2011 APPA Legal Seminar

PROTECTING CRITICAL ENERGY INFRASTRUCTURE INFORMATION: A STATE ACTION APPROACH

NOVEMBER 7, 2011

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

Protecting Critical Energy Infrastructure Information: A State Action Approach

Ever since 9/11, people have been worried about critical infrastructure information of various types and energy providers have been concerned about such information related to their systems and supplies. Congress early on tried to do something about it but the effort was less than complete. It involved only information being provided to a single federal agency, the new Department of Homeland Security (DHS), and only information voluntarily provided.[1] Although DHS issued regulations[2], the limited application of this provision has been recently exposed.[3]

Obviously, information about infrastructure is communicated more broadly than that. As it affects our industry, communications come to us from the Federal Energy Regulatory Commission ("FERC" or the "Commission"), the North American Electric Reliability Corporation ("NERC") or the Regional Entities. For those of us who live in areas serviced by power marketing administrations ("PMA's"), we have the opportunity for dialogue with them as they do with FERC, NERC and the appropriate Regional Entity. Indeed, communications about infrastructure can come to or be sent to any one of these entities by us and we can receive information from any and all of these sources.

Protecting the portion of that information that needs protecting should be relatively simple. Between private entities, confidentiality agreements are being and can be utilized. If litigation is involved or anticipated, common defense agreements can also be effective.

However, in the ordinary course of business when federal agencies are involved, the Freedom of Information Act ("FOIA") comes into play.[4] It provides some protection for confidential information[5] but that confidentiality can be waived. That waiver may be triggered by sharing the information with a non-federal entity, either a private corporation or a public entity.[6] The problems that emanate from FOIA are beyond the scope of this paper but are so acute that PMA's have expressed considerable concern about the use of confidentiality agreements and other communications under the existing status of federal law.

For our purposes, our problems emanate from provisions of our states' and other governmental organizations' public records laws and regulations. FERC, NERC and the Regional Entities seem to assume that somehow information they send to us or information we send to them can be kept confidential because that is the way they want it. There really isn't any serious effort yet to come to grips with the issue about whether and to what extent individual state and local public records rules interfere with keeping designated information confidential.

---

[1] Section 214 of the Critical Infrastructure Information Act of 2002, 6 U.S.C. § 133, originating in Subtitle B of Title II of Public Law 107-296, 116 Stat. 2135 (November 25, 2002).

[2] 6 C.F.R., Part 29, 72 Fed.Reg. 65420, et seq. (November 20, 2007).

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

[4] 5 U.S.C. § 552.

[5] 5 U.S.C. § 552(b)(1)-(9). See: *National Association of Homebuilders v. Norton*, 309 F.3d, 26 (C.A.D.C. 2002).

[6] *Maydale v. U.S. Dept. of Justice*, 362 F.Supp. 2d 316 (D.D.C. 2005), reconsideration denied, 579 F.Supp. 2d 105; *County of San Miguel v. Kempthorne*, 587 F.Supp. 2d 64 (D.D.C. 2008).

Congress has taken a couple of shots at this. Language has kicked around in both the House and the Senate over the last several Congresses but nothing has happened.

The General Accounting Office (GAO) has also recently gotten into the debate on the key subject of cybersecurity.[7] Its report highlights the lack of mechanisms to protect confidentiality[8], acknowledges that public power exists[9], and should be included in future coordination of efforts by FERC and others[10], but doesn't address the protection of information under FOIA or state public records laws.

While these developments were unfolding, the American Public Power Association ("APPA") has enlisted several attorneys, including myself, to work with NERC and its Legal Advisory Committee on confidentiality agreement forms. We needed these forms to recognize the problem that public power entities have if public records requests are given to them for this type of information. We have been relatively successful in getting agreement with our private sector counterparts on exculpatory language and getting understanding from NERC about the need for such language in any agreement that a public power entity might sign.

That is certainly an improvement from a couple of years ago when neither NERC nor attorneys representing private utilities had the appreciation they now have for the problems we face in dealing with public records laws. In any event, signing an agreement that says you may have to give up the information anyway doesn't solve the problem. It doesn't look like Congress is going to successfully come to grips with this problem any time soon either. Just last month House Republicans published a cybersecurity task force report that at least acknowledges that protection of information is a problem[11], but that is a long way from a solution.

Hence the idea for a model state law that would allow the states and their political subdivisions to protect information from state public records law requests even if Congress won't. The draft bill that accompanies this paper is intended to do just that. Because of the wide variation in state public records provisions, it is written to be freestanding and self-contained as to definitions.

What follows now is a brief explanation for the provisions in this model.

Finding. In Arizona at least, this finding would be necessary in order to overcome the ability of charter cities to make their own law on a particular subject. It is included for the purpose of ensuring that such types of independent authorities can be overridden to provide a uniform provision.

Definitions. The critical infrastructure and critical energy infrastructure information definitions are taken from existing federal definitions in order to form a uniform base by which to determine the breadth of subject matter covered. It doesn't mean that these definitions are not too limiting

---

[7] Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed. GAO Report No. 11-117 (January 2011).

[8] GAO-11-117, p.14 and n.17.

[9] GAO-11-117, p.20.

[10] GAO-11-117, p.27.

[11] Recommendations of the House Republican Cybersecurity Task Force, October 2011, pp.10-11.

or might be expanded in an individual state setting. It does mean that they form a floor because these definitions are utilized every time federal legislation is proposed on this subject and will continue to be utilized in that fashion.

The definition of local government is intended to cover everything we could think of. If we have missed something, let us know.

Protection. The protection provisions should be self-explanatory. The exception for investigation or prosecution is taken from an earlier version of proposed federal law that I wrote. It was included there and is included here because of suggestions from congressional staff and others that this sort of exception would be not only useful but necessary.

Non-Waiver. Likewise the non-waiver provision resulted from dialogue with staff and representatives and attorneys around the country who suggested that trade secret and other matters would be of particular sensitivity.

Intent. Finally, the intent provision is directed expressly at lines of cases that say that a restriction on divulging public records should be narrowly construed when the policy of the state is to promote access to public records. In this instance, the presumption should work the other way.

This proposal is not intended to be the conclusion of this effort but rather the beginning. I have drafted for APPA provisions to provide protection both from public records laws and FOIA that are longer and more complicated than this and one or two that are even shorter. When you get into the federal realm, there are some other considerations not addressed here. However, if Congress is unable to deal effectively with this subject, the only way we can protect our clients is to suggest to our legislatures that it is up to them. In doing so, collective dialogue and ideas are most often more helpful than efforts to go it alone. Hence the proliferation of ListServe subjects that APPA has generated and that many of us use almost daily.

This is a work-in-progress. I need to go to our legislature in January with something, this or some other version of the subject. I would appreciate your help. I would appreciate knowing whether and to what extent any of you might likewise be so inclined to approach your legislatures with this subject.

I look forward to hearing from you.

PROPOSED MODEL STATE
CEII LEGISLATION

RSL
11-7-2011

Section 1: Findings: The legislature finds that the protection of critical energy infrastructure information is a matter of statewide importance and concern and a necessary modification to state policy and statutory requirements concerning the availability of public records.

Section 2: Protection of Critical Energy Infrastructure Information

a. Definitions

1) "Critical Infrastructure" has the meaning given that term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).

2) The term "Critical Energy Infrastructure Information" has the meaning given that term in 18 C.F.R. Section 388.113(c)(1).[12]

3) For purposes of this Act, the term "Local Government" means any county, parish, city, town, special district or other political subdivision of this State including joint powers or joint action agencies and State educational institutions.

b. Protection

1) In General. - - Notwithstanding any other provision of law, critical energy infrastructure information including cyber security information that is in the possession of or submitted to or provided by the State, a State agency, commission or other instrumentality or a local government of this State –

[12] FERC Order 683, 71 Fed.Reg. 58273 (October 3, 2006), FERC Stats. & Regs. ¶ 31,228 (2006).

a) Shall be exempt from inspection, copying or other disclosure requirements of any State or local government law or regulation requiring disclosure of information or records; and

b) Shall not be made available during or as a result of any judicial or quasi-judicial process except in furtherance of an investigation or the prosecution of a violation of federal law or a criminal act under State law.

2) Non-Waiver. - - The provision of critical energy infrastructure information to the State, a State agency, commission or other instrumentality or a local government of this State shall not constitute the waiver of any applicable privilege or protection against disclosure provided under law to such information, such as trade secret protection.

Section 3: Intent.—It is the intent of the legislature in enacting these protections against disclosure of critical energy infrastructure information that the provisions hereof be liberally interpreted in any judicial or quasi-judicial proceeding in favor of protection of information subject of this Act.