From:	JMatos@burlingtonhydro.com
To:	Stuart Wright
Cc:	Cybersecurity; Andres Mand
Subject:	Re: Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario (EB 2016-0032) – CSWG - Position Paper Feedback
Date:	October-07-16 2:50:40 PM

HI Stuart,

Thanks for the opportunity to participate in the OEB's Cyber Security Working Group (CSWG), and reviewing the four discussion papers.

Overall I am impressed with the quality of work done to date as demonstrated in the 4 discussion papers. Most of my comments were addressed at the CSWG meeting on Wednesday.

I have only a few additional comments to make:

1. My one overriding comment and concern has to do with the scope of this initiative, specifically the proposed expansion of that scope to include Privacy by Design (PbD) within the framework.

I think we can all agree that there is a clear linkage between privacy and security. And Privacy by Design is an excellent set of principles to follow in designing or redeveloping business systems to ensure privacy is built in from the ground up.

However privacy and security are different domains with different scopes, and have different customer facing aspects; therefore they are cover by different roles and responsibilities in most enterprises and within the LDC's. By practice and by regulation every enterprise in Ontario has a Privacy Officer. The title and area of responsibility may differ by company, but the privacy officer is often attached to the Legal, HR or Customer Relations departments.In my experience this role is rarely if ever in the IT, OT, or Security departments. On the other hand cyber security is most often within the IT departments, sometimes with a distinct CISO role. This organizational state reflects the differences in these two domains.

As I understood it, the focus of the cyber security framework is on security of the organization's IT and OT (cyber) assets, including data and databases, servers, networks, programmable devices, etc. On the other hand, PbD is concerned with data design, usage and minimization, limited retention, specific purpose, etc. These are important from a privacy perspective, but are not directly relevant to cyber security. In other words, cyber security is concerned with protecting the data and other assets from exposure or intrusion, but is not directly concerned with how that data is used within the business application or if the organization is collecting more data than is necessary to perform its functions.

By embedding Privacy by Design within the cyber security framework at this stage will present several problems that will make implementation more challenging and problematic. Such challenges include, but are not limited to:

- bringing the Privacy Officer at each LDC into the conversation and direction of cyber security; at this late stage and with a tight deadline looming, that will add time to the process and delay the deliverables
- PbD is primarily a systems engineering process for developing or enhancing applications and databases that house private and confidential data; cyber security is concerned with the processes to secure the data (and all other IT and OT assets) from internal or external exposure or intrusion
- by mixing these two domains, we risk "muddying the waters" in terms of scope, and risk

confusing or diluting the accountabilities between the CISO and the Privacy Officer

Notwithstanding AESI's compelling analysis in section 4 of the Standards Assessment Discussion Paper, I would recommend that we stick to the original scope of cyber security, perhaps make reference to PbD in the Framework for informational purposes only, and consider embedding PbD into the framework at a later phase, with more time to thoroughly consider and understand where these two domains intersect, and also where they differ and why. My issue is not with inclusion of PbD, but the timing and complexity. If time is of the essence then scope creep must be contained.

2. As an added comment, I would suggest the Glossary include a definition of cyber security, and clarify the definition of Privacy by Design.

3. In order to ensure the Framework is implemented in a reasonable timeframe and with consistency across all LDC's, it would be very beneficial for the OEB, or a body designated by the OEB (such as IESO or EDA or a vendor such as AESI) to develop standard programs and templates that can be used by all the LDC's for many of the Framework deliverables, e.g. Security Awareness Programs, Executive and Board level reporting or dashboards, perhaps lists of vetted vendors capable of providing certain services or software, etc. This would significantly reduce implementation time and complexity, and may be the only way that small LDC's can cope with this.

4. I have not addressed spelling or grammatical issues as I am sure you will have picked those up already. However, I would note that on pages 1 and 33 of the Electrical System Cyber Risk Awareness Discussion Paper, the correct word is "tenets" (not "tenants") of the Framework.

Thanks for taking these comments into consideration.

Respectfully submitted,

John Matos

Burlington hydro
energizing our community™
partner since 2009
John Matos
Interim Chief Information Officer
1340 Brant Street, Burlington, ON · L7R 3Z7 · (905)·336·4380
burlingtonhydro.com jmatos@burlingtonhydro.com