Dear Chelan PUD Commissioners:

After presenting a large volume of information to the Chelan City Council, we received a considerable amount of concern about how easily Smart Meters can be hacked.

It was suggested to us that the commissioners be informed.

Thank you for reviewing this information.

Smart Meter Awareness Group in Chelan County

Senator Patrick Colbeck, R-Canton, testified on March 7, 2017, before the House Energy and Technology Committee in support of House Bill 4220, legislation that would restore consumer protections regarding the type of meters that are installed upon their personal property. https://www.youtube.com/watch?v=xMnLZiMMfGI&sns=em

The "Cindy" he referred to in his testimony is the following person: Cynthia Ayers.

Expert Testimony on Smart Meters/Grid: "Retain analog systems to the extent possible."

Posted on March 12, 2017 by SkyVision Solutions

by K.T. Weaver, SkyVision Solutions

Cynthia Ayers is a national security threat analyst, currently working as an independent consultant within the Mission Control and Cyber Division of the Center for Strategic Leadership, U.S. Army War College. She is also serving as Deputy to the Executive Director of the Congressionally sponsored Task Force on National and Homeland Security.

On March 7, 2017, Ayers presented testimony before the Michigan House Committee on Energy Policy. Her testimony included an analysis of how smart meters introduce safety and security threats to the electric grid and to civilization itself. Excerpts from the written testimony [1] include the following:

"My testimony will concentrate on the possibility of a catastrophic cyber attack to the systems we depend on for the delivery of electricity – the lifeblood of our modern civilization. …

As our electric grid becomes 'smarter' and more networked, it also becomes more vulnerable, making it a very inviting – perhaps *the most* inviting – target for adversaries. Threats specific to smart grid technology range from the tactical (e.g., house-to-house, building to building) to the national strategic level. As with cyber activities world-wide, operational attacks against small, inconspicuous elements (**smart meters**, for example) could ultimately have a much larger, truly catastrophic impact to the grid and to the society it sustains.

Although security can always be improved, all networks, all systems – virtually anything computerized – can be hacked. As systems become more highly networked, it becomes

easier for attackers to locate 'backdoors'. Multiple 'smart' appliances and other home or business devices are being developed and sold on the market, with the assumption that IoT (Internet of Things) networking and metering will soon be (if not already) commonly available.

Demand for full optimization of **smart meters** will ultimately rule out limited, billing-only usage (e.g., Meter to Cash or M2C). The number of gaps in security will multiply per person, per household; and a successful ingress of any 'backdoor' could have detrimental effects on neighbors, communities, regions, states, the nation and beyond (e.g. Canada and Mexico). Passive cyber defenses will be of prime importance, yet ubiquitous usage of components will only serve to increase gaps in security, regardless of the options given to consumers.

Smart meters can provide digital backdoors to facilities (e.g. the home, office, building, etc.) via the items within (e.g. televisions, refrigerators, thermostats, etc.). They can also allow access to multiple components of external electric infrastructure. Therefore, the use of **smart meters** must be carefully evaluated in the context of threats to personal safety as well as the safety of the grid. …

Another physical aspect of **smart meters** was raised by a Fire Chief Duane Roddy during your hearing of February 21, 2017. In a discussion of electrical arching [*sic*] and a fire that began only 36 hours after installation of a **smart meter** in his own home, the Chief stated that there is no surge protection associated with the new meters (older meters do have surge protection).

It should be noted that massive surges (with much greater effects than weather related or other types of flow interruptions) are associated with severe space weather (geomagnetic storms caused by coronal mass ejections from the sun) and electromagnetic pulse (EMP) associated with high-altitude nuclear explosions – both of which have been known to cause arching [*sic*] and fires.

Hackers are also figuring out how to cause surges, using **smart meters** to access air conditioning systems. 'If an attacker were to turn the air conditioners on and off repeatedly, [they] could create disturbances and imbalances in the grid that could trip breakers beyond the neighborhood they're targeting and cause an even more widespread blackout.' [5] …

Recommendations:
"Use an 'all-hazards' approach for grid mitigation. **Retain analog systems to the extent possible.** …"

The purpose of the hearings being conducted by the Michigan House Committee on Energy Policy is to discuss the proposed provisions of HB 4220 [2] which would primarily allow customers to retain traditional usage meters without incurring monthly fees as long as those customers agree to self-report their usage back to the utility; otherwise, there would be a fee not to exceed $5.00 per month.

Based upon the above testimony, the actual discussions that need to be conducted are for proposing and/or requiring that ***everyone*** needs to retain their analog meters so as

to avoid possible catastrophic consequences in the future, … because as also stated in the Cynthia Ayers testimony:

"Worst case does happen. … Consider the possibility that in one decisive action, critical vulnerabilities existing within our electric infrastructure could be exploited so successfully ***that the first and last battle in the next war occur simultaneously***. …

Due to the manner in which cyber attacks are propagated, cybersecurity is everyone's business. It is ultimately up to individuals and the companies who employ them, to do what is necessary to meet this looming crisis. Leaders, in both the public and private spheres, must provide an environment conducive to national security. The destruction of our critical infrastructure is not simply a 'worst case scenario' that will never happen. It is a 'weapon of choice' that will ensure victory to the attacker."

I will certainly do my part to "retain analog systems to the extent possible" in order to protect myself, my family, my property, and civilization itself. What about you? What about our elected representatives? Will they do their part?

References

[1] Expert Testimony of Cynthia E. Ayers, before the Michigan House Energy Policy Committee, "The Cyber/Smart Grid Tech Threat to the Integrated North American Critical Electric Infrastructure," March 7, 2017; available at https://skyvisionsolutions.files.wordpress.com/2017/03/ayers-testimony-for-mi-house-committee-7-march-2017.pdf

[2] Michigan House Bill 4220 on allowing consumer choice of a traditional or advanced utility meter (introduced February 15, 2017); available at https://skyvisionsolutions.files.wordpress.com/2017/03/proposed-mi-2017-hb-4220.pdf; also refer to a fiscal analysis at: http://web.archive.org/web/20170312182849/http://www.legislature.mi.gov/documents/2017-2018/billanalysis/House/htm/2017-HLA-4220-7D61C897.htm