Engaging Government authorities in our Security Mandate

Tom O’Neill, Hydro-Québec
• Local and National Environment
• Available tools
• Engagement/Shared Partnership
Environment

• Federal, State/Provincial, Regional, Local
  • Intelligence sharing (Fusion Centres)
  • Regulatory (E-ISAC)
  • Law Enforcement
    • First responders, investigations, intelligence

Remind them importance of Critical infrastructure
Protecting critical infrastructure, including pipelines, electricity grids, financial systems and transportation systems, is essential to ensuring Canada's economic stability and national security. The interconnected nature of critical infrastructure requires governments, the private sector, international allies and first responders to take a coordinated approach. As such, the Sub-sub-program will continue to work with the Government of Canada, law enforcement partners, and the private sector to implement a cybercrime strategy for the protection of digital infrastructure and Canadians online.
27 Separate Federal Programs Protect the Power Grid

And that's just between the Energy Department, the Homeland Security Department and the Federal Energy Regulatory Commission.

By Mohana Ravindranath, Staff Correspondent

FEBRUARY 27, 2017

<table>
<thead>
<tr>
<th>Activity type</th>
<th>Number of federal efforts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency preparedness and response</td>
<td>19</td>
</tr>
<tr>
<td>Research and development</td>
<td>15</td>
</tr>
<tr>
<td>Modelling, analytics, and risk assessment</td>
<td>12</td>
</tr>
<tr>
<td>Standard setting</td>
<td>12</td>
</tr>
<tr>
<td>Information sharing</td>
<td>10</td>
</tr>
<tr>
<td>Institutional support and technical assistance</td>
<td>10</td>
</tr>
<tr>
<td>Regulatory guidance</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: GAO analysis of DOE, DHS, and FERC questionnaire responses. | GAO-17-153
Protecting the Power Grid

Our electricity system is a fundamental component of our quality of life and our economy. It is one of 10 critical infrastructure sectors in North America.

The electricity sector is especially crucial because all the other critical infrastructure sectors depend on electricity. It is vital that we identify emerging threats and that we protect the security, reliability, and stability of the integrated North American power grid.

Providing stable and reliable power to Canadians

While Canada’s electricity system falls within provincial jurisdiction, at the federal level, Public Safety Canada helps to develop management tools and facilitate information sharing in support of strengthening and maintaining the security and reliability of the Canadian electricity system.

In the US, this role is shared by the Department of Energy and the Department of Homeland Security. By participating in security forums at every level of government and on both sides of the border, CEA helps to ensure that the knowledge and expertise of Canadian electricity companies contributes to our shared security.
As we wrap up this year's National Cybersecurity Awareness Month blog series, I hope you now have a better understanding of the Department of Energy's (DOE) commitment to protect the Nation's power grid and oil and natural gas infrastructure from the cyber threat—a rapidly-evolving challenge that requires strong partnerships and a sustained focus on preparedness, cyber incident response and recovery, and innovative research, development, and demonstration of resilient energy delivery systems.

Next month, we will join our partners from industry and the public sector at GridEx IV, the exercise hosted every two years by the North American Electric Reliability Corporation (NERC). These exercises, which simulate scenarios of cyber and physical attacks on the grid, are designed to test and improve the electricity sector's ability to respond. Participants at GridEx IV will include representatives from electric utilities, Federal and regional government agencies, critical
DOE Now Issuing Situation Reports on Hurricane Florence
<table>
<thead>
<tr>
<th>Threat or hazard</th>
<th>Number of federal efforts addressing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberattack</td>
<td>15</td>
</tr>
<tr>
<td>Physical attack</td>
<td>12</td>
</tr>
<tr>
<td>Natural disaster</td>
<td>12</td>
</tr>
<tr>
<td>Operational accident</td>
<td>5</td>
</tr>
</tbody>
</table>

Source: GAO analysis of questionnaire responses from the Department of Energy (DOE), the Department of Homeland Security (DHS), and the Federal Energy Regulatory Commission (FERC). | GAO-17-153
Trump Orders Preparation for Electric Grid Cyber Attacks

Policy upgrade comes as threats to infrastructure increase

BY Bill Gertz Follow @BillGertz
May 12, 2017 2:30 pm

President Trump ordered the federal government to prepare for a devastating cyber attack against America’s electric grid amid growing fears foreign states are set to carry out attacks aimed at plunging the nation into darkness.

A presidential order signed Thursday directed key federal agencies to assess preparations for a prolonged power outage resulting from cyber attacks designed to disrupt the power grid.

An assessment of the danger must be carried out by the Energy Department, Homeland Security, DNI and state and local governments to examine the readiness of the United State to manage a shutdown of the power grid. The assessment will also identify gaps and shortcomings in efforts that would be used restore power.

New cyber security measures outlined in the executive order come as the commander of Cyber Command warned two days earlier that America’s critical infrastructure is vulnerable to disruption by foreign cyber attacks.

Cyber command chief Adm. Mike Rogers said several nations, including Iran, have been tied to disruptions and remote intrusions into U.S. critical infrastructures, such as the electric grid, financial networks, and others.

Rogers said destructive cyber attacks on critical infrastructure are one of his two worst case scenarios. The second involves the threat of cyber intrusions aimed at manipulating data within networks.

Iran tried to disrupt the function of a dam in upstate New York in 2013, and Russia has used industrial control malware called BlackEnergy to attack Ukraine’s electric grid, Rogers said.
Yamana mining digital gold - Find out how
Webinar Digital Transformation: Worth its Weight in Gold
SEPTEMBER 26, 2018 - 1:00 PM TO 2:00 PM ET
REGISTER TODAY

Israel’s guide to securing the national electrical grid
Howard Solomon @howarditwc
Published: January 30th, 2017

HAIFA, Israel – The electrical grid is arguably the most critical infrastructure in a country – without power there’s no water generation, offices and plants close, telecom networks shutdown... and the list goes on.
Tools

– Legislative
  – Tap in
    – Be informed of upcoming legislation
  – Influence
    – Copper theft
    – Drones
    – Other issues which are of concern

– Analysis
  – Task
  – Subscribe
  – Create dialogue
Keep engaged

– Bronze
  – Introduction
  – Training
    – Include government partners in training

– Silver
  – Tie into their priorities
    – Example: GRIZZLY STEPPE 2016

– Gold
  – Think of access to Senior Management
    – Good info for Senior Management

Plan annually and use sparingly
Tom O'Neill
Chef – Plan d’urgence corporatif, sécurité internationale et Évaluation du risque et de la menace
Direction principale - Sécurité Corporative
Tél. : (514) 289-2211 poste 7267
Mobile : (438) 888-7267
Courriel : oneill.tom@hydro.qc.ca