

ORIGINAL

Antonio Gill

Generic Smart Meter Investigation E-00000C-11-0328



0000136478

From: Warren Woodward [w634578]
Sent: Tuesday, May 08, 2012 8:54
To: Pierce-Web; Newman-Web; E
Cc: paboud@azleg.gov; salen@...
Subject: Hacking Expert David Chalk Joins Urgent Call to Halt Smart Grid

Re: AZ Corp. Comm. Docket # E-00000C-11-0328

Commissioners,

Did you see this (below) from The Wall Street Journal's Market Watch?

The evidence continues to mount. In the interest of public safety it should be recognized and admitted that these radio meters are a colossal mistake which should be abandoned at once.

Warren Woodward
Sedona, AZ

Arizona Corporation Commission DOCKETED

http://www.marketwatch.com/story/hacking-expert-david-chalk-joins-urgent-call-to-halt-smart-grid-2012-04-12

DOCKETED BY [Signature]

April 12, 2012, 10:26 a.m. EDT

Hacking Expert David Chalk Joins Urgent Call to Halt Smart Grid

"100% certainty of catastrophic failure of energy grid within 3 years"



VANCOUVER, British Columbia, Apr 12, 2012 (BUSINESS WIRE) -- The vulnerability of the energy industry's new wireless smart grid will inevitably lead to lights out for everyone, according to leading cyber expert David Chalk.

Back Your Power' (www.ThePowerFilm.org), Chalk says the entire power grid will be at risk to being taken down by cyber attack, and if installations continue it's only a matter of time.

"We're in a state of crisis," said Chalk. "The front door is open and there is no lock to be had. There is not a power meter or device on the grid that is protected from hacking - if not already infected - with some sort of trojan horse that can cause the grid to be shut down or completely annihilated."

"One of the most amazing things that has happened to mankind in the last 100 years is the Internet. It's given us possibility beyond our wildest imagination. But we also know the vulnerabilities that exist inside of it. And then we have the backbone, the power grid that powers our nations. Those two are coming together. And it's the smart meter on your home or business that's now allowing that connectivity."

Chalk also issued a challenge to governments, media and technology producers to show him one piece of digital technology that is hack-proof.

"The computer companies that are involved, the manufacturers that are involved, bring forward a technology and I will show you that it's penetrable," said Chalk. "I'll do it on national TV, I'll do it anywhere. But I can guarantee you 100% that there is nothing out there today -- nothing -- that can't be penetrated."

Chalk's strong words come amidst increasing reports of the smart grid's fatal insecurities, even from the governments and energy companies who are forcing their hand with the smart program. "Every endpoint [meter] is a new potential threat vector," according to Doug Powell, manager, SMI Security, Privacy & Safety, for Canadian utility BC Hydro.

And in an interview with EnergyNow.com, former CIA Director James Woolsey was also highly critical of energy policy makers, whose plans received multi-billion dollar funding as part of the Economic Stimulus Act of 2008. "The so-called 'smart grid' that is as vulnerable as what we've got now is not smart at all," said Woolsey. "It's a really, really stupid grid."

But there's more. In an audit released in January, the US Inspector General Gregory Friedman was also highly critical. "Without a formal risk assessment and associated mitigation strategy, threats and weaknesses may go unidentified and expose the ... systems to an unacceptable level of risk," Friedman wrote.

Energy officials knew of these weaknesses but approved plans for the projects anyway, auditors said. "The initial weaknesses had not always been fully addressed, and did not include a number of security practices commonly recommended for federal government and industry systems."

And security is not the only technologically-based obstacle faced by smart grid proponents. In March, alarm bells were rung following current CIA Director David Patraeus' confirmation that governments will use wireless smart appliances to spy on citizens. "Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters," Patraeus said at a meeting of In-Q-Tel, the CIA's venture capital firm. He added that this will prompt a rethink of "our notions of identity and secrecy."

With strong criticism to the smart grid now coming from many directions, energy corporations and governments now have the challenge to explain to an increasingly unapproving public why they

continue to fast-track smart grid installations.

Citizen groups and organizations throughout the US, Canada and Europe have launched legal actions to stop the installation of smart meters. They cite issues such as cost increases, health risks, privacy concerns, grid vulnerability and the lack of democratic process. In Chalk's home province of British Columbia, Citizens for Safe Technology (www.citizensforsafetechnology.org) and the BC Coalition to Stop Smart Meters are leading a growing challenge.

Options for opting out of the smart metering program have been announced in markets including California, Maine, Vermont, Louisiana, Michigan, Connecticut, Quebec, the UK and the Netherlands. In the US, several regions including the counties of Santa Cruz and Marin are enforcing outright moratoriums.

“Unless we wake up and realize what we're doing, there is 100% certainty of total catastrophic failure of the entire power infrastructure within 3 years,” said Chalk. “This could actually be worse than a nuclear war, because it would happen everywhere. How governments and utilities are blindly merging the power grid with the Internet, and effectively without any protection, is insanity at its finest.”

The full video interview with David Chalk can be seen on www.thepowerfilm.org . The feature film documentary 'Take Back Your Power', which critically examines the smart grid program, will be released online this spring.