

CYBEREYE—Commentary

## Government seizes opportunity to build security into new critical infrastructure

- By [William Jackson](#)
- Mar 30, 2009



Development of a new generation of intelligent power grids for energy distribution is a high priority for President Barack Obama's administration, and \$4.5 billion has been included in the economic stimulus package for the Energy Department to pursue this goal.

It makes good sense. A Smart Grid that can monitor where power is being distributed and how it is used could help the environment, as well as the economy, by improving the efficiency of an aging infrastructure that has been in place for decades. This is the network equivalent of installing traffic cameras on highways and at intersections to better understand and control traffic.

And what also makes sense is that [security](#) is not being ignored in this rush to develop new technology. Part of the \$4.5 billion in stimulus money will be going to the National Institute of Standards and Technology to fund creation of guidelines and standards for securing what will be a new critical infrastructure.

The Smart Grid would have two-way communications so that managers can monitor activities and control performance down to the individual customer level. One of the first pieces of this infrastructure to be deployed are smart meters that not only can report power usage to utilities for billing but also provide information on energy demand and patterns of use that can be analyzed to provide more economical service. They also can be used to remotely shut off service to a customer. The same kind of controls also could be applied to any point in the distribution system.

In the end, the Smart Grid is a large Supervisory Control and Data Acquisition (SCADA) network with all the vulnerabilities of SCADA networks, said Curt Barker, NIST's chief cybersecurity adviser.

"No brand new vulnerabilities," Barker said. "What is a little different is the scale of the system," and the potentially catastrophic results of exploiting those vulnerabilities.

The saving grace of SCADA networks controlling vital systems so far is that they have usually been developed as silo systems with little interconnections and often with proprietary technology. This does not make them invulnerable, but it makes them harder to attack on a large scale, providing a low return on investment for hackers and attackers.

This is beginning to change, as users move to benefit from the economies of standardized, interoperable, Internet-based systems. The Smart Grid presumably would be built from scratch as a standards-based, interoperable IP network. Sort of like a new Internet. And we know how secure the Internet is.


But we have a chance now to learn from the mistakes of the past and design this new network with security in mind from the beginning. NIST has been given the job of developing the guidelines for this and the Federal Energy Regulatory Commission will have the power to mandate them as standards for the industry.

NIST has demonstrated under the Federal Information Security Management Act its ability to develop comprehensive standards and specifications for IT security. It has demonstrated under Homeland Security Presidential Directive 12 its ability to do this quickly by developing technical standards for the Personal Identity Verification card. NIST's job with the Smart Grid will not be as big as its job under FISMA. A lot of workable standards already exist: NIST's job will be to identify and harmonize them and fill in the gaps. And it will not be as rushed as it was under HSPD-12.

Standards alone cannot protect a network and there is no reason to believe the Smart Grid will be invulnerable. But we can hope that it will be an intelligent, flexible network with a minimized attack surface that can be easily defended.


#### About the Author

William Jackson is a senior writer for GCN.



To help you achieve your mission.  
Technology for better business outcomes

HP ProLiant BL495c G5 server with the  
AMD Optron™ Processor



© 1996-2009 1105 Media, Inc. All Rights Reserved.