STATE OF NEW HAMPSHIRE
PUBLIC UTILITIES COMMISSION

LIBERTY UTILITIES (ENERGYNORTH NATURAL GAS) CORP.
d/b/a LIBERTY

Docket No. DG 20-105

Distribution Service Rate Case

Record Request – Exhibit 58

REQUEST:

Please provide the directive from the Department of Homeland Security that supports the Company's installation of forward-looking infrared (FLIR) cameras at the Keene and Manchester production facilities, listed as projects 8840-2044 and 8843-2044 in Exhibit 49 at Bates 028 (and elsewhere in this docket).

RESPONSE:

The requirement for Liberty to install the FLIR cameras and associated equipment in Keene and Manchester arises from the Chemical Facility Anti-Terrorism Standards ("CFATS") law, 6 U.S.C. §621 *et seq*. The CFATS law established within the Department of Homeland Security ("DHS") a program to, among other things, "identify … covered chemical facilities," to "establish risk-based performance standards designed to address high levels of security risk at covered chemical facilities," and to "require each covered chemical facility to … develop, submit, and implement a site security plan." 6 U.S.C. §622(a)(2). Failure to comply could result in civil penalties. 6 U.S.C. § 624.

DHS subsequently promulgated rules that more specifically directed Liberty to undertake the work at issue here:

> Each covered facility must select, develop in their Site Security Plan, and implement appropriately risk-based measures designed to satisfy the following performance standards:
>
> (1) Restrict area perimeter. Secure and monitor the perimeter of the facility.

DHS also issued a guidance document to help covered facilities comply with the law, including specific guidance on how covered facilities may comply with the requirement to "secure and

monitor the perimeter of the facility" by breaking down that broad directive into a number of metrics. Excerpts of the Guidance are attached.

As to Metric 1.4, which addresses "monitoring and surveillance," the Guidance states as follows:

> The facility has a monitoring system that allows for the identification of the presence of an intrusion in the area(s) containing critical asset(s). To achieve this, a facility typically could, for example, use security patrols of the facility or an integrated monitoring system that provides intrusion detection and video surveillance around the facility perimeter or critical assets and is fully operable during all lighting conditions.

Risk-Based Performance Standards Guidance, attached, at Bates 009. Note that Liberty's facilities are Tier 4 covered chemical facilities due to the storage of propane in Keene and both propane and LNG in Manchester. See 6 C.F.R. Part 27, Appendix A.

To comply with these requirements, Liberty installed the FLIR cameras in Keene and Manchester and incurred the costs that are detailed in the documents related to projects 8840-2044 and 8843-2044.

DHS visited the sites after installation and provided Liberty with oral confirmation that the FLIR cameras satisfied the CFATS law.

Risk-Based Performance Standards Guidance

Chemical Facility Anti-Terrorism Standards

May 2009

Homeland Security

Department of Homeland Security
Office of Infrastructure Protection
Infrastructure Security Compliance Division
Mail Stop 8100
Washington, DC 20528
Website: www.dhs.gov/chemicalsecurity

Table of Contents

Note: This document is a "guidance document" and does not establish any legally enforceable requirements. All security measures, practices, and metrics contained herein simply are possible, nonexclusive examples for facilities to consider as part of their overall strategy to address the risk-based performance standards under the Chemical Facility Anti Terrorism Standards and are not prerequisites to regulatory compliance.

Table 3: RBPS Metrics – RBPS 1 – Restrict Area Perimeter				
RBPS 1 - Restrict Area Perimeter - Secure and monitor the perimeter of the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 1.1 – Perimeter Security	The facility has an extremely vigorous, high-integrity system to secure the perimeter that severely restricts or delays any attempts by unauthorized persons to gain access to the facility. To achieve this standard, a facility could, for example, use the following: • An exterior perimeter security fence or equivalent barrier that meets industrial consensus standards. • A clear zone on either side of the fence that allows persons to be detected at the boundary. Where vehicles can access either side of the boundary, the clear zone is wide enough to allow detection of the presence of vehicles.	The facility has a vigorous, high-integrity system to secure the perimeter that would give unauthorized persons a very low probability of gaining access to the facility. To achieve this standard, a facility could, for example, use the following: • An exterior perimeter security fence or equivalent barrier that meets industrial consensus standards. • A clear zone on either side of the fence that allows persons to be detected at the boundary. Where vehicles can access either side of the boundary, the clear zone is wide enough to allow detection of the presence of vehicles.	The facility has a system to secure the perimeter that would give unauthorized persons a low probability of gaining access to the facility. To achieve this standard, a facility could, for example, use a single security barrier, such as: • An exterior perimeter security fence or equivalent barrier that meets industrial consensus standards.	The facility has a system to secure the perimeter that reduces the possibility of access to the facility by unauthorized persons. To achieve this standard, a facility could, for example, use a single security barrier, such as: • An exterior perimeter security fence or equivalent barrier that meets industrial consensus standards.
Metric 1.2 – Vehicle Barriers	Vehicles would have a very low likelihood of accessing the facility by force anywhere along the entire perimeter where vehicle attack is a possible mode of attack. To achieve this, a facility could use, for example: • Vehicle deterrence measures, such as bollards, landscaping, berms, ditches, drainage swale, or buried concrete anchors retaining anti-vehicle cable wherever the perimeter is accessible to a vehicle. • Entrances equipped with traffic control systems to slow incoming traffic, such as serpentine barriers outside the gate.	Vehicles would have a low likelihood of accessing the facility by force anywhere along the entire perimeter where vehicle attack is a possible mode of attack. To achieve this, a facility could use, for example: • Vehicle deterrence measures, such as bollards, landscaping, berms, ditches, drainage swale, or buried concrete anchors retaining anti-vehicle cable wherever the perimeter is accessible to a vehicle. • Entrances equipped with traffic control systems to slow incoming traffic, such as serpentine barriers outside the gate.	Vehicles would have a reduced likelihood of accessing the facility by force anywhere along the entire perimeter where vehicle attack is a possible mode of attack. To achieve this, a facility could use, for example, active or passive barriers at perimeter control points where vehicles normally enter and leave the facility and other anti-vehicle barriers, such as ditches, revetments, or other man-made or naturally occurring barriers, for the remainder of the perimeter where vehicle attack is a possible mode of attack.	Vehicles would have a reduced likelihood of accessing the facility by force at the perimeter control points where vehicles normally enter and leave the facility. To achieve this, a facility could, for example, use anti-vehicle barriers such as ditches, revetments, or other man-made or naturally occurring barriers.

Table 3: RBPS Metrics – RBPS 1 – Restrict Area Perimeter				
RBPS 1 - Restrict Area Perimeter - Secure and monitor the perimeter of the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
Metric 1.3 – Standoff Distance	Sufficient vehicle standoff distance or alternative protective means are provided to ensure that a VBIED is extremely unlikely to be able to compromise a critical asset.		N/A	
Metric 1.4 – Monitoring and Surveillance	The facility has an extremely reliable perimeter monitoring system that continuously monitors the entire length of the facility perimeter or the perimeter around each critical asset, allows for the identification and evaluation of an intrusion in real time, and provides notification of intrusion to a continuously manned location. In the context of this metric, "real time" means that an adversary act virtually always is detected and reported to responders at the time of occurrence. "Extremely reliable" means that the monitoring system is operable during all anticipated conditions, including complete darkness, twilight, inclement weather, and loss of power; with monitoring system components designed, laid out, and constructed to avoid common cause/dependent failures and provide redundant signal processing equipment where digital signal processing is used. To achieve this, a facility typically could, for example, use an integrated, multi-sensor system that: • Provides intrusion detection and video surveillance around 100% of the perimeter or 100% of the perimeter around all critical assets. • Provides images or other output that are continuously monitored by a dedicated person, software, or other detection method used in	The facility has a very reliable perimeter monitoring system that continuously monitors the entire length of the facility perimeter or the perimeter around each critical asset, allows for the identification and evaluation of an intrusion in real time, and provides notification of intrusion to a continuously monitored location. In the context of this metric, "real time" means that an adversary act most likely is detected and reported to responders at the time of occurrence. "Very reliable" means that the monitoring system is operable during ambient light, inclement weather, and fluctuating power conditions; with monitoring system components designed, laid out, and constructed to avoid common cause/dependent failures and provide redundant signal processing equipment where digital signal processing is used. To achieve this, a facility typically could, for example, use an integrated monitoring system that: • Provides intrusion detection and video surveillance around the facility perimeter or critical assets. • Provides images or other output that are continuously monitored by a dedicated person,	The facility has a reliable perimeter monitoring system that allows for the identification of the presence of an intrusion in real time for the area(s) containing critical asset(s). In the context of this metric, "real time" means that an adversary act likely is detected and reported to responders in a timely manner. "Reliable" means that the monitoring system is operable during ambient light conditions. To achieve this, a facility typically could, for example, use an integrated monitoring system that: • Provides intrusion detection and video surveillance around the facility perimeter or critical assets. • Has emergency back-up power and/or an equivalent written contingency procedure.	The facility has a monitoring system that allows for the identification of the presence of an intrusion in the area(s) containing critical asset(s). To achieve this, a facility typically could, for example, use security patrols of the facility or an integrated monitoring system that provides intrusion detection and video surveillance around the facility perimeter or critical assets and is fully operable during all lighting conditions.

Table 3: RBPS Metrics – RBPS 1 – Restrict Area Perimeter				
RBPS 1 – Restrict Area Perimeter - Secure and monitor the perimeter of the facility.				
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**
	conjunction with the system. • Has emergency backup power and/or an equivalent written contingency procedure. • Has general-area as well as access-portal (face-view) CCTV surveillance at all gates.	software, or other detection method used in conjunction with the system. • Has emergency backup power and/or an equivalent written contingency procedure.		