MAY 2019
VOL. 19-5

PRATT'S ENERGY LAW REPORT

LexisNexis®

Pratt's Energy Law Report

VOLUME 19 NUMBER 5 MAY 2019

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please email:
Jacqueline M. Morris at ..... (908) 673-1528
Email: ..... jacqueline.m.morris@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:
Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call
Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

ISBN: 978-1-6328-0836-3 (print)
ISBN: 978-1-6328-0837-0 (ebook)
ISSN: 2374-3395 (print)
ISSN: 2374-3409 (online)

Cite this publication as:

[author name], [*article title*], [vol. no.] Pratt's Energy Law Report [page number] (LexisNexis A.S. Pratt);
Ian Coles, *Rare Earth Elements: Deep Sea Mining and the Law of the Sea*, 14 Pratt's Energy Law Report 4 (LexisNexis A.S. Pratt)

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(5/2019–Pub.1898)

Editor-in-Chief, Editor & Board of Editors

Hydraulic Fracturing Developments
Eric Rothenberg
Partner, O'Melveny & Myers LLP

Pratt's Energy Law Report is published 10 times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house energy counsel, government lawyers, senior business executives, and anyone interested in energy-related environmental preservation, the laws governing cutting-edge alternative energy technologies, and legal developments affecting traditional and new energy providers. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to Pratt's Energy Law Report, LexisNexis Matthew Bender, 121 Chanlon Road, North Building, New Providence, NJ 07974.

As Cyberattacks Loom, So Does Regulators' Increased Scrutiny of Utilities' Cybersecurity Systems

By Charles R. Mills, Daniel A. Mullen, Steven J. Ross, Wesley J. Heath, Shaun Boedicker, Natty Brower, and Karen Bruni*

The government has made clear that industry needs to take cyberthreats seriously and that it will not hesitate to impose further regulation and use enforcement tools if necessary. The authors of this article discuss the issue and advise utilities to go beyond compliance with mandatory standards and ensure proper systems, management involvement, training, communications, and continuous attention to reliability to prevent devastating attacks.

A major utility has agreed to pay a record-setting $10 million fine to settle allegations by the North American Electric Reliability Corporation ("NERC") for 127 cybersecurity code violations, which "collectively posed a serious risk to the security and reliability" of the bulk power system.[1] The fine is more than triple the previous record for NERC security violations, a $2.7 million penalty issued by the regulator last year. These penalties combined with recent and expected rulemakings and mounting political pressure send a clear message to utilities to get their cybersecurity systems in order or risk, in addition to the exposure to cyberthreats, heavy penalties.

NOTICE OF PENALTY

According to NERC's January 25, 2019 Notice of Penalty explaining the facts and submitting the penalty to the Federal Energy Regulatory Commission ("FERC"), many of the utility's alleged violations involved "long durations,

---

* Charles R. Mills (cmills@steptoe.com), Daniel A. Mullen (daniel.mullen@steptoe.com), and Steven J. Ross (sross@steptoe.com) are partners at Steptoe & Johnson LLP. Wesley J. Heath (wheath@steptoe.com) is of counsel and Shaun Boedicker (sboedicker@steptoe.com), Natty Brower (nbrower@steptoe.com), and Karen Bruni (kbruni@steptoe.com) are associates at the firm.

[1] NERC's January 25, 2019 Public Notice of Penalty, *available at* https://www.nerc.com/pa/comp/CE/Pages/Actions_2019/Enforcement-Actions-2019.aspx. While the identity of the utility is redacted from NERC's public filing, it was confirmed by both E&E News, https://www.eenews.net/stories/1060119265, and *The Wall Street Journal* https://www.wsj.com/articles/duke-energy-broke-rules-designed-to-keep-electric-grid-safe-11549056238, shortly after publication. FERC and NERC have since been criticized for shielding the name of the company. *See e.g.*, Motion to Intervene and Request of Public Citizen, Inc. for the Commission to Direct the Public Release of the Violator Under 18 C.F.R. § 39.7(b)(4), FERC Docket No. NP19-4 (Feb. 19, 2019).

multiple instances of noncompliance, and repeated failures to implement physical and cybersecurity protections."[2] The reliability organization found that the utility's lack of management involvement was an "aggravating factor for penalty purposes."[3] The Notice of Penalty states that "management passively accepted the [c]ompanies' prior violations by creating and allowing a culture to exist that permitted [] systemic problems to continue for over five years."[4] NERC also found that the utility's "organizational silos" created a lack of communication between management levels and across business units, which contributed to the violations.[5]

In addition to paying the $10 million fine and implementing mitigation activities, the utility committed to costly additional measures "to help ensure the effectiveness and sustainability of [its Critical Infrastructure Protection ("CIP")] compliance and security program" and "to support and assist staff in implementing a sustainable CIP compliance program."[6]

According to the Notice of Penalty, these activities include:

- Increasing senior leadership involvement and oversight;
- Creating a centralized CIP oversight department and restructuring roles within that department;
- Conducting industry surveys and benchmark discussions to help develop best practices relating to sustainable security and compliance practices;
- Continuing to develop an in-house CIP program and talent development program;
- Investing in enterprise-wide tools relating to asset and configuration management, visitor logging, access management, and configuration monitoring and vulnerability assessments;
- Adding resources to help manage and implement compliance and security efforts;
- Instituting annual compliance drills; and
- Creating three levels of training (oversight training, awareness training

---

[2] Notice of Penalty at 12.

[3] *Id.* at 53.

[4] *Id.*

[5] *Id.* at 11.

[6] *Id.*

for all staff, and performance training for staff implementing the security and compliance tasks).[7]

FERC ORDER NO. 850

NERC's Notice of Penalty comes on the heels of FERC Order No. 850 that approved new mandatory Reliability Standards to bolster supply chain risk management protections for the bulk electric system.[8] The order requires medium-sized and large power companies to construct a system to flag vendor security incidents, employee terminations and vulnerabilities in contract services, coordinate incident responses with third parties and verify software integrity. Last summer, FERC also directed NERC to revise its Reliability Standards to develop enhanced cybersecurity incident reporting requirements. The goal of these requirements, which will require the reporting of cybersecurity incidents that compromise or attempt to compromise electronic security perimeters or associated electronic access control or monitoring systems, is to "improve awareness of existing and future cybersecurity threats and potential vulnerabilities."[9] FERC gave NERC six months to prepare and file the revised Reliability Standards.

PRESSURE TO ADDRESS CYBERTHREATS

The Trump administration also has taken a number of steps to address cyberthreats, including the creation of the Department of Energy's ("DOE's") Office of Cybersecurity, Energy Security, and Emergency Response ("CESER") last year. DOE and FERC recently announced that they will co-host a technical conference on Security Investments for Energy Infrastructure to discuss security practices to protect energy infrastructure.[10]

The mounting political pressure on FERC and NERC to ramp up scrutiny of utilities' cybersecurity systems was apparent during the Senate Energy & Natural Resources Committee hearing on cybersecurity efforts in the energy

---

[7] *Id.*

[8] *Supply Chain Risk Management Reliability Standards*, 165 FERC ¶ 61,020 (Oct. 18, 2018) (Order No. 850). A recent *Wall Street Journal* report detailed the vulnerability of the electric grid to attacks via small contractors, https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112.

[9] *Cyber Security Incident Reporting Reliability Standards*, 164 FERC ¶ 61,033 at P 2 (July 19, 2018) (Order No. 848).

[10] Information on the March 28, 2019 technical conference is available at https://www.ferc.gov/EventCalendar/EventDetails.aspx?ID=13307&CalType=%20&CalendarID=116&Date=03/28/2019&View=Listview&csrt=8424261357368477389.

industry.[11] In his testimony, FERC Chairman Chatterjee noted that "while I think both industry and government have made significant strides toward addressing this issue, I believe more work still needs to be done." He emphasized that compliance with mandatory standards is not enough—the industry also needs to take advantage of voluntary initiatives. Chairman Chatterjee reiterated previously expressed concerns about the security of natural gas infrastructure and the need for robust oversight, but stopped short of supporting mandatory standards for the natural gas industry. Despite current progress in the public and private sector, senators seemed frustrated with the pace at which industry and regulators are tackling this issue, the lack of urgency and information sharing, and the existence of operational silos.

CONCLUSION

The government has made clear that industry needs to take cyberthreats seriously and that it will not hesitate from imposing further regulation and using enforcement tools if necessary. But utilities need to go beyond compliance with mandatory standards and ensure proper systems, management involvement, training, communications, and continuous attention to reliability to prevent devastating attacks. Failure to do so not only leaves utilities more vulnerable but also increases the risk of adverse findings and higher penalties in any reliability investigation.

Reliability expert Earl Shockley even has suggested that a major cyberattack on the grid "would shatter the ideal cybersecurity framework of private-sector accountability for maintaining security of this critical infrastructure" and "could result in the government expropriating grid security responsibilities and creating different levels of oversight to ensure reliability and resilience of the electric power grid."[12]

---

[11] A video of the hearing and testimony of the witnesses is available on the Committee's website, https://www.energy.senate.gov/public/index.cfm/2019/2/hearing-to-consider-the-status-and-outlook-for-cybersecurity-efforts-in-the-energy-industry.

[12] Earl Shockley, *How to Avoid Shattering Private-Sector Accountability for Cybersecurity*, Electric Light & Power (Oct. 5, 2017), https://www.elp.com/articles/2017/10/how-to-avoid-shattering-private-sector-accountability-for-cybersecurity.html.