October 29, 2010

Office of Electricity Delivery and Energy Reliability
US Department of Energy
Room 8H033
1000 Independence Avenue, SW
Washington, DC 20585

Re: Comments on "*Smart Grid RFI: Addressing Policy and Logistical Challenges*"
75 FR 57006 [FR Doc. 2010-23251]

From: Steve Dauber
Vice-President, Marketing
RedSeal Systems
2121 South El Camino Real, Suite 300
San Mateo, CA 94403
Ph: 650-645-6209
sdauber@redseal.net
www.redseal.net

RedSeal Systems is a leading developer of security posture management software for large organizations and has provided their software to several major utilities for complex network security applications. RedSeal software - in use by more than 150 industry and government organizations (www.redseal.net/customers) - enables those organizations to continuously, comprehensively and automatically assess and strengthen their cyber-defenses before they are attacked. In addition to in-depth understanding of overall security posture, RedSeal delivers continuous compliance with regulations such as NERC CIP, PCI, FISMA, and SOX, and actionable steps for risk remediation.

RedSeal's core technology is the ability to understand the access control of the network as a whole - not simply the behavior of a single device. RedSeal analyzes the interactions of firewalls, routers and load balancers network wide to determine the traffic allowed between every two points. It compares actual access against network policies to automatically pinpoint inadvertent exposure and correlates access with host vulnerabilities to pinpoint sources of excessive risk. RedSeal's technology is protected by seven patents granted and pending.

RedSeal was founded in 2004 and has received $42 million in funding from blue chip venture capitalists. RedSeal is based in San Mateo, California.

RFI Topics Addressed

Reliability and Cyber Security

- What smart grid technologies are or will become available to help reduce the electric system's susceptibility to service disruptions?

- What is the role of federal, state, and local governments in assuring smart grid technologies are optimized, implemented, and maintained in a manner that ensures cyber security? How should the Federal and State entities coordinate with one another as well as with the private and nonprofit sector to fulfill this objective?

Comment

> *Cyber security for energy control systems has emerged as one of the Nation's most serious grid modernization and infrastructure protection issues…With so many vital services and critical infrastructures interconnected with energy systems, a large-scale cyber attack could disrupt power and cause cascading failures, affecting the economy and public safety of large communities…Smart Grid technologies present new cyber security challenges for utilities, end users, and the Nation as a whole.*[1]

The NERC CIP standards were put in place to protect the critical assets of the grid and the systems that support those assets. They are extensive, and with the force of law from FERC, are backed by audits that can be enforced with fines. However, audits are only a spot check, and **passing an audit does not mean the entire system is in compliance. Further, audits occur at a single point in time and can not verify that the system remains in compliance after the audit concludes. Continuous monitoring and near real-time risk management is the only way to assure that the system remains secure on an ongoing basis.**

Control systems that govern electric generation, transmission and distribution are increasingly networked, are often built on older operating systems, and have high availability requirements. Because of this, it is difficult to patch vulnerabilities that can be exploited by hackers, so control systems must be treated like a "boy in the bubble" and have access restricted by network security (firewalls, etc.). Unfortunately, the architecture, rulesets and policies of this network security can be complex and changes to these rulesets are frequent.[2] Any errors in network security can expose control systems to attack by cyber adversaries. This challenge is exacerbated by the deployment of smart grid technologies that will significantly increase the number and availability of digital access points for hackers to cause harm through smart meters, automated control equipment and the networks connecting them, further complicating the network security architecture.

While the smart grid will incorporate sophisticated network security controls, complexity and change in this infrastructure make it unlikely that the controls can be effectively implemented without strong assurance mechanisms. The federal government's Joint Task Force Transformation Initiative (JTFTI) Interagency Working Group (from NIST, DoD, ODNI and other agencies) has crafted a risk management framework for complex critical IT systems which forms the basis for the newly updated Federal Information

[1] DOE Office of Chief Financial Officer, *FY11 Congressional Budget Request*, Vol 3, Febr 2010, p 542.
[2] Department of Commerce, National Institute of Standards and Technology (NIST), *Guide to Industrial Control Systems (ICS) Security*, Special Publication 800-82, September 2008.

Security Management Act (FISMA) regulations. Its revised guidance document[3] recommends continuous monitoring, with automated support tools that facilitate near real-time risk management, for highly dynamic environments.

The US can (and must) be a global leader in developing continuous monitoring and near real-time risk management software for smart grid network security. The role of DOE should be to provide financial and technical support for the research, development and deployment of such technologies, including a requirement that the 116 Smart Grid Investment Grant (SGIG) and Demonstration Program award winners address continuous monitoring and near real-time risk management of their grids; 20% of the SGIG merit review criterion was having a technical approach to interoperability and cyber security.

Technical Discussion

Many organizations use a combination of an annual assessment and incremental change management as their assurance mechanism for controls. While seemingly reasonable, this approach leaves organizations vulnerable to errors and omissions that are easily overlooked by even the most diligent manual reviews. In the updated framework, NIST cautions against this approach:

> "*Planning and implementing security configurations and then managing and controlling change is not a guarantee that information systems will remain configured as expected. Using automated tools, organizations can identify when the information system is not in compliance with security policy and standards and take remediation actions as necessary. Continuous monitoring identifies undiscovered system components, mis-configurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk.*"[4]

Without automated systems to provide continuous monitoring of network security controls, they are not likely to be effective. Network security is architected using many individual devices arrayed in defense-in-depth architectures. These protect control systems in multiple subnets from multiple threat sources (internet connections, meter connections…). Individual network security devices, such as firewalls, often contain thousands of individual rules. Determining what access is blocked or allowed between every two points in the network is a complex calculation that requires identifying all potential network paths and calculating the cumulative effect of all of the devices along that path. This is a computationally exponential problem (n^2 order of magnitude).

RedSeal has developed proprietary heuristics that allow these calculations to be performed in a matter of hours for even very complex networks, enabling the analysis to

[3] Department of Commerce, NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53 Revision 3, May 2010, Supplemental Guidance, page F-37.
[4] NIST Risk Management Framework, *Monitor Step FAQs*, April 30 2009, page 12.

be done on a daily basis. With government and industry contributions, the RedSeal technology will be able to incorporate capabilities for the smart grid that support the continuous monitoring tasks detailed in NIST 800-37 Appendix E[5], including assessing the security impact of changes, ongoing network security control assessments, identifying remediation actions, determining risk, and outputting reports that detail security status to executive management.

[5] Department of Commerce, NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Special Publication 800-37 Revision 1, February 2010, pages E4-E5.