uniongas
An Enbridge Company

July 17, 2017

Ms. Kirsten Walli
Board Secretary
Ontario Energy Board
2300 Yonge Street, 27th Floor
Toronto, ON M4P 1E4

Dear Ms. Walli:

Re: Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario (Cyber Security Framework)
Board File No. EB-2016-0032

Following are the submissions of Union Gas Limited on the Staff Report to the Board on a proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors and the accompanying industry-developed Cyber Security Framework.

On June 1, 2017, the Ontario Energy Board released the Staff Report on a Proposed Cyber Security Framework along with a companion white paper developed by AESI Inc. for comment.

The AESI white paper sets out the proposed Cyber Security Framework which is intended to provide oversight and validation of the cyber security measures taken by electricity distributors and transmitters for non-bulk assets in Ontario for the protection of consumer privacy and the electricity system infrastructure. The proposed Cyber Security Framework is designed to address what it describes as the primary problems facing electricity distributors:

(1) insufficient threat awareness;
(2) convergence of information technology and operational technology;
(3) lack of cyber security-trained human resources;
(4) copious third-party access; and
(5) insufficiently widespread use of security tools.

The AESI white paper identifies potential vulnerabilities at various stages of the electricity system, including network protocols and physical security.

The proposed Cyber Security Framework then identifies best practices that should be built into Ontario's smart electricity grid to ensure reliability and consumer protection, and lays out a number of self-assessment tools to assess risk profile and preparedness at the LDC level. The proposed Cyber Security Framework relies on LDC self-assessment and self-certification to ensure that best practices are uniformly applied across Ontario's energy sector.

The proposed Cyber Security Framework is expected to be implemented in late 2017 with LDCs required to start submitting cyber security reports to the OEB within three months of the issuance of the Framework. Additionally, LDCs will also be subject to annual cyber security self-certification of cyber security capability starting in 2018.

The Board has invited comments from all interested stakeholders on the proposed Cyber Security Framework or Staff Report, especially in the following areas:

- Regulatory requirements and reporting;
- Additional implementation tools and guidance required;
- Adequate guidance with respect to integration of privacy requirements; and
- Other aspects to be incorporated.

NIST Framework Background

Cyber security threats and exploits have increased in complexity and connectivity of critical infrastructure systems, placing Canada's and the United States' security, economy, public safety and health at risk. Similar to financial and reputational risk, cyber security risk affects a company's financial results. It can drive up costs and impact revenue. It can also harm an organization's ability to innovate and to gain and maintain customers.

To better address these risks, the President of the United States issued Executive Order 13636 ("Improving Critical Infrastructure Cyber Security") on February 12, 2013 which called for the development of a voluntary Cyber Security Framework that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk. The intent was to enhance the security and resilience of critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. [1]

The Executive Order also required the cyber security framework to include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cyber security activities. While processes and existing needs will differ, the cyber security framework was to be designed to assist organizations in incorporating privacy and civil liberties as part of a comprehensive cyber security program.

The National Institute of Standards and Technology (NIST) is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. NIST delivered a cyber security framework that focuses on using business drivers to guide cyber security activities and considering cyber security risks as part of the organization's risk management processes.

[1] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014, pages 1 - 2

The NIST cyber security framework, created through collaboration between government and the private sector, uses a common language to address and manage cyber security risks in a cost-effective way based addressing business needs without placing additional regulatory requirements on businesses.

Equally important, the NIST cyber security framework is not a one-size-fits-all approach to managing cyber security risk for critical infrastructure. The NIST framework enables organizations – regardless of size, degree of cyber security risk, or cyber security sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The NIST framework provides organization and structure to today's multiple approaches to cyber security by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cyber security, the NIST framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cyber security.

Organizations continue to have unique risks, different threats, different vulnerabilities, and different risk tolerances. How they implement the practices in the NIST framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the NIST framework is aimed at reducing and better managing cyber security risks.

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

With an understanding of risk tolerance, organizations can prioritize cyber security activities, enabling organizations to make informed decisions about cyber security expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cyber security programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

The NIST framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cyber security. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cyber security activities that reflect desired outcomes. Thus, the framework gives organizations the ability to dynamically select and direct improvement in cyber security risk management for the information technology and operational technology environments.

The NIST framework helps organizations manage and reduce cyber security risks. The framework assists in identifying the most important activities to assure critical operations

and service delivery. It helps prioritize investments and provides a common language inside and outside the organization for cyber security and risk management.

The NIST framework is based on well-known standards and practices, and represents the best current practice in cyber security. However, each organization and industry will have to identify their special themes and topics to pay particular attention to. Most topics, however, are common to all sectors.

The Implementation Tiers of the NIST framework provide context on how an organization views cyber security risk and the processes in place to manage that risk. The tiers describe an increasing degree of rigor and sophistication in cyber security risk management practices and the extent to which cyber security risk management is informed by business needs and is integrated into an organization's overall risk management practices.

The tiers are sometimes referred to as maturity levels, but according to NIST they are more a tool for internal communication between cyber security risk management and operational risk management, and should not be seen as maturity level. Nevertheless, higher tiers represent higher degree of sophistication and maturity in the management of cyber security risks and responses.

- Tier 1 – Partial
  Organizational cyber security risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. There is limited awareness of cyber security risk at the organizational level and an organization-wide approach to managing cyber security risk has not been established.

- Tier 2 - Risk Informed
  Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cyber security activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. There is an awareness of cyber security risk at the organizational level but an organization-wide approach to managing cyber security risk has not been established. Cyber security information is shared within the organization on an informal basis.

- Tier 3 – Repeatable
  The organization's risk management practices are formally approved and expressed as policy. Organizational cyber security practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape. There is an organization-wide approach to manage cyber security risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.

- Tier 4 – Adaptive
  The organization adapts its cyber security practices based on lessons learned and predictive indicators derived from previous and current cyber security activities.

Through a process of continuous improvement incorporating advanced cyber security technologies and practices, the organization actively adapts to a changing cyber security landscape and responds to evolving and sophisticated threats in a timely manner. The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cyber security before a cyber security event occurs.

The NIST framework consists of 5 core functions:

1. Identify - Develop the organizational understanding to manage cyber security risk to systems, assets, data, and capabilities.
2. Protect - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. Detect - Develop and implement the appropriate activities to identify the occurrence of a cyber security event.
4. Respond - Develop and implement the appropriate activities to take action regarding a detected cyber security event.
5. Recover - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event.

Union Gas Alignment to the NIST Framework

Spectra Energy (Union's previous parent company), and by association Union Gas, adopted the NIST cyber security framework in principle once it was published in February 2014.

In 2016, the Enbridge Cyber Controls Framework was completed. In keeping with best practice, it applies the relevant components of external frameworks including those of the National Institute of Standards in Technology (NIST) and the Center for Internet Security (CIS) standard, Control Objectives for Information and Related Technologies (COBIT) and Payment Card Industry (PCI) standards. It further applies the Enbridge Enterprise Risk Framework and produces a controls framework that provides a higher granularity focus on cyber security risks and threats specific to Enbridge and establishes Enbridge's cyber security risk tolerance levels, which in turn allows management to be targeted in our cyber security investments.

The outcome of this work was the development of controls that provide greater granularity on the existing Enbridge cyber security standards and three policies that have governed the program since 2015. The controls can be categorized as technical controls (automation i.e., firewalls), operational controls (process and automation i.e., vulnerability management), and operational and process controls (i.e., technology change control).

This collection of policies, standards and controls form the Enbridge Cyber Controls Framework and the Cyber Security Program and associated Cyber Security Scorecard provide tactics, plans and measurement to reinforce the controls needed to keep risk within acceptable tolerance. This program applies to information and operational technology including Industrial Control Systems.

At Union Gas, through the integrated services with Enbridge, we perform the following cyber security functions in accordance with the core functions of the NIST framework:

Identify

Through the use of threat and risk assessments, information security risk management is an essential part of an effective approach to information systems security and involves cyber risk assessments and risk treatment plans. Our security risk management approach increases management awareness of information security exposures, provides a practical mechanism for understanding the magnitude of exposures, assists in the evaluation and selection of appropriate safeguards and helps in the prioritize of competing risks.

Processes are in place to support compliance of cyber security activities with applicable privacy laws and regulations. Guidelines are in place to aid in the collection of electronic information and also to protect the employees and contractors gathering the information. This ensures that considerations are made for the collection of information, the information required and the resources needed to gather and interpret the data. It also enables appropriate parties to be notified and approve (IT Security, Corporate Security, Human Resources, Legal, Compliance) of the reasoning behind the request and ensures privacy rights are protected consistent with our policy. This procedure applies across the enterprise.

Documentation of asset owners and custodians (includes asset classification). Within Union Gas, the Application Teams have developed an asset management plan. The asset management plan inventoried all applications, identifies key applications and provides a risk based score that has included cyber security. This inventory list and scoring undergoes and annual review process.

A centralized cyber risk governance and policy team exists to develop the enterprise cyber security policies. Union's polices are based on the NIST framework. Owners of the cyber security controls are responsible for communicating, developing and implementing procedures and guidelines that align with the policy. The cyber security control framework has an annual review process to incorporate feedback from the various control owner areas.

Protect

The identification and authorization of individuals to access organizational assets and systems is completed through Union's Identity and Access Management program with semi-annual access reviews and documented employee and contractor hire and termination processes, privileged access management process and segregation of duties as it relates to IT functions.

IT Change Management is handled through an application workflow that has defined processes and timelines for each change type. Changes are classified into one of five categories, namely; standard, minor, significant, major and emergency. Each type requires a specific set of approval conditions and flow. Significant and major changes go through either a change approval board, technical advisory board or both for review. Implementation of a change follows a specific flow from development, quality assurance and finally to the production environment.

Enterprise-wide security awareness training sessions are conducted during our annual compliance event which is mandatory for all employees. There are also phishing simulation tests and training programs that send out simulated phishing emails company-wide. Training is provided to new employees and employees that are deemed to be at a higher risk.

Union Gas uses confidential, proprietary and personal data in the course of doing business. This includes commercially sensitive information related to Union as well as third parties. Union Gas complies with laws, regulations and applicable industry standards intended to protect sensitive data from unlawful disclosure and use. Failure to comply with these laws, regulations and standards can cause irreparable damage to our brand and can result in legal penalties, adverse regulatory actions and restrictions on normal business operations. It can also prohibit us from doing business within certain countries. There are data security treatments in place based on these classifications.

Examples of data security controls that Union already has in place:

- Data encryption in transit when it is being sent or received from a third party.
- Data encryption at rest in databases.
- Hard drives on laptops are encrypted.
- Input sanitization for externally facing web applications. The web sessions are protected through secure connectivity.
- Proper segmentation of internet web applications from the internal networks.

Detect

The Security Operations Center (SOC) collects log data from various sources such as servers, perimeter protection appliances, critical applications, anti-virus appliances, etc. and, through the use of technical correlation and algorithms, determines if a security incident may have occurred. The SOC specialist investigates potential incidents and takes appropriate action to secure the network and other computer related environments.

Vulnerability management is the process of utilizing vulnerability scanning, patching, to make decisions on what the best course of action may be with an identified vulnerability. Vulnerability scanning consists of using a computer program to identify vulnerabilities in computer or network infrastructure. It is an input into the vulnerability management program. Union's cyber security program is committed to be compliant with our policies, implement best practices in a practical manner and to respond to our findings. This is accomplished by completing weekly scans and providing the results to our support teams to remediate.

Union Gas participates in the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC). It is an association made up of similar companies across North America that share cyber security related information anonymous. Security specialists share threat indicators, vulnerabilities, and remediation plans among association members.

Respond

Centralized security incident management ensures that Cyber Incident Responses are managed at the appropriate level relative to the threat and risk they may pose. This approach ensures that the program complies with all applicable laws and regulations, ensures that response procedures are available for security related threats and incidents, manages security related activities and resources during an incident and ensures that the plans are update to date, validated and tested.

Recover

Union's security recovery plan is an integrated component of our applications and their associated environment's backup plan and our application disaster recovery plan. Disaster recovery planning is one of the disciplines associated with our integrated preparedness planning activities. It is the process of having resources and arrangements ready to re-enable computer operations of critical and essential software applications and related components after a catastrophe event. Recovery Planning is the "technology partner" of business continuity plan.

Concerns with OEB Staff's Proposed Cyber Security Framework

The regulatory and legislative basis for the proposed cyber security framework is not clearly evident to Union.

Union has already identified the appropriate cyber security risks and have either addressed gaps or have made plans to address them. Union is concerned that mandatory participation in and reporting associated with the Board Staff's proposed cyber security framework would result in duplication of effort with questionable benefit to ratepayers and no identifiable improvement to outcomes consistent with the Renewed Regulatory Framework.

Given that we are already a member of well-established information sharing forums such as the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC), the Canadian Gas Association (CGA), the Interstate Gas Association of America (INGAA), and the Canadian Cyber Incident Response Centre (CCIRC), Union feels that participation in the OEB's proposed Cyber Security Information Sharing Forum (CSIF) should be left to our discretion. Union is also concerned that the OEB's proposed cyber security framework will deviate from the NIST framework over time, l4eaving Union to manage within two cyber security frameworks.

The Board Staff report appears to position the OEB as an entity proficient in cyber security, where it develops initiatives and guidance for the energy sector and drives related policy. In its whitepaper, AESI suggests that a Centralized Compliance Authority (CCA) could be established as a sector-created and managed entity or a separate division within the OEB[2].

AESI has recommended in their implementation plan that the self-assessment questionnaire results be managed by the proposed CCA[3]. Typically, the responses to these questionnaires

[2] AESI White Paper - Cyber Security Framework, page 60

[3] AESI White Paper - Cyber Security Framework, page 60

contain commercial information that is highly sensitive. Adequate privacy safeguards must be put in place to protect access to such information.

AESI further recommends developing status and trending reports for the OEB to measure the progress of the LDCs in reaching baseline controls:

- Percentage of staff dedicated to cyber security
- Percentage of employees with super user access
- Percentage of endpoints with inactive/suspended end-point protection tools (i.e., virus and firewall)
- Percentage of un-patched "known" vulnerabilities
- Number of successful cyber security breaches within the year
- Number of detected network attacks during the year
- Average number of days between notification of job departure and elimination of corporate access (physical access and logical access)
- Turns to reporting on the residual risk of the LDCs and the sector by collecting information on the status of the effectiveness of the security controls
    - Establishes risk-based and rotational testing consisting of:
    - Self-assessment
    - Desktop audits
    - On-site tests, by CCA or independent 3rd party

In addition to the aforementioned, other ongoing reporting expectations of the framework are substantial, including a three month interim sign-off, providing the OEB an annual certification confirming that risk profiles have been completed, control requirements have been established, and a current cyber readiness assessment has been completed.

In Union's view, the Board should continue with its original position as stated in its Supplemental Report on Smart Grid dated February 11, 2013 in which the Board established its expectations for electricity distributors and transmitters, including that they should take into consideration cyber security and privacy as they plan for the modernization of their systems. At that time, the Board concluded that it would not develop its own set of cyber security and privacy standards:

> *"The Board will not develop its own set of cyber security and privacy standards but instead will require regulated entities to provide evidence of meeting appropriate cyber security and privacy standards. For example, in the case of cyber security, this could take the form of providing a third-party audit confirming compliance with the standards of the National Institute of Standards and Technology's (NIST) Guidelines for Smart Grid Cyber Security. With respect to privacy, a regulated entity could, for example, provide evidence that existing privacy laws and standards, as well as best practices such as the Privacy by Design framework set by Ontario's Privacy Commissioner, have been met."*[4]

[4] EB-2011-0004 - Report of the Board - Supplemental Report on Smart Grid, February 11, 2013, page 19

Should you have any questions, please do not hesitate to contact me.

Yours truly,

[Original signed by]

Patrick McMahon
Manager, Regulatory Research and Records
pmcmahon@uniongas.com
(519) 436-5325