140 FERC ¶ 61,149
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Jon Wellinghoff, Chairman;
Philip D. Moeller, John R. Norris,
Cheryl A. LaFleur, and Tony T. Clark.

Reporting On North American Energy Standards Board Public Key Infrastructure Standards — Docket No. EL12-86-000

REPORT ON USE OF NORTH AMERICAN ENERGY STANDARDS BOARD PUBLIC KEY INFRASTRUCTURE STANDARDS

(Issued August 27, 2012)

1. On July 20, 2012, the Commission issued an order directing all Certification Authorities who have acquired or are seeking to acquire North American Energy Standards Board (NAESB) certification pursuant to the NAESB standard on Public Key Infrastructure (PKI)[1] to report on the use of PKI by utilities. The Commission took this action due to allegations of improper use of the NAESB PKI standards.[2] The Commission received responses from four companies. Based on the information received, further action by the Commission does not appear necessary at this time. However, as explained below, the NAESB PKI standards are aimed at facilitating the security of commercial transactions, and are separate from the obligation of affected utilities under section 215 of the Federal Power Act (FPA) to take steps to ensure the cybersecurity of the bulk-power system. As discussed further below, we remind utilities of their primary role and responsibility in ensuring the security of critical cyber assets, and of the need to frequently reassess their cybersecurity protections to confirm their sufficiency.

[1] *Standards for Business Practices and Communication Protocols for Public Utilities*, Order No. 676-C, FERC Stats. & Regs. ¶ 31,274, *order on clarification and reh'g*, Order No. 676-D, 124 FERC ¶ 61,317 (2008).

[2] *Reporting On North American Energy Standards Board Public Key Infrastructure Standards*, 140 FERC ¶ 61,066 (2012) (*Reporting Order*).

Background

2. On July 21, 2008, in Order No. 676-C, the Commission incorporated by reference into Part 38 of its regulations certain standards adopted by the Wholesale Electric Quadrant (WEQ) of NAESB including a standard on PKI. A "key," or string of characters, is used as an input to a cryptographic function in order to make the information being transmitted electronically more difficult to access by an unintended recipient. PKI deals with managing a large number of public keys within a cryptographic system.[3] As originally incorporated by reference in Order No. 676-C, the NAESB PKI Standards describe: (1) the requirements an Authorized Certification Authority must meet in order to issue certificates that are compliant with the NAESB PKI Standards; and (2) the minimum physical characteristics that a certificate must meet in order to achieve compliance with the NAESB PKI Standards. In Order No. 676-D, the Commission found that while public utilities are not required to use the NAESB PKI Standards to conduct business transactions over the Internet, if they do contract with an Authorized Certification Authority, they must comply with the NAESB PKI Standards. Thus, while the Commission required utilities to incorporate the NAESB PKI Standards into their tariffs, there was no requirement that public utilities operate under or utilize the PKI Standards.

3. PKI is one approach to addressing key management. Rather than public keys being shared between individual users, a Certification Authority is created to act as a clearinghouse for "key" exchange, verifying a user and its access to the system, and linking that identity to its public key. This Certification Authority will create a certificate that other members of the system can use to verify one another when they communicate. A Certificate Authority must first establish a root key pair and a root certificate, which is used by the Certificate Authority to digitally sign certificates. A server certificate, which is installed on a web server, is used by web sites to prove their identity and to secure and encrypt data. A client certificate, which is located on the end user's computer, is then used to verify an end user's identity.

4. This security feature is based on each user trusting the Certification Authority to properly verify the individual or entity using the system. The use of a certificate establishes a user's identity and assures a party that it is communicating with the entities with whom it wishes to do business. Such transactions are common in commercial applications and can be evidenced in various on-line transactions by the use of commercial companies such as VeriSign or the designation of "https" in an Internet browser to designate that a connection is secure.

[3] A "public" key is uniquely associated with a single entity and may be made public. This "public" key is mathematically linked with a corresponding "private" (confidential) key and is used to verify the entity's digital signature.

5. According to Order No. 676-C, NAESB adopted its PKI standards (WEQ-012) to create greater security for business transactions taking place over the Internet. Pursuant to the Commission's regulations, WEQ-012 applies to "any public utility that owns, operates, or controls facilities used for the transmission of electric energy in interstate commerce or for the sale of electric energy at wholesale in interstate commerce and to any non-public utility that seeks voluntary compliance with jurisdictional transmission tariff reciprocity conditions."[4] Also, the PKI standards state that "end entities that wish to use the public key infrastructure established by these standards must attest to their understanding of and compliance with their Authorized Certification Authority's Certificate Policy or Certification Practice Statements, and agree to be bound to electronic transactions entered into by the end entity using a valid Certificate issued in the name of the end entity."[5]

Commission Order Requiring Reporting

6. The Commission's *Reporting Order* was issued to determine the nature of any current practices under these standards and whether the Commission should propose or recommend any changes in applicable law. Allegations had been raised that Certification Authorities are issuing certificates that are not compliant with the NAESB PKI standards. Specifically, it had been suggested that entities are issuing certificates without NAESB authorization, without adequate identity authentication, or for too long a duration. If true, these allegations would affect how these standards may be implemented by public utilities. Thus, the Commission instituted this proceeding pursuant to section 307(a) of the FPA to investigate the facts and practices surrounding Certification Authorities' implementation of the NAESB PKI standards.

7. The Commission required all Certification Authorities who had acquired or were seeking to acquire NAESB certification to submit a report containing the following information:

a. Are you authorized by NAESB as an Authorized Certification Authority, or have you claimed such status previously? If so, please provide all documents demonstrating the authorization.

b. Are you issuing certificates to electric utilities or to others to use in communicating with electric utilities? If so, please identify all such entities and the dates of certificate issuance.

[4] 18 C.F.R. § 38.1 (2012).

[5] NAESB WEQ v002.1: 012 Introduction.

c. It has been suggested that there is a concern with how entities are validating and certifying the identity of individuals requesting or requiring PKI certificates. Please explain the process and procedures that your organization follows when you validate the identity of an individual who requests/requires a PKI certificate, and provide all documents describing your process and procedures.

d. What key lifetimes do you adhere to for the various certificates that you create and administer?

Responses

8. The Commission received responses from four companies: Shift Systems, LLC (Shift), Systrends USA,[6] Open Access Technology International, Inc. (OATI), and GMO GlobalSign Inc. (GlobalSign). Also, the Commission notes that on July 20, 2012, NAESB issued information regarding its PKI standards.[7] In that issuance, NAESB states that all Certificate Authorities applications are currently in a pending status. According to NAESB, the pending status is related to the fact that it is currently in the process of revising its PKI standards.

9. The responses from the companies also generally pointed to the fact that NAESB is currently revising its PKI standards and has not certified any Certification Authorities. GlobalSign and OATI state that they are listed as pending approval as Authorized Certificate Authorities by NAESB. Shift states that it is the first company to be identified by NAESB as an Authorized Certification Authority.

10. GlobalSign, OATI, and Shift each described the process by which they verify the identities of individuals and organizations for certificate requests. OATI and Shift each specifically state that they comply with the provisions in WEQ-012. In describing its process, GlobalSign cites to provisions of the NAESB PKI standards.

11. In addition, the responses discussed the key lifetimes for the different types of certificates. According to OATI, the root certificate is the underlying backbone within a Certification Authority for the trust and signing of digital certificates. The current NAESB PKI standards allow for a key pair to have a maximum lifetime not to exceed 20 years. OATI asserts that the selection of a specific period of time for this validity

[6] Systrends USA states that it entered into a partnership with GlobalSign to issue digital certificates under GlobalSign authority and has thus issued no certificates.

[7] NAESB WEQ Board of Directors, *Re: Information on Cyber-Security Standards* (July 2012), *available at* http://www.naesb.org/weq/weq_bod.asp.

period balances the level of security with the impact on customers and systems associated with changes in key pairs. The root certificate expires at the end of its validity period. A Certification Authority can also retire a root certificate key pair at any time prior to the end of the root certificate's validity period. OATI and GlobalSign both state that their root certificates are valid for 20 years, as allowed under the NAESB standards. Shift states that its root keys and certificates have a lifetime validity of no longer than ten years. With respect to end entity certificates, Shift states that its subscriber certificates have a lifetime validity of no longer than one year, GlobalSign's end entity certificates are valid for one or two years, and OATI states that its end entity certificates are valid for two years.

12. However, Shift states that it has not issued certificates to electric utilities because it "cannot attest to the security of the public key infrastructure and cannot participate in the public key infrastructure as relying parties because the public key infrastructure is compromised."[8] Shift also asserts that it has discussed with "certain Certification Authorities" that "notwithstanding their public statements otherwise, these Certificate Authorities are issuing certificates that are not compliant with the mandatory WEQ-012 requirements (among other things, they are wholly and cryptographically dependent upon noncompliant root certificates and key pairs), refuse to remediate their noncompliance, and exhibit a general disregard for relevant regulatory requirements, thus undermining any potential attestation by Shift as a relying party."

Discussion

13. First, it is important to understand the Commission's authority with respect to the NAESB PKI standards. NAESB is a voluntary organization focused on commercial business practices. The NAESB PKI standards are incorporated into our regulations under sections 205 and 206 of the FPA, our ratemaking authority with respect to sales for resale and transmission of electricity in interstate commerce, instead of our authority under FPA section 215 to approve and enforce standards (including cybersecurity standards) developed by the Electric Reliability Organization (ERO) to protect the reliability of the bulk-power system. Neither NAESB nor the Certification Authorities are public utilities subject to our ratemaking authority. Therefore, the Commission does not have jurisdiction over NAESB or the Certification Authorities with respect to the allegations before us. The Commission can only enforce those provisions in the NAESB PKI standards that apply to public utilities if a public utility chooses to contract with an Authorized Certification Authority. Moreover, according to NAESB, the PKI standards that apply to Authorized Certification Authorities are not yet enforceable because NAESB has not yet approved any such authorities pending further revisions to WEQ-012. And finally, the Commission does not have the authority to modify the standards

[8] Shift at 2.

developed under NAESB process or author or modify standards developed under the ERO processes but instead, can only choose to either adopt or approve, or decline to adopt or remand (in the case of standards developed by the ERO process), the final result in its entirety.

14. The NAESB PKI standards identify the key lifetimes for certificates. According to the current NASEB PKI standards:

> [Certification Authority] key pairs are retired from service at the end of their respective maximum lifetimes as defined in the [Certification Authority's Certification Practice Statement] but not to exceed 20 years. [Certificate Authority] Certificates may be renewed as long as the cumulative certified lifetime of the [Certification Authority] key pair does not exceed 20 years. [Certification Authorities] must ensure that key changeover procedures are followed and that those procedures provide a smooth transition to a new [Certification Authority] key pair. The [Certification Authority] key changeover process must allow an overlap period to ensure that service is not interrupted and must provide at least 60 days notice to all certificate holders.[[9]]

15. The Commission instituted this proceeding to investigate the facts and practices surrounding Certification Authorities' implementation of the NAESB PKI standards. The Commission was investigating allegations that Certification Authorities are issuing certificates that are not compliant with the NAESB PKI standards. Specifically, it had been suggested that entities are issuing certificates without NAESB authorization, without adequate identity authentication, or for too long a duration. The *Reporting Order* was issued to determine the nature of any current practices under the NAESB standards and whether the Commission should propose or recommend any changes in applicable law.

16. While Shift raises concerns in its filing, the information received in this proceeding does not provide specific evidence to support the allegations. Thus, we do not believe any further Commission action is warranted on the record here. With regard to the allegation that the 20-year lifetime of the root keys and certificates is too long, the Commission is concerned that this time period may present an unacceptable risk of

---

[9] NAESB WEQ v002.1: 012-1.19.7 Key Changeover (RFC 3647 Section 5.6). By contrast, NAESB WEQ v002.1: 012-1.23.5 provides that "[c]ertificates to individual or role Subscribers shall have a validity period not to exceed two years. Certificates issued to devices or applications shall have a usage period not to exceed three years."

compromise and therefore recommends that NAESB consider this issue through updates in its standards in an expeditious manner. Such long life spans increase the likelihood of a user's keys or certificates being compromised.

17. As noted above, the Commission has authority over electric reliability under section 215 of the FPA. A reliability standard adopted under that provision can include protection against a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system. The Commission has approved eight cybersecurity (CIP) standards. Requirement R2.4 of Reliability Standard CIP-005-3a requires that "[w]here external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party…." The Commission reminds utilities of the importance of maintaining the security of critical cyber assets[10] and of taking into account new information in ensuring they have strong controls at the access points to critical cyber assets. While the Commission seeks to use its authority and resources to aid utilities in their efforts to secure the grid and to ensure utilities' compliance with their obligations under the CIP standards, the responsibility for cyber security protection rests first and foremost with the utilities themselves.

18. While the Commission is monitoring the development and enforcement of CIP standards under section 215, we note that the statute leaves a gap with respect to ensuring the security of the bulk-power system against fast-moving cybersecurity threats. The current authority of the Commission under section 215 to approve or remand reliability standards developed by the ERO, and to enforce compliance with those standards, is not adequate to address imminent cyber or other national security threats to the reliability of our transmission and power system. These types of threats pose an increasing risk to our Nation's electric grid, which undergirds our government and economy and helps ensure the health and welfare of our citizens. The standards development process envisioned by Congress in section 215 and implemented by the Commission is unlikely to be able to address an imminent, fast-moving cybersecurity threat in sufficient time to ensure that bulk-power system reliability is not compromised. Our report today does not advocate for or against new specific cybersecurity legislation, nor do we advocate that the Commission or any particular agency should be given authority to address imminent cybersecurity threats. These are choices for Congress. However, absent new legislation to address the issue, it is clear that the responsibility for any imminent actions to protect

[10] The Commission also notes that data can be a critical cyber asset. *See Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, at PP 259-273 (2008).

the grid remains primarily with the utilities themselves. We will support their efforts to the full extent of our authority, including requiring and approving new standards when appropriate.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.