DIVISION OF RATEPAYER ADVOCATES

DATA REQUEST

Pacific Gas and Electric Company
Advanced Metering Infrastructure – Bakersfield Issues

Date: April 28, 2010

Due Date: May 10, 2010

To:	Redacted Rate Department Sidney Bob Dietz II, Regulatory Relations Pacific Gas and Electric Company 77 Beale Street, San Francisco, CA 94105	E-mail: Redacted SBD4@pge.com

From:	Chris Danforth Division of Ratepayer Advocates 505 Van Ness Avenue, Room 4102 San Francisco, CA 94102	Phone: (415) 703-1481 E-mail: CTD@cpuc.ca.gov

Data Request No: DRA-011

Originated by: Karin Hieta   **Phone:** (415) 703-4253

Subject: Smart Meter Security Issues

Please provide the following information as it becomes available but no later than **May 10, 2010.** If you are unable to provide the information by this date, please provide a written explanation to me by **May 1, 2010** as to why the response date cannot be met and your best estimate of when the information can be provided. If you have any questions regarding this data request, please call me at the above phone number.

Attached is an article discussing the ability of hackers to tamper with smart meters. Please refer to the article in Attachment A.

Regarding the AMI meters PG&E is currently installing:

1. Have the meters been tested for security vulnerabilities?

    a. If not, does PG&E plan to have them tested? If PG&E plans to have them tested, please provide the schedule for the testing to occur.

    b. If yes, please provide the results.

2. Please provide any strategies or plans PG&E has developed to address meter security.

3. Is the data on PG&E's AMI meters encrypted?

   a. If not, how is the data secured?

   b. If yes, please describe the location and security of the digital keys needed to unlock the encrypted data.

4. Please provide any strategies or plans PG&E has developed to address data security.

5. Please provide a description of how data from the AMI meters is transmitted back to PG&E.

END

Associated Press - **'Smart' meters have security holes**

Flaws could allow hackers to tamper with power grid, reserachers say

By <u>Jordan Robertson,</u> March 26

SAN FRANCISCO - Computer-security researchers say new "smart" meters that are designed to help deliver electricity more efficiently also have flaws that could let hackers tamper with the power grid in previously impossible ways.

At the very least, the vulnerabilities open the door for attackers to jack up strangers' power bills. These flaws also could get hackers a key step closer to exploiting one of the most dangerous capabilities of the new technology, which is the ability to remotely turn someone else's power on and off.

The attacks could be pulled off by stealing meters — which can be situated outside of a home — and reprogramming them. Or an attacker could sit near a home or business and wirelessly hack the meter from a laptop, according to Joshua Wright, a senior security analyst with InGuardians Inc. The firm was hired by three utilities to study their smart meters' resistance to attack.

These utilities, which he would not name, have already done small deployments of smart meters and plan to roll the technology out to hundreds of thousands of power customers, Wright told The Associated Press.

There is no evidence the security flaws have been exploited, although Wright said a utility could have been hacked without knowing it. InGuardians said it is working with the utilities to fix the problems.

New meters being rolled out

Power companies are aggressively rolling out the new meters. In the U.S. alone, more than 8 million smart meters have been deployed by electric utilities and nearly 60 million should be in place by 2020, according to a list of publicly announced projects kept by The Edison Foundation, an organization focused on the electric industry.

Unlike traditional electric meters that merely record power use — and then must be read in person once a month by a meter reader — smart meters measure consumption in real time. By being networked to computers in electric utilities, the new meters can signal people or their appliances to take certain actions, such as reducing power usage when electricity prices spike.

But the very interactivity that makes smart meters so attractive also makes them vulnerable to hackers, because each meter essentially is a computer connected to a vast network.

Computer worm hop

There are few public studies on the meters' resistance to attack, in part because the technology is new. However, last summer, Mike Davis, a researcher from IOActive Inc., showed how a computer worm could hop between meters in a power grid with smart meters, giving criminals control over those meters.

Alan Paller, director of research for the SANS Institute, a security research and training organization that was not involved in Wright's work with InGuardians, said it proved that hacking smart meters is a serious concern.

"We weren't sure it was possible," Paller said. "He actually verified it's possible ... If the Department of Energy is going to make sure the meters are safe, then Josh's work is really important."

SANS has invited Wright to present his research Tuesday at a conference it is sponsoring on the security of utilities and other "critical infrastructure."

Industry representatives say utilities are doing rigorous security testing that will make new power grids more secure than the patchwork system we have now, which is already under hacking attacks from adversaries believed to be working overseas.

"We know that automation will bring new vulnerabilities, and our task — which we tackle on a daily basis — is making sure the system is secure," said Ed Legge, spokesman for Edison Electric Institute, a trade organization for shareholder-owned electric companies.

More testing needed, some say

But many security researchers say the technology is being deployed without enough security probing.

Wright said his firm found "egregious" errors, such as flaws in the meters and the technologies that utilities use to manage data from meters. "Even though these protocols were designed recently, they exhibit security failures we've known about for the past 10 years," Wright said.

He said InGuardians found vulnerabilities in products from all five of the meter makers the firm studied. He would not disclose those manufacturers.

One of the most alarming findings involved a weakness in a communications standard used by the new meters to talk to utilities' computers.

Wright found that hackers could exploit the weakness to break into meters remotely, which would be a key step for shutting down someone's power. Or someone could impersonate meters to the power company, to inflate victims' bills or lower his own. A criminal could even sneak into the utilities' computer networks to steal data or stage bigger attacks on the grid.

Key storage

Wright said similar vulnerabilities used to be common in wireless Internet networking equipment, but have vanished with an emphasis on better security.

For instance, the meters encrypt their data — scrambling the information to hide it from outsiders. But the digital "keys" needed to unlock the encryption were stored on data-routing equipment known as access points that many meters relay data to.

Stealing the keys lets an attacker eavesdrop on all communication between meters and that access point, so the keys instead should be kept on computers deep inside the utilities' networks, where they would be safer.

"That lesson seems to be lost on these meter vendors," he said. That speaks to the "relative immaturity" of the meter technology, Wright added.