2019 APPA Legal & Regulatory Conference

PROTECTING CYBERSECURITY STRATEGIES AND PROGRAMS: CLOSING THE GAP BETWEEN EXISTING LAWS AND FOIA; A LEGISLATIVE PROPOSAL

OCTOBER 22, 2019

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 Cybersecurity Strategies and Programs:
Closing the Gap Between Existing Laws and FOIA;
A Legislative Proposal

Robert S. Lynch
Robert S. Lynch & Associates

After the attack on the World Trade Center on September 11, 2001, Congress defined[1] and several federal agencies have since dealt in various ways with the Congressionally-defined term "Critical Infrastructure" ("CI").[2] Then, in 2002, as part of the Homeland Security Act ("HSA")[3], Congress passed the Critical Infrastructure Information Act of 2002.[4] That law is intended to protect Critical Infrastructure Information ("CII") but only such information "voluntarily" submitted to this new agency and approved as such by it.[5] The American Public Power Association ("APPA") early on focused on CII, the limits in its Congressional definition, its emergence as a ubiquitous definition, and its application to the power industry as Critical Energy Infrastructure Information ("CEII"), as well as other early post-9/11 developments.[6]

Fast forward four (4) years and Congress sought to focus attention on the subject in the Energy Policy Act of 2005, which generated multiple responses from the Federal Energy Regulatory Commission ("FERC") but still left the electric utility industry, especially public power, with an incomplete program of protection under the Freedom of Information Act ("FOIA"), both for CEII and the emerging new subject of CyberSecurity Information ("CSI").[7]

Lack of further action by Congress prompted interest in developing a model state law that would at least give those of us who represent them a leg up in protecting both CEII and CSI in the hands of our public power clients.[8] This interest also included the same problems with the emerging use of smart meters[9], albeit without finding any solution.[10]

Meanwhile, the Supreme Court of the United States ("Court") was throwing everyone a curve. Agencies had been using Exemption 2 of FOIA (documents "related solely to the internal

---

1 Critical Infrastructure Protection Act of 2001, § 1016, H.R. 3162, 115 Stat. 272 at 400-402, October 26, 2001.
2 *Id.*, § 1016(E), 115 Stat. 401.
3 Homeland Security Act, Pub. L. 107-296, 116 Stat. 2135 (November 25, 2002).
4 116 Stat. 2150-5, codified at 6 U.S.C. ¶¶ 101 note, 131-4, now 6 U.S.C. ¶¶ 671-4.
5 6 U.S.C. ¶ 133, now ¶ 673.
6 For example, Security and Privacy of Critical Infrastructure Information Under Federal, State and Local Law, 2003 APPA Legal Seminar, October 27, 2003, currently available at www.rslynch-az.com.
7 CyberSecurity: Data Confidentiality Issues and Proposed Legislation, May 8, 2009, currently available at www.rslynch-az.com.
8 Protecting Critical Energy Infrastructure Information: A State Action Approach, 2011 APPA Legal Seminar, November 7, 2011, currently available at www.rslynch-az.com.
9 Regulating the "Smart" in Smart Meters, 2011 APPA Legal Seminar, November 7, 2011, currently available at www.rslynch-az.com.
10 I can report to you with confidence that neither Congress nor the Arizona Legislature rushed to address the issues outlined in these papers.

personnel rules and practices of an agency")[11] for decades to withhold critical infrastructure records. However, in *Milner v. Department of Navy*[12], the Court cashiered use of that FOIA exemption, leaving everyone guessing whether any FOIA exemption could protect CII and CEII.

Congress again took up the subject in 2013, but did not finish the job.[13] Meanwhile, the model state law crashed and burned in the Arizona Legislature, but the Legislature did pass what many consider a more draconian measure in the same session.[14]

While this was going on, a non-profit group, Public Employees for Environmental Responsibility ("PEER"), was suing the International Boundary and Water Commission ("IBWC") for records related to structural deficiencies of and emergency action plans for the Amistad and Falcon Dams on the Rio Grande River bordering Mexico, managed by IBWC.[15] Initially, IBWC sought shelter for some of these records under Exemption 2. After *Milner*, IBWC sought to invoke Exemptions 5 (deliberative process privilege) and 7(E) and 7(F) – records collected for law enforcement purposes.[16] In an opinion written by then-Judge Brett Kavanaugh, the Court of Appeals remanded the Exemption 5 issue because a potentially dispositive issue was unresolved[17] and upheld the use of the shield in Exemption 7(E) for shielding emergency action plans and upheld the use of Exemption 7(F) for shielding potential dam failure inundation maps.[18] In doing so, the Court leaned heavily on Justice Samuel Alito's concurrence in *Milner*.

The concerns after the *PEER* decision were two-fold. On the one hand, the "watch-dog" community, if you will, sounded the alarm bells over the drastic expansion of Exemption 7.[19] In the electric utility community, the concerns leaned the other way. The remand centered on whether the consultant report on dam safety issues was "intra-agency" because it was sought as part of the agency's deliberative process, the so-called "consultant corollary".[20] How much CII and CEII could pass muster under that test? And how much CII and CEII can equate to dam failure emergency action plans?

Then came 2015 and a Congressional awakening engrafted onto the Fixing America's Surface Transportation ("FAST") Act.[21]

---

11 5 U.S.C. 552(b)(2).

12 562 U.S. 562, 569 (2011).

13 Critical Infrastructure Information: Threat of Disclosure Under Open Records Requirements & FOIA Requests – Federal Legislation and Regulation; Arizona Response, 2013 APPA Legal Seminar, October 21, 2013, currently available at www.rslynch-az.com.

14 *Ibid*.

15 *Public Employees for Environmental Responsibility v. United States Section, International Boundary and Water Commission, U.S. -Mexico*, 408 U.S. App. D.C. 61, 740 F.3d 195 (2014).

16 In his concurring opinion in *Milner*, Justice Alito had suggested that Exemption 7 might provide some protection for critical infrastructure records. *Milner v. Department of Navy*, *supra*, 562 U.S. at 581-585.

17 *PEER v. IBWC*, *supra*, n. 16, 408 U.S. App. D.C. at 69, 740 F.3d at 199.

18 *Id*., 408 U.S. App. D.C. at 72, 740 F.3d at 206. See also *Living Rivers, Inc. v. United States Bureau of Reclamation*, 272 F. Supp. 2d 1313 (D. Utah 2003).

19 Society of Environmental Journalists press release dated February 19, 2014.

20 *Id*., note 18, 408 U.S. App. D.C. at 67-8, 740 F.3d at 201-2.

21 Fixing America's Surface Transportation (FAST) Act, H.R. 22, § 61003, P.L. 114-94, signed 12/04/2015.

Section 61003 of the FAST Act amended the Federal Power Act ("FPA") by adding § 215A entitled "Critical Electric Infrastructure Security".[22] In addition to a lengthy provision for definitions (Subsection (a)), the statute provides for protection of CEII from FOIA (thus invoking FOIA Exemption 3)[23], overrides state and local public records laws as to CEII, orders FERC to establish regulations to designate information as CEII, limits such designation to five (5) years subject to renewal or removal of the designation, establishes the Department of Energy ("DOE") and FERC authority to designate and provides other implementing direction.[24] FERC then set about establishing the regulations as it was directed.[25]

Thus, Congress had established the same "submit, designate, protect" scheme as in the HSA but notably didn't include the "voluntary" parameter found in the 2002 legislation. So, for an electric utility to protect what it believes it has in its possession that qualifies as CEII, the utility must submit that information to FERC or the Secretary. FERC has created a form for that exercise, filing guidelines and instructions for that purpose.[26]

At this point, one might think that we (public power utilities) are home free. Our only risk is that we may possess CEII that we haven't sent to FERC or DOE for labelling. Unfortunately, that may not be true. Section 215A of the Federal Power Act as enacted by § 61003 of the FAST Act defines "critical electric infrastructure" and "critical electric infrastructure information", CEI and CEII, using the same limited language found in the USA Patriot Act[27] and the HSA.[28] What's missing? Cybersecurity protection protocols, software, guidance, directives, etc. While the 2005 Energy Policy Act mentions cybersecurity, it is in the context of standard setting, not protection. Nor does § 215A mention cybersecurity although the term had been in the lexicon for at least a decade courtesy of the 2005 Act when the 2015 law was enacted. Even if we would like to read these protection strategies into the existing definition, the Supreme Court has articulated a tenet of statutory construction that makes a relaxed reading of statutes, especially FOIA, unlikely. On June 24, 2019, the Court issued its opinion in *Food Marketing Institute v. Argus Leader Media dba Argus Leader*.[29] While this case involved FOIA Exemption 4 (commercial or financial information obtained from a person and privileged or confidential), it is the principles of statutory construction that the Court uses that are relevant here. The Court looked at the "ordinary, contemporary, common meaning" of words used in FOIA when enacted in 1966.[30] The Court also overruled a case where an additional requirement had been read into the language of Exemption 4.[31] In doing so, the Court said: "In statutory interpretation disputes, a court's proper starting point lies in a careful examination of the ordinary meaning and structure of the

---

22 Codified at 16 U.S.C. 824o-l.

23 5 U.S.C. 552(b)(3). Exemption 3 is an attractive shield because, to the extent successfully invoked, it means that "Congress [has] itself made the basic decision and [has] left to the administrator only the task of implementation." *American Jewish Congress v. Kreps*, 187 U.S. App. D.C. 413, 419, 574 F.2d 624, 630 (C.A.D.C. 1978).

24 Subsection (d).

25 81 Fed.Reg. 93732 (December 21, 2016), technical correction 82 Fed.Reg. 1183 (January 5, 2017).

26 FERC news release dated May 17, 2018, updated April 1, 2019.

27 Section 1016(E), 115 Stat. 401.

28 6 U.S.C. 131 transferred to 6 U.S.C. 671.

29 588 U.S. _____, 139 S.Ct. 2356.

30 Slip Op., p.5.

31 *National Parks & Conservation Assn. v. Morton*, 498 F.2d 765, 767 (C.A.D.C. 1974); Slip Op. 7.

law itself. [Citation omitted.] Where, as here, that examination yields a clear answer, judges must stop."[32]

Applying these same principles to the definition of CEII in the FPA and the HSA makes it problematic that the Supreme Court would allow us to read cybersecurity strategies, software, etc., into these definitions even if cyber "risks" (information gathering and reporting) might possibly make the cut. To use a football analogy, it is like the team's defense playbook being protected but its offense playbook being left unprotected and accessible by the opposing team.

What is the solution? For us, amending the definitions in the Patriot Act, Homeland Security Act and § 215A is the obvious choice. That way, we can clearly invoke Exemption 3 not only in response to a FOIA request but to turn aside a state or local public records request for all matters related to cybersecurity, offense and defense. Hopefully, we can also avoid a battle with the media and others that bristle at the thought of expanding Exemption 3 in any way.[33]

As if to prove my point, while I have been writing this paper I received a call from FERC on Monday, August 26, 2019 letting me know that a white paper was about to be released the next day. Then I received an e-mail the next morning giving me and a handful of other recipients a "heads up" that FERC was about to post a Joint FERC/ North American Electric Reliability Corporation ("NERC") White Paper precipitated by what FERC described as "an unprecedented number of [FOIA] requests for non-public information in the Notices of Penalties (NOPs) for violation of Critical Infrastructure Protection (CIP) reliability standards." Later that same day (August 27, 2019), FERC posted on its website and filed in Docket No. AD19-18-000 the Notice of White Paper and the Joint Staff White Paper addressing how it intends to deal in the future with FOIA requests for NOPs information. This information relates to violations of the standards mandated by the 2005 Act, including cybersecurity standards, not CEII protection in the 2015 Act. The White Paper spends eleven plus (11+) pages attempting to justify changing NOPs forms and justifying case by case determinations whether to release even the violator's name, let alone the violation and penalty, while keeping violation details non-public. FERC regulations are not proposed to be amended for this purpose.

Central to the discussion in the White Paper is an attempt to clothe NOPs with CEII protection, thus invoking Exemption 3 (viz. the FAST Act) and also invoking Exemption 7(F) (obviously taken from then-Judge, now Justice Kavanaugh's opinion in *PEER v. IBWC*). One has to ask: If the application of those exemptions, first enlarging the FAST Act language to included NOPs, and second comparing the IBWC flood inundation maps to a utility's name, are so cut and dried, why does this White Paper read like agonizing rationalization? The original comment deadline (September 26, 2019) has been extended to October 28, 2019.[34] The comments FERC and NERC receive will be instructive in themselves. I can't help but believe that they will prove the thesis of this paper.

---

32 Slip Op. 8.

33 Federal Open Government Guide 10th Edition, The Reporters Committee for Freedom of the Press (2009), p.17.

34 John McCaffrey email of September 20, 2019, 9:20 a.m.

More Recent Developments

The Senate Energy and Natural Resources Committee marked and passed S. 2095 (Gardner/Bennet) on September 25, 2019, without amendments. The bill cures some ills but doesn't cure all of them. On a positive note, it mentions cybersecurity along with physical security in ordering a Department of Energy program and report to Congress,[35] and protects information "provided to, or collected by, the Federal Government",[36] thus invoking Exemption 3. On the other hand, it only deals with information "voluntarily" submitted,[37] thus apparently excluding CEII in required reports. Moreover, it doesn't address the regulatory conundrum: FERC has regulatory authority in this arena, DOE does not. Nor does it address FERC's practice of collecting information but not designating it until requested, leaving us (except Arizona) stil hanging out.

The Government Accounting Office (GAO) has also gotten into the act, pointing out shortcomings in DOE and FERC programs and recommending an expanded DOE program without addressing any of the existing shortcomings.[38]

Additionally, on September 26, 2019, Senators Murkowski and Manchin introduced the Protecting Resources On The Electric Grid With Cybersecurity Technology Act, aka The PROTECT Act of 2019.[39] The bill orders FERC to establish incentive-based rate treatment for development of advanced cybersecurity technology[40], labels information provided to or collected by the Federal Government in this process as CEII[41], and seeks to protect ratepayers in the process.[42] Interestingly enough, the bill establishes a $50 million grant program for five (5) years aimed at:

1. Rural electric cooperatives and publicly-owned (non-FERC jurisdictional) electric utilities; and
2. Focused on entities with limited cybersecurity resources, with critical assets, or defense critical infrastructure.[43]

Like other bills that have preceded it, S. 2556 doesn't bite the definition bullet nor does it wade into the DOE/FERC quagmire.

Lurking in the background is the ongoing saga of the Notice of Penalty (NOP) controversy that is before FERC in Docket Nos. NP19-4-000, et al. There, an intervenor claims that certain NOP's had had their CEII designations expire and were discoverable under FOIA. The FERC proceeding drags on with multiple filings and interventions over the last nine (9) months.

---

35 S. 2095, pp. 2, 4.
36 Id., pp. 4, 5.
37 Id., p. 2.
38 GAO-19-332, Critical Infrastructure Protection, August 2019.
39 S. 2556.
40 Id., p. 3.
41 Id., p. 5.
42 Id., pp. 4-5.
43 Id., pp. 5-9

Included in this dispute is NERC's position, defended somewhat by a Trade Association's intervention[44], that it isn't subject to FOIA.[45]

Congress, DOE, FERC and others all seem to want to solve problems but are unwilling to recognize the tough issues in this political climate. Not being so reticent, we have a solution which may never pass but actually attempts to address the unresolved definitional issues.

What is it, you ask? Come to the Seminar and find out.

[44] Motion to Intervene in NP19-4-000, et al., dated March 28, 2019.

[45] Docket Nos. NP19-4-000, et seq.