CYBER SECURITY:

DATA CONFIDENTIALITY ISSUES

AND PROPOSED LEGISLATION

MAY 8, 2009

Robert S. Lynch
ROBERT S. LYNCH & ASSOCIATES
340 E. Palm Lane, Suite 140
Phoenix, Arizona 85004-4603
(602) 254-5908
(602) 257-9542 facsimile
e-mail: rslynch@rslynchaty.com

Responding to the direction of Congress in Section 215 of the Energy Policy Act of 2005,[1] the Federal Energy Regulatory Commission (FERC) has approved 83 reliability criteria.[2] An additional 8 criteria have been approved specifically related to cyber security.[3] FERC has approved the North American Electric Reliability Corporation (NERC) to be the electric reliability organization (ERO) and it in turn has delegated enforcement responsibility to the regional reliability organizations.[4] NERC, in turn, has proposed rules for it and Regional Entities acquiring information from Registered Entities.[5]

This structure presents some unique problems for the public bodies that operate electric utility systems and public power utilities. It also presents some problems for the federal agencies that deal with this system as well.

The reliability criteria program contains requirements that are intended to protect critical infrastructure information and separate requirements that are aimed specifically at cyber security information. The Energy Policy Act of 2005 authorizes FERC to delegate the management and enforcement of these criteria to a non-governmental organization denominated an ERO. To no one's surprise, the existing national industry reliability organization (NERC) applied for and was selected to perform that function. Regional reliability organizations, again industry formed non-governmental organizations, were then delegated these roles. These NGO's, dominated by private utility companies, do not have to comply with the Freedom of Information Act (FOIA) or with state public records laws. The 2005 Act did not address these issues.

In the private sector, confidentiality is generally protected by bilateral agreements. That business model found its way into NERC consideration

---

[1] 16 U.S.C. § 824o.

[2] FERC Order No. 693, FERC Stats. & Regs. ¶ 31,242 (2007); Order No. 693-A, rehearing denied, 120 FERC ¶ 61,053 (2007).

[3] FERC Order No. 706, 73 Fed.Reg. 7367, et seq. (February 7, 2008), 122 FERC ¶ 61,040 (2008); Order No. 706-A, denying rehearing and granting clarification, 123 FERC ¶ 61,174 (May 16, 2008).

[4] Order No. 672, 71 Fed.Reg. 8662 (February 17, 2006), FERC Stats. & Regs. ¶ 31,204 (2006); Order on rehearing, Order No. 672-A, 71 Fed.Reg. 19814 (April 18, 2006), FERC Stats. & Regs. ¶ 31,212 (2006); NAERC ERO Certification Order, 116 FERC ¶ 61,062, order on rehearing and compliance, 117 FERC ¶ 61,126 (2006).

[5] See: Order Conditionally Approving Amended Rules of Procedure, 122 FERC ¶ 61,142 (February 21, 2008). This effort is currently on hold because of the problems identified in this paper.

and its Legal Advisory Committee[6] established a Task Force to develop a standard form confidentiality agreement. That agreement model is intended to provide the necessary structure for protecting that portion of the flow of information to implement the reliability criteria that requires confidentiality. That agreement model is still a work in progress and discussing it has brought to the table the problems we in the public sector have in protecting the confidentiality of such information.

Our confidentiality problems lie in two general categories; the impact of the Freedom of Information Act on federal agencies, and the impact of state public records laws on public entities operating in the electric utility industry.

In the design of the FERC reliability criteria, information is intended to flow both upstream and downstream. The key problems with the Freedom of Information Act (FOIA)[7] are (1) whether the information held by a federal agency is exempt from required disclosure, and (2) the concern that, by communicating reliability information to a non-governmental organization, the federal agency will waive any protections inherent in FOIA for information otherwise deemed confidential. The flip side of (2) is whether critical infrastructure information provided to a federal agency from NERC and/or a regional entity, both NGO's, protected in the first instance as confidential under FOIA. These are the questions that the federal agencies, most especially the power marketing administrations and the generating agencies, must find answers for. Research is being led by the Bonneville Power Administration which cannot share the results of its work at this time because of the fear of waiving its confidentiality.

The second problem relates to the family of laws generally known as state public records laws. Post-9/11, a number of states began looking at various ways to protect information, including information about the electric power systems in their states. As you might imagine, fifty plus efforts or dialogues on this subject were not designed to create uniformity.[8] Public

---

[6] A committee of attorneys of NERC stakeholders chartered to provide a discussion forum, develop advice to NERC's General Counsel, identify emerging legal issues and provide common solutions to benefit NERC stakeholders. Its formation was approved by the NERC Board on May 22, 2007.

[7] 5 U.S.C. § 552.

[8] At least one effort is underway to track post-9/11 changes to state public records laws. University of Florida College of Journalism and Communications, Marion Brechner Citizen Access Project, found at: http://www.citizenaccess.org. Given the federal moving target, tracking state responses may be a never-ending task.

bodies' records are generally public. Exceptions have to be crafted legislatively. So a state agency or a political subdivision generally must manage its recordkeeping within the public records framework. It can deny access to its records only when authorized to do so by legislation. The states, to the extent any of them have considered this subject, have done so in at least a partial vacuum because the federal response to 9/11 was not uniform nor focused until passage of the Energy Policy Act in 2005. Even so, the federal response, as it relates to the electric utility industry, is still being put in place.[9] Thus, the opportunity for a consistent and uniform state by state response is effectively nonexistent.

Entities subject to state public records laws have similar problems to the ones federal agencies have with FOIA, i.e., whether some communication will constitute a waiver and whether restriction of access to the information is authorized at all in the first instance. There is some argument that general confidentiality provisions in some public records laws could cover information flowing to and from the federal reliability criteria network. Outcomes in this circumstance would largely depend on the specific wording of each state's public records laws and the interpretation of those laws by the respective state judiciaries. This is not a prescription for uniformity nor comprehensive treatment. In the first instance, one has to be concerned about whether the subject matter of any protective statute at the state level would be broad enough to cover those things intended in the federal system to be protected as confidential. Since we are early in the game of attempting to define and administer a federal confidentiality program, defining the breadth of what is necessary to be treated as confidential is an ongoing exercise. The tensions that fights over requests for information bring to such a program have not really yet developed. Nor has the judicial guidance these fights produce.

The second aspect of protecting information at the state level is related to process. If someone requests information of a public body and is denied access, what remedy does that person have and how is it administered? Is it totally then a judicial branch process? Are there some tasks delegated to the executive branch in a particular state prior to the judiciary getting involved? Are there constitutional issues in some states

[9] Just recently, FERC has sought to expend the reach of Rule 706 to cover nuclear facilities not regulated by the Nuclear Regulatory Commission. Order on Proposed Clarification, 124 FERC ¶ 61,247 (September 18, 2008), 73 Fed.Reg. 55459-60 (September 25, 2008). Comments originally due October 20, 2008 are now due by November 3, 2008

where providing information to a non-governmental organization, even under the aegis of federal regulation, reaches beyond the state's ability to legislate confidentiality?

As these questions foretell, the response this dialogue leads one toward is a federal response, an Act of Congress. There is a model to consider. There is a provision in the 2002 Homeland Security Act which, at first blush, looks like it takes care of the problem.[10]

On closer inspection, this language does leave holes in the umbrella. The provision deals only with information submitted to the Department of Homeland Security (DHS), submitted voluntarily, and not to information in possession of others not communicated to/from DHS[11]. Moreover, the involvement of non-governmental entities that are not "local governments" raises issues about just how far a provision like this could be used to protect critical information and cyber security information, if it were applied to the electric utility industry. Homeland Security has issued regulations to implement this provision,[12] but the "permission" mechanism central to protecting NGO information remains untested.

It is an open question whether and to what extent the limited regulatory umbrella that Homeland Security has been given will stand the test of time. Nevertheless, as a model, the Homeland Security statute and its accompanying regulation point out the need to be comprehensive and inclusive in fashioning a statute for the electric utility industry. We need one that would provide the uniformity and comprehensiveness that protection of truly critical infrastructure information including cyber security information would require in order to be effective. This does not require inventing a new approach. It only requires some thoughtful editing of the Homeland Security concept. The attached modification to the Senate legislative proposal is one way of approaching the problem.

---

[10] Known as the Critical Infrastructure Information Act of 2002, it is Subtitle B of Title II of Public Law 107-296, 116 Stat. 2135 (November 25, 2002). The operative statute, Section 214, is codified at 6 U.S.C. § 133.

[11] County of Santa Clara v. Superior Court, 170 Cal.App. 4th 1301, 89 Cal.Rptr. 3d 374 (February 5, 2009).

[12] 6 C.F.R. Part 29, 72 Fed.Reg. 65420, et seq. (November 20, 2007).