

STATE OF NEW HAMPSHIRE

Inter-Department Communication

DATE: November 7, 2014**AT (OFFICE):** NHPUC**FROM:** Amanda O. Noonan **SUBJECT:** DG 11-040 Third Party Assessment of the Liberty
Utilities Family of Companies' Network Security Compliance with ISO
2700-1**TO:** Martin Honigberg
Robert Scott**CC:** Stephen Frink
Randy Knepper
Grant Siwinski
David Wiesner

On April 16, 2014, Staff filed a memorandum which, among other things, recommended the Commission open an investigation into Liberty Utilities' (Liberty) compliance with certain provisions of the settlement agreement approved in this docket, including the requirement to conduct a third party assessment of the Liberty Utilities Family of Companies' Network Security Compliance with the International Organization for Standardization (ISO) Standard 2700-1. Under the settlement agreement, Liberty was required to ensure such a baseline assessment was conducted prior to the closing date for the sale of Granite State Electric and Energy North to Liberty, and to undertake another assessment following the full implementation of the IT Migration Plan. Biennial security assessments of equivalent scope and scale would occur thereafter.

On May 27, 2014, the Commission conducted a status conference consistent with Staff's recommendation. At the status conference, Liberty Utilities indicated that, while it believed the baseline assessment conducted prior to the closing was in compliance with the settlement agreement requirements, it welcomed the opportunity to work with Staff and its consultant to discuss an appropriate scope for the upcoming IT security assessment that would be conducted following full implementation of the IT Migration Plan. Liberty anticipated then that the assessment work would begin in the late summer or early fall time period.

Since that time, Staff and its consultant, Gorham/Gold/Greenwich Associates, have had numerous telephone conferences with Liberty and the Office of Consumer Advocate regarding the details of an appropriate scope for the third party IT security assessment. Staff is pleased to report that consensus has been reached on a detailed scope for Liberty's IT network security assessment, and that Liberty plans to issue a request for proposals for performance of the first phase of the assessment work on or about November 10th. Copies of the documents describing the assessment scope in detail are attached to this memo.

SERVICE LIST - EMAIL ADDRESSES - DOCKET RELATED

Pursuant to N.H. Admin Rule Puc 203.11 (a) (1): Serve an electronic copy on each person identified on the service list.

Executive.Director@puc.nh.gov
alex@krakowsouris.com
amanda.noonan@puc.nh.gov
david.wiesner@puc.nh.gov
diane.bateman@puc.nh.gov
dnute@jordaninstitute.org
grant.siwinski@puc.nh.gov
leszek.stachow@puc.nh.gov
lynn.fabrizio@puc.nh.gov
mark.naylor@puc.nh.gov
mlicata@nhbia.org
patrick.taylor@mclane.com
robert.wyatt@puc.nh.gov
Rorie.E.P.Hollenberg@oca.nh.gov
sarah.knowlton@libertyutilities.com
scott.j.rubin@gmail.com
shannon.coleman@libertyutilities.com
sjs@sjsullivanlaw.com
Stephen.Hall@libertyutilities.com
Stephen.R.Eckberg@puc.nh.gov
steve.frink@puc.nh.gov
steven.camerino@mclane.com
susan.chamberlin@oca.nh.gov
suzanne.amidon@puc.nh.gov
tom.frantz@puc.nh.gov

Docket #: 11-040-1 Printed: November 07, 2014

FILING INSTRUCTIONS:

- a) Pursuant to N.H. Admin Rule Puc 203.02 (a), with the exception of Discovery, file 7 copies, as well as an electronic copy, of all documents including cover letter with:
- DEBRA A HOWLAND
EXECUTIVE DIRECTOR
NHPUC
21 S. FRUIT ST, SUITE 10
CONCORD NH 03301-2429
- b) Serve an electronic copy with each person identified on the Commission's service list and with the Office of Consumer Advocate.
- c) Serve a written copy on each person on the service list not able to receive electronic mail.

**Liberty Utilities Post-Sale Monitoring
ISO/IEC 27001 Network Security Assessment
Two-Phase Verification and Compliance Assessment Process**

Summary Description

Staff proposes a two-phase assessment process for conducting the third party network security assessment required under Section V. D. 2 c, d, and e of the approved Settlement Agreement. This process is intended to verify and validate Liberty's representations that many of its current policies, procedures and practices are compliant with or functionally equivalent to the standards specified in ISO/IEC 27001. Only those topics with respect to which such compliance or functional equivalence have not been or cannot be verified and validated would be subject to a comprehensive ISO/IEC 27001 compliance assessment.

Both phases of the assessment process would be performed by a qualified and independent third party examiner. The solicitation of the third party examiner would be conducted based on consultation with and input from Staff and its consultant. The results of each phase of the assessment would be provided by the third party to both Liberty and Staff.

Phase I Verification and Validation

Phase I of the assessment process would verify and validate assertions made by Liberty's management that ISO/IEC 27001 requirements have been satisfied with respect to a number of specific topics that are shown as shaded green in the attached chart (the "Phase I Review Items").

In particular, Liberty's management has asserted that policies and procedures governing the Phase I Review Items have been developed and communicated to all responsible individuals, both employees and independent contractors, that related operational practices are regularly monitored and managed, that related incidents and events are logged and corrected as necessary, and that relevant changes are consistently managed and policies, procedures and practices revised accordingly. Liberty Utilities has further asserted that its efforts, and/or those taken by others on its behalf, with respect to the Phase I Review Items are functionally equivalent to those required in connection with a third-party assessment of compliance with ISO/IEC 27001 requirements.

In Phase I, a third party would be selected by Liberty to review and examine these assertions and documentation and representations presented or made available by Liberty Utilities, on its own behalf and on behalf of its operating public utilities in New Hampshire. Liberty would issue a request for proposals (RFP) to at least three firms with information technology security expertise to obtain bids to conduct the Phase I assessment. The RFP must include the specifications listed on Schedule A attached hereto. Liberty would provide the draft RFP to Staff and the Office of Consumer Advocate for review prior to its issuance.

The Phase I third party review and examination would address the questions set forth on Schedule B attached hereto. The examiner would have the discretionary authority to define sample sizes adequate to support its findings and conclusions, provided that, insofar as this is feasible and any determination of infeasibility is noted and described in the written results report, the sample sizes result in statistically significant findings. Liberty would afford the third party examiner all reasonable cooperation and would provide any requested documentation and data in a timely fashion.

Based on its review and examination, the third party examiner would issue an attestation statement to Liberty and Staff, containing substantially the following operative conclusion:

“We have reviewed and examined Liberty Utilities management’s assertions that its policies, procedures, practices and actions with respect to the Phase I Review Items are functionally equivalent to those required for compliance with ISO/IEC 27001, and we hereby attest that the documentation and representations presented and made available for our review and examination by Liberty Utilities are sufficient to validate and support all such management assertions with respect to each of the Phase I Review Items, as of the date specified herein. Our review and examination represents an independent and objective effort, the evidentiary standards employed are consistent with those prescribed by relevant certification bodies, and the conclusions expressed represent the professional opinions of our firm with respect to the Phase I Review Items.”

Any relevant ISO/IEC 27001 topic that is not the subject of such assertions by Liberty’s management or that cannot be verified and validated through the Phase I review conducted by the third party examiner would be included in the scope of the comprehensive ISO/IEC 27001 compliance assessment to be conducted in Phase II of the assessment process, unless excluded from such Phase II assessment scope as described below. In addition to the attestation statement, the third party examiner shall provide the written results of the Phase I verification and validation process to Liberty and Staff. Work papers produced during the course of the Phase I assessment will be maintained, secured, and made available to Liberty, Staff and the OCA upon request, both during and after performance of the work. Liberty shall provide the attestation statement and written results of the Phase I verification and validation process to Staff consistent with the attached schedule, which is predicated on the Company’s receipt of satisfactory responses to its RFP.

Phase II Compliance Assessment

Phase II of the assessment process would comprise a comprehensive ISO/IEC 27001 compliance assessment of any remaining topics that were not subject to the Phase I review and/or were not included in the Phase I examiner’s attestation statement. For those topics where the Phase I examiner could not verify and validate the assertions made by Liberty’s management, the topic may be excluded from the Phase II assessment if (1) the Phase I examiner has recommended an equivalent framework that will provide a more efficient or effective control than the ISO/IEC 27001 standard, and Liberty has taken the actions necessary to adopt and implement the recommended equivalent framework, or (2) the Phase I examiner determines that a specific component or element covered by any item on the attached chart is not within the scope of the

ISO/IEC 27001 standard, provided that, in the case of any such recommendation pursuant to (1) above or any such determination pursuant to (2) above, the recommendation or determination has been presented to Staff for its review and evaluation, and either (i) Staff has provided its written concurrence with such recommendation or determination, or (ii) the Phase II examiner has concurred with such recommendation or determination, if Staff does not provide written concurrence following its review and evaluation of the recommendation or determination.

The precise scope of the Phase II compliance assessment and the requirements for a competitive solicitation to select a qualified third party Phase II examiner would be determined by Liberty, with an opportunity for consultation with and input from Staff, following receipt of the Phase I attestation statement and any related report issued by the Phase I third party examiner. At a minimum, the solicitation documents would include the specifications listed in Schedule A and the following additional specification:

“The examination is meant to be conducted in a manner, and with such rigor required, as to confirm ISO/IEC 27001:2013 compliance with respect to the topics included within the scope of review. The examination will be conducted by a professional services firm or individual accredited by a recognized ISO standards organization as able and qualified to confer ISO/IEC 27001:2013 certification. For the avoidance of doubt, nothing in the foregoing specifications shall be deemed to require Liberty to seek or complete ISO/IEC 27001:2013 certification.”

The written results of the Phase II third party ISO/IEC 27001 compliance assessment, including the professional opinion of the third party examiner as to such results, would be provided to both Liberty and Staff. Liberty shall provide the Phase II written results including such professional opinion to Staff consisted with the attached schedule, which is predicated on the Company’s receipt of satisfactory responses to its RFP.

Remediation

If any deficiency or gap is identified as a result of the Phase I verification and validation process or the Phase II compliance assessment process, the third party independent examiner engaged by Liberty will provide a recommendation regarding the remediation of the deficiency or gap, with reference to the applicable ISO/IEC 27001 standard or to an equivalent framework that will provide a more efficient or effective control than the ISO/IEC 27001 standard, and Liberty will develop an action plan to adopt and implement the examiner’s recommendation.

The fact that any remediation action is taken as a result of or in connection with this two-phase verification and compliance assessment process, whether or not Staff has reviewed or provided input regarding such action, does not represent a determination by the Commission that the action taken was reasonable or prudent under the circumstances, nor does the need for remediation action represent a determination that the Company was imprudent as a result of the deficiency or gap.

SCHEDULE A

RFP Solicitation Minimum Specifications

The proposer must describe its qualifications and experience with respect to the specified type of work to be performed

The proposer must describe its experience in conducting ISO/IEC 27001 compliance assessments

The proposer must disclose any differences in methodology from that set forth in Schedule B that it intends to employ

The proposer must affirm its understanding and commitment that work papers produced during the course of each phase of the work it proposes to perform will be maintained, secured, and made available to Staff upon request, both during and after performance of the work

The proposer must expressly affirm its ability and willingness to attest to its work in accordance with the specified requirements

SCHEDULE B

Phase I Examination Questions

1. Is there a documented security policy governing this topic?
 - a. If yes, provide a source citation to the documented policy.
2. Is there evidence that the security policy governing this topic has been expressly approved by accountable management?
 - a. If yes, indicate how and when it was so approved.
3. Is there evidence that the security policy governing this topic has been communicated to the affected employees and contractors?
 - a. If yes, how and when was it communicated?
 - b. Is there a related policy that guides the communication of the security policy to new employees and contractors?
4. Is this policy subject to periodic review?
 - a. If yes, is it regularly reviewed?
 - b. What is the date of the most recent review?
 - c. Are the results of the review made actionable by executive management?
5. Is there evidence that this policy has been administered?
 - a. If yes, identify the organization/individual responsible for doing so and documentation to that effect.
6. Has this function been independently audited, either internally or externally?
 - a. If yes, by whom and when?
7. How often has this function been audited, either internally or externally, in the past 5 years?
 - a. Are the results of any such audits available for review or reference?
8. Is there an incident log associated with this topic that is maintained and available for review?
 - a. If so, who is responsible for it?
 - b. What, if any, documentation is available that illustrates the actions taken in response to those incidents?
9. Are there documented policies and procedures that govern how any incident is addressed and resolved?
 - a. Are these policies and procedures employed and enforced?
 - b. Are the results, and any related changes, communicated to the responsible parties?
10. Has there been any risk assessment of this particular topic conducted to date?
 - a. If so, who performed the assessment and what were the conclusions?

- b. Is there any documentation available for review or reference pertaining to that assessment work?
- c. What, if any, response has been made to the risks identified in that assessment?

11. What, if any, consequence is there to any security breach that might be associated with this topic?

- a. Who is responsible for making the determination?
- b. Do the associated employees understand the consequences?
- c. Does the process provide for involvement of law enforcement authorities?

12. Is there a controlled change management process that governs any modification to this topic or matter?

- a. Does the process require executive level authorization for any change?
- b. Is there documentation available for review or reference that demonstrates that the process is employed and enforced?

13. If the topic area involves third party participation, assistance or out-sourcing, is that effort fully supervised?

- a. Is the work undertaken by the third parties subject to further scrutiny before use?
- b. Are background security checks undertaken before engaging third parties?
- c. Are third parties contractually bound?
- d. If so, has the form of contract been tested?
- e. If so, what have been the results of any such test?

	A.5 Information Security Policy	A.6 Organization of Information Security	A.7 Human Resources	A.8 Asset Management	A.9 Access Controls	A.10 Cryptography	A.11. Physical and Environmental Controls	A.12. Operational Security
	Priority ITGC AUISP	Priority ITGC AUISP	Priority ITGC AUISP	Priority ITGC AUISP	Priority ITGC AUISP	Priority ITGC AUISP	Priority ITGC AUISP	Priority ITGC AUISP
Internal Wire and Cables							H K6, NK1	
External wire and Cables Controller, routers					H K3 Sec. 7		H K6, NK1	H K12, K13 Sec 8,10.1, 15
Servers		H Sec. 6, 11			H K3 Sec. 7		H K6, NK1	H K12, K13 Sec 8,10.1, 15
Computing Stations		H Sec. 6, 11			H K2 Sec. 7			H Sec 8,10.1, 15
Other Attached Devices -including Mobile	H K1	H Sec. 6, 11			H K2 Sec. 7			H Sec 8,10.1, 15
Incoming Data and Sources	H K1	H Sec. 6, 11		H Sec. 5, 10	H K2 Sec. 7			
Retained Data	H K1	H Sec. 6, 11		H Sec. 5, 10	H K2 Sec. 7			H K12, K13 Sec 8,10.1, 15
Outgoing Data and Destination	H K1	H Sec. 6, 11		H Sec. 5, 10	H K3 Sec. 7	H Sec 7.10,10.5		
Software in Development	H K1	H K12 Sec. 6, 11						
Production Software		H K12 Sec. 6, 11			H K3 Sec. 7			H K12, K13 Sec 8,10.1, 15
Software Interfaces	H K1	H K12 Sec. 6, 11			H K3 Sec. 7			H K12, K13 Sec 8,10.1, 15
Power Supplies and AC		H Sec. 6, 11			H		H K6, NK1	
Building Organization								
People Permissions		H K3 Sec. 6, 11	H Sec. 11					
Safety Training and Review	H K1	H Sec. 6, 11	H Sec. 11					

Legend	
ITGC	
PwC 27001 Network Assessment	
Acceptable Use and Information Security Policy	
Third Party Service Provider Security Contract Addendum	
H	Items to be covered in Phase 2 plus gaps from Phase 1

PCL XL error

Subsystem: GE_VECTOR

Error: GEEmptyClipPath Warning: IllegalMediaSize