

Congress of the United States
House of Representatives
Washington, DC 20515-2105

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396-2900188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875-2900<http://markey.house.gov>

February 20, 2013

The Honorable Fred Upton
Chairman, House Committee on Energy and Commerce
The United States House of Representatives

Dear Chairman Upton,

I am writing to follow up on my November 20, 2012 letter (to which I have yet to receive a response) and to urge you in the strongest possible terms to take immediate action to pass the bipartisan GRID Act legislation we co-authored several years ago, so that we can secure our nation's electrical grid against devastating damage from cyber terrorist attacks. Based on an analysis released yesterday by the cyber-security company Mandiant¹ and reported on in *The New York Times*², it is clear that we cannot wait any longer to secure our critical electrical infrastructure against cyber terrorism.

The Mandiant report definitively identifies a large group of hackers with significant resources based in the Pudong New Area in Shanghai, China and convincingly connects this group to the Chinese military. Dubbed the "Advanced Persistent Threat 1" (APT1), this group is identified by the report as Unit 61398 of the People's Liberation Army. Mandiant has observed almost 2,000 attacks on 141 companies across 20 industries from 2006 to the present, with the vast majority of these attacks targeting U.S. companies and government agencies. These attacks are only the ones observed by Mandiant for its clients, so likely represent only the tip of the iceberg in terms of the extent of APT1-launched cyber attacks in the U.S. Furthermore, APT1 is just the most prolific of 20 similar groups based in China that Mandiant has tracked the activity of.

It is troubling to note that the energy sector was the sixth most common target of APT1. The Mandiant report reveals that APT1 was responsible for the security breach at Telvent Canada (now Schneider Electric) that was reported late last year³. Telvent provides supervisory control and data acquisition (SCADA) systems to the operators of power grids and oil and gas pipelines that allow them to remotely control valves and switches in their infrastructure. While these SCADA systems can improve operations and reduce costs, they also expose critical controls to the possibility of hacking. APT1 apparently stole the project files for a premier offering, OASyS SCADA, providing APT1 with the blueprints for the software that controls

¹ <http://intelreport.mandiant.com/>

² http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=1&_r=1

³ <http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/>

critical U.S. power infrastructure. In addition, Telvent maintained direct access to clients' SCADA systems for support and troubleshooting purposes. While Telvent indicates that it closed such access before APT1 was able to gain access to any systems outside their own, this incident indicates that APT1 was barely a keystroke away from being able to trigger a true cyber disaster.

Secretary of Defense Leon Panetta has identified a "cyber-attack perpetrated by nation states or extremist groups" as capable of being "as destructive as the terrorist attack on 9/11."⁴ Many of the protections that are necessary to secure our critical infrastructure are known, but because of a regulatory vacuum they are not widely implemented. For example, the North American Electric Reliability Corporation has suggested strategies to prevent attacks using Stuxnet and other specific malware tools, but these are voluntary measures and have not been widely adopted by the industry. All five commissioners of the Federal Energy Regulatory Commission (FERC) spoke clearly when they told me in a Sept. 2011 hearing that the threat of cyber attack on the electrical infrastructure was at the top of their list of risks to contend with and that they needed new authority for FERC to rapidly issue rules that addressed emerging cyber vulnerabilities to properly secure our grid⁵.

In the 111th Congress, we worked together in a bipartisan effort to pass the GRID Act (H.R. 5026; 111th Congress) in the House. This bill gave the Federal Energy Regulatory Commission the authority to issue rules and orders to protect critical electrical infrastructure. It was approved 47-0 in the Energy and Commerce Committee and passed the House by voice vote in June 2010. As you said when we introduced the bill, "the security of our Nation's energy infrastructure from attack is one of the most important issues that this Congress might address this year, and it's not an issue that we can take lightly."⁶ I agree completely. I stand ready to work with you to take immediate action on this critical problem.

Sincerely,



Edward J. Markey

⁴ <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>

⁵ http://democrats.energycommerce.house.gov/sites/default/files/image_uploads/091411%20EP%20The%20American%20Energy%20Initiative%2012%20-%20Impacts%20of%20the%20Environmental%20Protection%20Agency%27s%20New%20and%20Proposed%20Power%20Sector%20Regulations%20on%20Electric%20Reliability.pdf

⁶ <http://thomas.loc.gov/cgi-bin/query/F?r111:1:./temp/~r111AIHM4v:e18290:>