MARCH 2016
VOL. 16-3

ENERGY LAW REPORT

LexisNexis®

Pratt's Energy Law Report

VOLUME 16 NUMBER 3 MARCH 2016

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please email:
Jacqueline M. Morris
Email: ..... jacqueline.m.morris@lexisnexis.com
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) 487-3000
Fax Number . . . . . (518) 487-3584
Customer Service Web site . . . . . 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 . . . . . (518) 487-3000

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)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a registered trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2016 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

An A.S. Pratt® Publication

Editorial Office
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
www.lexisnexis.com

MATTHEW BENDER

(2016–Pub.1898)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Samuel B. Boxerman
Partner, Sidley Austin LLP

Andrew Calder
Partner, Kirkland & Ellis LLP

M. Seth Ginther
Partner, Hirschler Fleischer, P.C.

R. Todd Johnson
Partner, Jones Day

Barclay Nicholson
Partner, Norton Rose Fulbright

Bradley A. Walker
Counsel, Buchanan Ingersoll & Rooney PC

Elaine M. Walsh
Partner, Baker Botts L.L.P.

Sean T. Wheeler
Partner, Latham & Watkins LLP

Wanda B. Whigham
Senior Counsel, Holland & Knight LLP

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. Copyright 2016 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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, 347.235.0882. 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.

President Obama Signs Two New Cybersecurity Laws; FERC, Congress Take Aim at Cybersecurity Risks in the Electric Utility Sector

By Norma M. Krayem and Alvin Taylor*

A new law gives the President and the U.S. Secretary of Energy emergency powers over the electric sector in a grid security emergency and seeks to increase cyber information sharing to better protect all sectors including the energy sector. In addition, the Federal Energy Regulatory Commission has issued a Notice of Proposed Rulemaking to address cybersecurity concerns involving the electric grid, specifically the risk of malicious software being introduced into industrial control systems, software, and network services prior to their delivery to the customer. The authors of this article discuss these developments.

In light of the potentially devastating economic losses that could result from a cybersecurity attack causing widespread power outages as well as continued concerns about the vulnerability of the nation's electric utility system, President Barack Obama signed into law two bills of import and the Federal Energy Regulatory Commission ("FERC") continues to take actions to address critical cybersecurity concerns to the industry.

PRESIDENT OBAMA SIGNS NEW CYBERSECURITY LAWS INTO PLACE

President Obama has signed two cybersecurity bills into law that will impact the energy sector. First, P.L. 114-94 gives the President emergency authorities over the energy sector in the event of a grid security emergency. The President can then direct the U.S. Secretary of Energy to take any action needed in the sector as a result. The Secretary "may, with or without notice, hearing or report, issue such orders for emergency measures as are necessary in the judgement of the Secretary to protect or restore the reliability of critical electric infrastructure during such emergency." Grid security emergencies include cybersecurity and physical threats. These wide-ranging powers extend to all Electric Reliability Organizations, regional entities, or any owner, user or operator of "critical

* Norma M. Krayem is co-chair of Holland & Knight's cybersecurity and privacy practice and a senior policy advisor. Alvin Taylor is a senior counsel and represents clients in regulatory and transactional energy matters. Resident in the firm's Washington, D.C., office, the authors may be contacted at norma.krayem@hklaw.com and alvin.taylor@hklaw.com, respectively.

electric infrastructure." The term critical electric infrastructure is defined as "a system or asset of the bulk power system whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety or any combination of such matters" and tracks the concerns identified in Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."

Congress also continues to express serious concerns over the cybersecurity preparedness of the electric sector. The House Energy and Commerce Committee has spent a considerable amount of time on cybersecurity concerns with the electric grid as well. Chairman Fred Upton (R-Mich.), was instrumental in inserting the provisions in H.R. 22 while at the same time, moving his own bill, H.R. 8, the North American Energy Security and Infrastructure Act of 2015, which passed the House on December 3, 2015, and was sent over to the Senate. In the past few months, the Senate Energy and Natural Resources Committee passed S. 2012, the Energy Policy Modernization Act of 2015 out of committee by a bipartisan vote of 18-4. The bill designates the U.S. Department of Energy ("DOE") as the Sector-Specific Agency for the energy sector. Importantly, the bill provides for the President to notify the Secretary of Energy that "immediate action is needed to protect the bulk power system," and upon that notification, the Secretary of Energy has immediate emergency powers to order a bulk power system owner, operator or user to take actions immediately to avert or mitigate a cyber threat.

Second, the President signed into law P.L. 114-113, the Consolidated Appropriations Act, 2016, which includes the much discussed and debated cybersecurity information sharing bill. The new law is the first ever that provides limited liability protections to companies who share cyber threat indicators with the federal government as well as with each other. The Act codifies guidance provided in April 2014 by the U.S. Department of Justice ("DOJ") and the Federal Trade Commission ("FTC") that two companies sharing cyber threat indicators are not an antitrust violation. The DOJ and the U.S. Department of Homeland Security ("DHS") had until February 18, 2016, to issue interim guidelines for how the private sector should share information with the federal government. Final guidelines must be completed by June 18, 2016.

Increased sharing of cyber threat indicators focuses on ensuring that all companies understand that there are consistent threats that span all aspects of critical infrastructure and also seeks to raise preparedness, response and recovery levels. U.S. government officials have been quoted in recent days about attempts by the Islamic State of Iraq and the Levant ("ISIL") to hack into computers in the nation's electricity grid. Recent cybersecurity attacks on the

Ukrainian grid that caused blackouts have reportedly been traced back to the BlackEnergy family of malware. Public reports about attempted cybersecurity attacks—reportedly originating from Iran—on some U.S. dams have also caused alarm.

FERC ACTION

FERC issued a Notice of Proposed Rulemaking ("NOPR") on July 16, 2015, to address cybersecurity concerns involving the electric grid, specifically the risk of malicious software being introduced into industrial control systems, software and network services prior to their delivery to the customer. FERC's actions comes in response to two recently identified malware infections, one of which (Havex) was implanted in control systems and affected several European companies, and another (BlackEnergy) that was likely planted in 2011 but only recently activated.

While FERC does not have authority over upstream suppliers, it recently sought comments on how best to ensure the integrity and security of supply chain equipment and software based on those obligations on entities already subject to the North American Electric Reliability Corporation's ("NERC") authority. Based on these comments, FERC has indicated it intends to direct NERC to develop a new reliability standard to implement security controls over the supply chain.

This action is a result of serious and systemic concerns over cybersecurity risks in the supply chain and, demonstrating how significant FERC considers this threat, marks only the third time that FERC has exercised its authority to direct NERC to develop a reliability standard. FERC held a Technical Conference on January 28, 2016, to "facilitate a structured dialogue on supply chain risk management." In addition, the NOPR sought to correct two other vulnerabilities it does not believe were adequately addressed by NERC's proposed cybersecurity standards. First, FERC was concerned that NERC had not provided adequate physical protections for non-programmable components, e.g., cables and switches, of the communication systems between cyber assets that could enable "man-in-the-middle" attacks utilizing intercepted data. To correct this shortcoming, FERC directed NERC to modify its proposed standard to require the protection of all communication links and sensitive data between the electric system's control centers, including those carried by third-party networks.

Second, FERC questioned NERC's proposal to only establish security controls for transient devices (such as flash drives) connected to medium- and high-impact cyber systems but imposing no restrictions for devices connected to low-impact systems. Concerned that this approach created a security gap by which malware could still reach critical cyber assets connected to low-impact

systems, FERC directed NERC to provide more justification for its decision.

Although FERC is respecting its existing jurisdiction and is not seeking to directly impose obligations beyond those entities already subject to electric reliability standards, its proposals will begin to substantially change the working—and ultimately, the contractual—relationship the electric industry has with its suppliers. To close these gaps that could be exploited by sophisticated hackers, purchases of control systems and software will likely be limited to providers that can certify compliance with the final standards developed by NERC, and communications over telecom wires as well as wireless networks will be subject to new security provisions.

CONCLUSION

As cybersecurity concerns mount and concerns over physical security reinsert themselves in the electric utility sector, expect more oversight from DHS, DOE, and FERC, as well as increased activity at NERC.