From: Dennis and Sharon Noble [mailto:dsnoble@shaw.ca]
Sent: December 11, 2015 9:18 PM
To: 'Dan.Albas@parl.gc.ca' <Dan.Albas@parl.gc.ca>; 'John.Aldag@parl.gc.ca' <John.Aldag@parl.gc.ca>; 'Mel.Arnold@parl.gc.ca' <Mel.Arnold@parl.gc.ca>; 'Terry.Beech@parl.gc.ca' <Terry.Beech@parl.gc.ca>; 'Rachel.Blaney@parl.gc.ca' <Rachel.Blaney@parl.gc.ca>; 'Richard.Cannings@parl.gc.ca' <Richard.Cannings@parl.gc.ca>; 'nathan.cullen@parl.gc.ca' <nathan.cullen@parl.gc.ca>; 'don.davies@parl.gc.ca' <don.davies@parl.gc.ca>; 'Sukh.Dhaliwal@parl.gc.ca' <Sukh.Dhaliwal@parl.gc.ca>; 'Todd.Doherty@parl.gc.ca' <Todd.Doherty@parl.gc.ca>; 'fin.donnelly@parl.gc.ca' <fin.donnelly@parl.gc.ca>; 'ed.fast@parl.gc.ca' <ed.fast@parl.gc.ca>; 'hedy.fry@parl.gc.ca' <hedy.fry@parl.gc.ca>; 'Stephen.Fuhr@parl.gc.ca' <Stephen.Fuhr@parl.gc.ca>; 'Randall.Garrison@parl.gc.ca' <Randall.Garrison@parl.gc.ca>; 'Pam.Goldsmith-Jones@parl.gc.ca' <Pam.Goldsmith-Jones@parl.gc.ca>; 'Ken.Hardie@parl.gc.ca' <Ken.Hardie@parl.gc.ca>; 'Gord.Johns@parl.gc.ca' <Gord.Johns@parl.gc.ca>; 'peter.julian@parl.gc.ca' <peter.julian@parl.gc.ca>; 'Jenny.Kwan@parl.gc.ca' <Jenny.Kwan@parl.gc.ca>; 'Alistair.MacGregor@parl.gc.ca' <Alistair.MacGregor@parl.gc.ca>; 'Sheila.Malcolmson@parl.gc.ca' <Sheila.Malcolmson@parl.gc.ca>; 'Elizabeth.May@parl.gc.ca' <Elizabeth.May@parl.gc.ca>; 'Ron.McKinnon@parl.gc.ca' <Ron.McKinnon@parl.gc.ca>; 'cathy.mcleod@parl.gc.ca' <cathy.mcleod@parl.gc.ca>; 'joyce.murray@parl.gc.ca' <joyce.murray@parl.gc.ca>; 'Joe.Peschisolido@parl.gc.ca' <Joe.Peschisolido@parl.gc.ca>; 'Carla.Qualtrough@parl.gc.ca' <Carla.Qualtrough@parl.gc.ca>; 'Murray.Rankin@parl.gc.ca' <Murray.Rankin@parl.gc.ca>; 'Dan.Ruimy@parl.gc.ca' <Dan.Ruimy@parl.gc.ca>; 'HarjitS.Sajjan@parl.gc.ca' <HarjitS.Sajjan@parl.gc.ca>; 'Randeep.Sarai@parl.gc.ca' <Randeep.Sarai@parl.gc.ca>; 'Jati.Sidhu@parl.gc.ca' <Jati.Sidhu@parl.gc.ca>; 'Wayne.Stetski@parl.gc.ca' <Wayne.Stetski@parl.gc.ca>; 'Kennedy.Stewart@parl.gc.ca' <Kennedy.Stewart@parl.gc.ca>; 'Mark.Strahl@parl.gc.ca' <Mark.Strahl@parl.gc.ca>; 'mark.warawa@parl.gc.ca' <mark.warawa@parl.gc.ca>; 'Dianne.Watts@parl.gc.ca' <Dianne.Watts@parl.gc.ca>; 'Jonathan.Wilkinson@parl.gc.ca' <Jonathan.Wilkinson@parl.gc.ca>; 'Jody.Wilson-Raybould@parl.gc.ca' <Jody.Wilson-Raybould@parl.gc.ca>; 'alice.wong@parl.gc.ca' <alice.wong@parl.gc.ca>; 'Bob.Zimmer@parl.gc.ca' <Bob.Zimmer@parl.gc.ca>
Subject: Smart meter cybersecurity

Dear Members of Parliament for BC,

Over the last 2-3 years I have been receiving and sharing information about the smart meter program as it has been mandated and implemented in British Columbia. This is a provincial program and therefore I have been attempting to have MLAs and the government acknowledge most of the problems which are not in federal jurisdiction.

One major problem that I have raised is cybersecurity. Like all the other problems, this too has not been acknowledged by any provincial politician or BC Hydro. In its most recent financial report there is not one dollar allotted to address this vital issue. Therefore, I am raising it to you, our federal representatives.

The smart grid is being developed across the continent and, when completed, will be shared with the U.S. The major components are wireless, such as the smart meters which are key and vulnerable entry points. Various agencies and departments in the U.S. government, the FBI, CIA, Homeland Security and Congress, have been warning about potential cyberattack or accident, with dire warnings of returning to the "dark ages" for many months or even years when (not if) such an incident occurs.

Recently CSIS finally has acknowledged the issue. (see #4 below). And last week US Congressman Donald Norcross issued warnings about the smart meters on homes increasing vulnerability of the electrical grid. According to many experts in cybersecurity, the grid may already have a virus in it, waiting to attack. When this happens, all of our infrastructure will be affected. We will be left without food, water, heat, and essential services. Former US CIA director Leon Panetta believes this will be the "next" Pearl Harbor. (#7 below), and this time Canada will be a direct victim of the attack.

There has been no indication from the former government that any increased measures were being taken or that provincial utilities were being required to increase their security measures. I ask that you bring this to the attention of the minister responsible for security, and to Prime Minister Trudeau. BC Hydro must be ordered to spend the necessary money to immediately protect the citizens of BC, just as all utilities across Canada must be.

Below are a few of the many references pertaining to this issue that I have gathered. Should you have questions about any of them or if you would like more information, please let me know.

Respectfully,
Sharon Noble
Victoria, BC
250-478-7892

1) ***"More than a year ago, our colleague from the Global Research and Analysis Team, David Jacoby looked around his living-room, and decided to investigate how susceptible the devices he owned were to a cyber-attack. He discovered that almost all of them were vulnerable. So, we asked ourselves: was that a coincidence, or are the smart 'IoT' products currently on the market really that exposed? To find the answer, earlier this year***

we gathered up a random selection of connected home devices and took a look at how they work.

…cybercriminals are not the only ones who might become interested in IoT. For instance, this summer the Russian Ministry of Interior Affairs ordered (RU) to research possible ways of collecting forensic data from devices built with the use of smart technologies. And the Canadian military recently published a procurement request for a contractor that can "find vulnerabilities and security measures" for cars and will "develop and demonstrate exploits".

This doesn't mean that people should avoid using the IoT because of all the risks. The safe option is to choose wisely: consider what IoT device or system you want, what you plan to use it for and where."

https://securelist.com/analysis/publications/72595/surviving-in-an-iot-enabled-world/

2) **CBC report on the sorry state of Canada's preparation for a cyberattack and data hacking.**

http://www.cbc.ca/news/technology/canada-cybercrime-hacking-seglins-1.3312153

3) **Ontario MPP raises concerns about hacking of $$meters**.

http://news.nationalpost.com/news/canada/smart-meters-are-vulnerable-to-hacking-and-present-a-threat-to-personal-privacy-ontario-new-democrat-warns

4) **"The head of Canada's main spy agency says he views the possibility of a cyberattack by ISIS or other extremist groups on the country's "critical infrastructure" as "a major threat.""**

http://www.cbc.ca/news/canada/csis-cyberattack-michel-coloumbe-1.3325531

5) **"This annex provides a brief overview on the basic ICT security concepts affecting smart grids environments. The next section provides a review of real incidents or events affecting power grids which show that cyber security can have real consequences. Chapter 3 makes a review on risk factors and vulnerabilities that should be considered when protecting smart grids, including aspects such as technological vulnerabilities, human factors or physical security. Section 4 is devoted to the threats and attack scenarios that can take advantage of the vulnerabilities presented in section 3. Chapters 5 and 6 are directly related to the main challenges that security professionals will have to face when protecting smart grids**."

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

6) **"The Bipartisan Policy Center (BPC) has published a new report titled "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat." Its authors include a former director of both the CIA and the NSA, the former chairman of FERC and other notables"**

http://www.smartgridnews.com/story/cia-nsa-and-others-tell-utilities-how-their-cybersecurity/2014-03-05

7) **James Woolsey, former director of the CIA, warns that it is a matter of when, not if, the "smart" grid is attacked or an accident renders it useless and us in the "dark ages".**

http://smartgridawareness.org/privacy-and-data-security/smart-grid-vulnerability/

8) **"Congressman Norcross this week added an amendment to the North American Energy Security and Infrastructure Act of 2015. It calls for the U.S. Energy Secretary to analyze and report to Congress on potential vulnerabilities to our nation's power supply through "smart meters" placed on residential, commercial, and industrial properties. The Norcross amendment was adopted and added to the bill, which passed in the U.S. House of Representatives Thursday."**

https://norcross.house.gov/media-center/press-releases/protecting-our-nation-s-power-supply