQUEST: (a) What are the acceptance criteria for the Comprehensive IT Testing Plans and how does IEEE Standard 829 relate to this process? (b) What are the acceptance criteria for the Liberty Utilities Family of Companies' network security assessments?.

RESPONSE: Please see Attachments (A) and (B) to this response.

Question presented: What are the acceptance criteria for the Comprehensive IT Testing Plans and how does IEEE Standard 829 relate to this process?

Standard 829 of the IEEE governs the establishment of an IT system testing process; it does not govern the results of that process. Liberty Utilities' IT testing approach has three phases. The first phase is the development and documentation of an overall test strategy. The test strategy outlines the scope of the test, roles and responsibilities of participants, standards and processes to follow, timelines, test scenarios and a reporting process to acquire final approval and sign off to proceed. The end result of the test strategy is a set of detailed testing scripts/cases created that address each requirement from the project. All tests scripts are logged on the test control sheet. The test control sheet acts as a monitoring tool to evaluate the progress of testing. Through testing and verifying each requirement, confidence can be achieved that all needs of the application are met and functioning as desired.

The second phase of testing consists of generating test cycles. Through several cycles of testing, problems are identified, corrected and re-tested through the rigorous testing cycles. As many as four cycles may be performed with each cycle increasing in duration. This method of testing reduces the overall time to bring an application migration to implementation readiness.

The final phase of testing entails user acceptance testing (UAT). UAT enables the actual end-users/customers to use documented test scenarios and their own testing to facilitate the implementation approvals of the application. Only after business approval has been received can an application proceed to production.

The IEEE 829 standards specify the types of test documentation that must be produced to achieve compliance with the standard, and these include the types of tests to be performed, i.e., unity, system, integration, stress, user acceptance, and readiness testing. Liberty intends to follow these standards for all its applications and ensure its vendors support the rigorous documentation and testing standards within them.

IEEE 829 provides guidance to management that it must establish criteria that conform to the needs of the business, users, and stakeholders such that the information technology systems maintain integrity of operations. An example scheme of integrity evaluation is:

Integrity Level Description	Level
Software must execute correctly or grave consequences (loss of life, loss of system, environmental damage, economic or social loss) will occur. No mitigation is possible.	4
Software must execute correctly or the intended use (mission) of system/software will not be realized causing serious consequences (permanent injury, major system degradation, environmental damage, economic or social impact). Partial-to-complete mitigation is possible.	3
Software must execute correctly or an intended function will not be realized causing minor consequences. Complete mitigation possible.	2
Software must execute correctly or intended function will not be realized causing negligible consequences. Mitigation not required.	1

Each Liberty application will be tested using pre-defined success measures that are unique to each, but that follow a common framework:

Accuracy – the test produces results that are consistent with expected results

Response time – the system provides users with information that reflects processing within the application and databases within intervals that are consistent with business needs

Completeness – the system produces all of the expected results

There are negative tests conducted for some systems and applications, i.e., a completeness test for a report will include an assessment that no other data than that required for a report is included; an error condition that is introduced will result in a rejection and not acceptance of a transaction.

Question presented: What are the acceptance criteria for the Liberty Utilities Family of Companies' network security assessments?

Liberty has committed to being evaluated and assessed again ISO27001, which establishes a framework for evaluating network IT security vulnerability.

ISO 27001 "Information Technology - Security Techniques - Information Security Management Systems – Requirements" is the best practice specification that helps businesses and organizations develop a best-in-class Information Security Management System (ISMS). Liberty has selected Price Waterhouse Coopers ("PWC") to perform this work.

The PWC assessment will evaluate whether any vulnerabilities exist and measure the risk attendant with those weak spots. PWC will focus on three specific areas:

- Configuration – assessment of the system configurations (i.e., password strength, lockout controls, unnecessary services/accounts, etc.) against "good" security practice
- Vulnerability– scanning to identify the potential weaknesses and vulnerabilities on the target Liberty Utilities systems and devices;
- Architecture – Determine the attack surfaces and points, assess the threats, and evaluate the security solutions and controls in place.

The results of the network security assessment are evaluated using a Common Vulnerability Scoring System ("CVSS"). The CVSS is an internationally recognized standard method for rating information technology ("IT") system vulnerabilities. Using this methodology, system risks are classified into four categories: critical, high, medium, and low. The overall impact of a risk on system vulnerability is then evaluated based on the data involved, the function of the system, and the risk classification, *i.e.*, a risk that is classified as medium that impacts highly confidential material may be more serious than a risk that is classified as high that impacts public information. Key controls are then developed and implemented to sufficiently mitigate these risks. These controls are then audited by either internal or external auditors to assess their effectiveness.