The Washington Post

'Smart Grid' Raises Security Concerns

By Brian Krebs
Washington Post Staff Writer
Tuesday, July 28, 2009

Electric utilities receiving "smart grid" grants must ensure cybersecurity.
(By David Zalubowski -- Associated Press)

Electric utilities vying for $3.9 billion in new federal "smart grid" grants will need to prove that they are taking steps to prevent cyberattacks as they move to link nearly all elements of the U.S. power grid to the public Internet.

The requirements from the Energy Department come amid mounting concern from security experts that many existing smart-grid efforts do not have sufficient built-in protections against computer hacking, such as new "smart meters" that put information about consumers' power use onto the Internet, grid-management software and other equipment.

The smart-grid spending in the federal stimulus package is intended to create jobs and improve the efficiency and reliability of the electricity grid by lowering peak demand, reducing energy consumption, integrating more renewable energy sources and easing the pressure to build new coal-fired power plants.

Many of those efficiency gains will be made possible by new technology being built on top of the existing power grid, such as smart meters, which provide real-time feedback on power consumption patterns and levels. An estimated 8 million smart meters are used in the United States today, and more than 50 million more could be installed in at least two

dozen states over the next five years, according to the Edison Foundation's Institute for Electric Efficiency.

Yet security researchers have found that these devices often are the weakest link in the smart-grid chain. Smart meters give consumers direct access to information about their power usage and the ability to manage that usage over the Web, but that two-way communication also opens up the possibility that the grid could be attacked from the outside. Many such systems require little authentication to carry out key functions, such as disconnecting customers from the power grid.

Indeed, at this week's Black Hat, the world's largest cybersecurity conference held annually in Las Vegas, researchers from IOActive of Seattle are slated to demonstrate a computer worm that spreads by taking advantage of the software update feature built into a prevalent brand of smart meters (IOActive is not disclosing which). The worm could in theory give the attackers who launched it the ability to very quickly sever tens of thousands of homes from the smart grid.

Joshua J. Pennell, IOActive president and chief executive, said he hopes the presentation will serve as a wake-up call for smart-grid technology vendors and the companies purchasing the products.

Federal grants for smaller smart-grid projects range from $300,000 to $20 million, while the federal share of funds for larger projects could be as much as $200 million. The Energy Department says it can reject any grant application that does not demonstrate that ensuring cybersecurity will be a top priority.

"We haven't described how to address the requirements, because we're trying to leave the door to innovation open," said Hank Kenchington, a senior manager with the Energy Department's Office of Electric Delivery and Energy Reliability. "But we do say -- even if an award scored 'A' grades on all aspects but doesn't address cyber -- we reserve right to not go forward with that grant. We realize you need to ask for the security up front and have it built-in up front, or you're going to end up paying for it later."