ReedSmith

Client Alert

Global Regulatory Enforcement

FERC Issues Order to Investigate Possible Violations of its Cyber Security Protocols for the Electric Grid

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Amy S. Koch
Partner, Washington, D.C.
+1 202 414 9223
akoch@reedsmith.com

Amy Mushahwar
Senior Associate,
Washington, D.C.
+1 202 414 9295
amushahwar@reedsmith.com

Christine E. Nielsen
Associate, Washington, D.C.
+1 312 207 6459
cnielsen@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

The Federal Energy Regulatory Commission (FERC) issued an order July 20, 2012, to investigate whether any Authorized Certification Authorities (ACAs) had violated the North American Energy Standards Board (NAESB) Public Key Infrastructure (PKI) Standards, which outline various security requirements and specifications for the electric grid.[1]

In Order No. 676-C, FERC incorporated by reference certain standards adopted from NAESB's standards relating to digital certificates and public key infrastructure, which apply to any public utility that operates facilities used for the transmission of electric energy; any public utility that sells electric energy at wholesale prices; and some non-public utilities as well.

The NAESB authorizes Certification Authorities (CAs) to become ACAs, who can then issue digital certificates to the industry. These digital certificates verify credentials and allow their holders to enter the electric grid's cyber business systems. The electric grid powers many aspects of Americans' lives, from utility companies to hospitals to homes.

The Senate Homeland Security and Governmental Affairs Committee recently received allegations that two (of the four total) ACAs had been issuing digital certificates with a 30-year lifespan, which is 10 years greater than allowed under FERC regulations. On May 31, the NAESB held a conference discussion about the current PKI expiration-length standards, which attempt to balance the cyber security needs of the grid with the amount of disruption imposed on businesses. ACAs fell on both sides of the debate, with some advocating for terms as little as five or 10 years, and some pushing for as much as 30 years.

On July 17, 2012, Sen. Joseph Lieberman (I-Conn.) sent a letter to FERC, expressing concern over this allegation and requesting that FERC perform an immediate, comprehensive investigation and provide the results (and any future steps that FERC might take) to the Senate Homeland Security and Governmental Affairs Committee, of which he is the chairman. The concern is that a longer certificate lifespan could mean that the entity with a "valid" certificate has outdated security procedures and may therefore be more susceptible to attack. According to his letter, Sen. Lieberman fears that a compromised certificate may provide an attacker with "'a skeleton key' to circumvent security measures and access a wide variety of systems on the electric grid." These fears could prove to be quite accurate, considering that the United States, using the computer virus Stuxnet, successfully infiltrated Iran's nuclear facilities with valid digital certificates.

FERC's July 20 Order requires all ACAs (and CAs seeking to acquire NAESB certification) to submit a report by July 27 on "the facts and practices surrounding the NAESB PKI standards." Specifically, FERC wants to know the processes and procedures each ACA uses to validate the identity of individuals requesting digital certificates, and the key lifetimes used for various certificates. These reports will allow FERC to determine the effectiveness of the current system, and whether any changes should be made to increase the cyber security protocols for entrance to the electric grid.

As we discussed in our last blog article, the cyber security of the electric grid is a hot topic in Congress, sparking various bills in both houses. Late last week, Sen. Lieberman submitted a revised edition of his bill, The Cybersecurity Act of 2012, which he hopes will gain the bipartisan support needed to pass before the August recess. On July 25, Senate Majority Leader Harry Reid (D-Nev.) invoked cloture to schedule a floor vote on the Cybersecurity Act prior to the Senate's August recess, which will determine whether the Act will eventually be negotiated in a Conference Committee with members of the House of Representatives, and could ultimately lead to a passed bill out of both of the Houses. Any new cyber security legislation that Congress passes could have a profound effect on the way the electric grid and other public-private critical infrastructure is secured.

---

1. Reporting on North American Energy Standards Board Public Key Infrastructure Standards, 140 FERC ¶ (2012).