AN A.S. PRATT PUBLICATION
JANUARY 2023
VOL. 9 NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: WE JUST CAN'T MOVE AWAY FROM CALIFORNIA
Victoria Prussen Spears

NEW WAVE OF "LIVE CHAT" AND "KEY STROKE" WIRETAPPING CLASS ACTIONS HITS CALIFORNIA COURTS
Paul M. Kakuske and Joel D. Siegel

CALIFORNIA AGE-APPROPRIATE DESIGN CODE IS NOT CHILD'S PLAY: 5 PRACTICAL TIPS TO COMPLY AND PROTECT KIDS' PRIVACY
Tambry Lynette Bradford, James Koenig, Ronald I. Raether Jr. and Robyn W. Lin

CALIFORNIA CONSUMER PRIVACY ACT ENFORCEMENT AND PREPARING FOR 2023 DATA PRIVACY RULES
Steven G. Stransky, Thora Knight and Thomas F. Zych

CALIFORNIA ATTORNEY GENERAL SENDS "STRONG MESSAGE" IN FINING SEPHORA $1.2 MILLION FOR PRIVACY ACT VIOLATIONS
Madeleine V. Findley and Effiong K. Dampha

FEDERAL TRADE COMMISSION MOVES FORWARD ON PRIVACY RULEMAKING
Christopher B. Leach, Arsen Kourinian, Dominique Shelton Leipzig, Jonathan H. Becker, Howard W. Waltzman, Michael Jaeger and Joshua M. Cohen

FEDERAL ENERGY REGULATORY COMMISSION PROPOSES TO OFFER RATE INCENTIVES FOR VOLUNTARY CYBERSECURITY INVESTMENT
Miles H. Kiger and Shereen Jennifer Panahi

CHINA'S LARGEST POTENTIAL DATA PRIVACY BREACH PROVIDES CAUTIONARY TALE FOR INTERNATIONAL EMPLOYERS: 5 STEPS FOR BUSINESSES TO TAKE
Nazanin Afshar, Ariella T. Onyeama and Nan Sato

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 1** **January 2023**

Editor's Note: We Just Can't Move Away from California
Victoria Prussen Spears 1

New Wave of "Live Chat" and "Key Stroke" Wiretapping Class Actions Hits California Courts
Paul M. Kakuske and Joel D. Siegel 3

California Age-Appropriate Design Code Is Not Child's Play: 5 Practical Tips to Comply and Protect Kids' Privacy
Tambry Lynette Bradford, James Koenig, Ronald I. Raether Jr. and Robyn W. Lin 6

California Consumer Privacy Act Enforcement and Preparing for 2023 Data Privacy Rules
Steven G. Stransky, Thora Knight and Thomas F. Zych 12

California Attorney General Sends "Strong Message" in Fining Sephora $1.2 Million for Privacy Act Violations
Madeleine V. Findley and Effiong K. Dampha 16

Federal Trade Commission Moves Forward on Privacy Rulemaking
Christopher B. Leach, Arsen Kourinian, Dominique Shelton Leipzig, Jonathan H. Becker, Howard W. Waltzman, Michael Jaeger and Joshua M. Cohen 19

Federal Energy Regulatory Commission Proposes to Offer Rate Incentives for Voluntary Cybersecurity Investment
Miles H. Kiger and Shereen Jennifer Panahi 25

China's Largest Potential Data Privacy Breach Provides Cautionary Tale for International Employers: 5 Steps for Businesses to Take
Nazanin Afshar, Ariella T. Onyeama and Nan Sato 33

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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) 487-3385
Fax Number ..... (800) 828-8341
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 ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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 trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2023 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

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2023–Pub. 4939)

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

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenisberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Baker & McKenzie LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2023 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, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. 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 Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Federal Energy Regulatory Commission Proposes to Offer Rate Incentives for Voluntary Cybersecurity Investment

By Miles H. Kiger and Shereen Jennifer Panahi*

In this article, the authors discuss a recent Notice of Proposed Rulemaking issued by the Federal Energy Regulatory Commission with cybersecurity implications.

The Federal Energy Regulatory Commission (FERC or Commission) recently issued a Notice of Proposed Rulemaking[1] to establish rules providing incentive-based rate treatment for utilities making certain voluntary cybersecurity investments (Cybersecurity NOPR or NOPR).[2]

According to FERC, the Cybersecurity NOPR sought to benefit consumers and national security by encouraging investments in advanced cybersecurity technology and participation by utilities in cybersecurity threat information sharing programs, as directed by Congress in the Infrastructure Investment and Jobs Act of 2021 (Infrastructure and Jobs Act or Act).[3]

While the Cybersecurity NOPR supersedes FERC's December 2020 cybersecurity NOPR (whose docket is being terminated), the instant Cybersecurity NOPR generally retains the incentive provisions outlined in the December 2020 NOPR.

Under the Cybersecurity NOPR, FERC proposes that:

- Cybersecurity expenditures, including both expenses and capital investments associated with advanced cybersecurity technology and participation in a cybersecurity threat information sharing program, would be eligible for an incentive.

- Eligible cybersecurity expenditures would be voluntary and have to materially improve the utility's cybersecurity posture. FERC proposes to establish a pre-qualified list (PQ List) of cybersecurity expenditures that are eligible for incentives.

---

* Miles H. Kiger and Shereen Jennifer Panahi are attorneys in the Washington, D.C., office of Troutman Pepper Hamilton Sanders LLP. They may be contacted at miles.kiger@troutman.com and jennifer.panahi@troutman.com, respectively.

[1] https://elibrary.ferc.gov/eLibrary/filedownload?fileid=8a9d1512-9b61-cd12-8b87-83663b200000.

[2] Incentives for Advanced Cybersecurity Investment; Cybersecurity Incentives, 180 FERC ¶ 61,189 (2022) (NOPR).

[3] Id. P 1.

- The incentives would take two forms:
    - A return on equity (ROE) adder of 200 basis points (ROE Incentive), or
    - Deferred cost recovery that would enable the utility to defer expenses and include the unamortized portion in its rate base (Regulatory Asset Incentive).
- Approved incentives, with certain exceptions, would remain in effect for up to five years from the date on which the investments enter service or expenses are incurred.

BACKGROUND

On November 15, 2021, the Infrastructure and Jobs Act was signed into law in which Congress, among other things, directed FERC to revise its regulations to establish incentive-based – including performance-based – rate treatments by encouraging utilities to invest in advanced cybersecurity technology and participate in cybersecurity threat information sharing programs.[4] The Act directed FERC to conduct a study in consultation with the Secretary of Energy, the North American Electric Reliability Corporation (NERC), the Electricity Subsector Coordinating Council, and the National Association of Regulatory Utility Commissioners to identify potential incentive treatments and to submit a proposed implementation plan to Congress within 180 days (May 2022 Report).[5] The Act requires FERC to establish its incentive-based rate treatments within one year of submitting the May 2022 Report, meaning FERC must issue a final rule by May 2023.

The Cybersecurity NOPR supersedes a December 2020 NOPR that represented the Commission's first attempt to create an incentive framework for public utilities to make additional investments in cybersecurity that exceed the requirements of the mandatory and enforceable NERC Critical Infrastructure Protection (CIP) Reliability Standards.[6] The December 2020 NOPR proposed two incentive approaches: (1) the NERC CIP Incentives approach, and (2) the National Institute of Standards and Technology (NIST) Framework approach.[7] Under the NERC CIP Incentives approach, utilities would have been eligible to receive incentive-based rate treatment for voluntarily applying certain CIP Reliability Standards to their facilities.[8]

---

[4] Infrastructure Investment and Jobs Act, Pub. L. 117-58, 135 Stat. 429 (to be codified at 16 U.S.C. § 824s-1).

[5] FERC, Incentives for Advanced Cybersecurity Technology Investment (May 2022) (May 2022 Report).

[6] Cybersecurity Incentives, Notice of Proposed Rulemaking, 86 FR 8309 (Feb. 5, 2021), 173 FERC ¶ 61,240 (2020).

[7] NOPR at P 11.

[8] Id.

Similarly, under the NIST Framework approach, utilities would have been eligible to receive incentive treatment for implementing certain security controls included in the NIST Framework that exceed the CIP Reliability Standards.[9] While the Cybersecurity NOPR generally retains the rate incentive provisions outlined in the December 2020 NOPR, i.e., the ROE and Regulatory Asset Incentives (discussed below), it jettisons the specific NERC CIP and NIST-based eligibility evaluations and replaces them with new standards to qualify for a cybersecurity incentive.

THE CYBERSECURITY NOPR

Proposed Approaches to Request an Incentive

Eligibility Criteria

FERC proposes new approaches to request a cybersecurity incentive under the NOPR.

First, FERC proposes certain threshold eligibility criteria to determine whether a cybersecurity expenditure qualifies for an incentive: A utility seeking an incentive must demonstrate that the expenditure would materially improve cybersecurity through either an investment in advanced cybersecurity technology[10] or participation in a cybersecurity threat information sharing program, and is not already mandated by CIP Reliability Standards, or otherwise mandated by local, state, or federal law.[11] The NOPR does not define what it means to "materially improve" cybersecurity, but FERC proposes to consider various sources in determining which cybersecurity expenditures will materially improve a utility's security posture.[12]

With respect to the first criterion, FERC sought comment on whether and how the Commission should evaluate the benefits of the cybersecurity expenditure relative to the costs of the expenditure and incentive to ensure the proposed rates are just and

---

[9] Id.

[10] FPA Section 219A(a)(1) defines the term advanced cybersecurity technology to mean any technology, operational capability, or service, including computer hardware, software, or a related asset, that enhances the security posture of public utilities through improvements in the ability to protect against, detect, respond to, or recover from a cybersecurity threat. Id. at n.7 (citing Infrastructure and Jobs Act, Pub. L. 117-58, Section 40123, 135 Stat. 429, 951).

[11] Id. at P 20.

[12] FERC specified that it will consider the following sources: (1) security controls enumerated in the NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations" catalog; (2) security controls satisfying an objective found in the NIST Cybersecurity Framework; (3) a specific recommendation from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency or from the Department of Energy (DOE); (4) a specific recommendation from the CISA Shields Up Campaign;[11] (5) participation in the DOE Cybersecurity Risk information Sharing Program (CRISP) or similar information sharing program; and/or (6) the Cybersecurity Capability Maturity Model Domains at the highest Maturity Indicator Level. Id. at P 21.

reasonable.[13] FERC also sought comment on whether these are the appropriate two eligibility criteria and whether there are additional criteria or limitations that it should consider.[14]

To identify the types of cybersecurity expenditures that the Commission will find eligible for an incentive, FERC proposes to use a list of pre-qualified investments, the so-called "PQ List," or an alternative case-by-case evaluation approach.[15] Under either approach, FERC proposes that a utility make a filing pursuant to FPA Section 205 for incentive-based rate treatment, even if a utility preliminarily files a petition for declaratory order seeking a ruling on its eligibility for an incentive.[16]

PQ List Approach

Under the PQ List approach to determining incentive eligibility, a utility would be required to demonstrate that its cybersecurity expenditure qualifies as one or more of the PQ List items in which case the expenditure would be entitled to a rebuttable presumption of eligibility for an incentive.[17] FERC proposes to include two eligible expenditures on the PQ List initially: (1) expenditures associated with participation in the DOE CRISP, a threat awareness and information sharing program,[18] and (2) expenditures associated with internal network security monitoring within the utility's cyber systems.[19] FERC sought comment on these and any additional cybersecurity expenditures to consider for inclusion on the initial PQ List.[20] FERC stressed that if a cybersecurity expenditure on the PQ List becomes mandatory, it would no longer be eligible for an incentive as of the effective date of the mandate.[21] FERC also noted that it would update the PQ List by adding, removing, or modifying cybersecurity expenditures, as needed via a rulemaking, whether *sua sponte* or in response to a petition.[22]

Case-by-Case Approach

Recognizing that the PQ List approach may limit expenditures eligible for incentives, FERC proposes an alternative case-by-case approach in which it would allow a utility to file for incentive-based rate treatment for any cybersecurity expenditure that satisfies the

[13] Id. at P 20.

[14] Id.

[15] Id. at P 23.

[16] Id.

[17] Id. at P 26.

[18] See DOE, Energy Sector Cybersecurity Preparedness, https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness.

[19] These internal network security monitoring expenditures would include information technology cyber systems and/or operational technology cyber systems and that could be associated with cyber systems that may or may not be subject to the CIP Reliability Standards. NOPR at P 28.

[20] Id. at P 30.

[21] Id. at P 31.

[22] Id.

eligibility criteria.[23] Under the case-by-case approach, there would be no presumption of eligibility for any given expenditure; utilities would bear the burden of demonstrating that the expenditure is voluntary and materially improves cybersecurity through either an investment in advanced cybersecurity technology or participation in a cybersecurity threat information sharing program.[24]

Proposed Rate Incentives

FERC proposes two rate incentives for utilities that make eligible cybersecurity investments: an ROE adder of 200 basis points that would be applied only to the incentive-eligible investments (ROE Incentive); and a deferral of eligible cybersecurity expenses, enabling them to be part of rate base such that a return can be earned on the unamortized portion (Regulatory Asset Incentive).[25] FERC proposed that the same expenditure should not be eligible for both the ROE Incentive and the Regulatory Asset Incentive.[26]

ROE Incentive

FERC proposes to allow a utility that makes eligible cybersecurity investments to request an ROE adder of 200 basis points that would be applied only to the incentive-eligible investments.[27] FERC proposes that any incentive granted would be subject to the total base and incentive return capped at the top of the utility's zone of reasonableness.[28] FERC explained that enterprise-wide investments – not just transmission-specific cybersecurity expenditures – would be eligible for the 200 basis-point ROE adder even if only a portion of those investments are allocated to the transmission function.[29]

Regulatory Asset Incentive

FERC proposes to allow a utility to defer recovery of eligible cybersecurity expenditures that are generally expensed and treat them as regulatory assets, while also allowing such regulatory assets to be included in transmission rate base.[30] Consistent with its rules associated with the Uniform System of Accounts, FERC proposes to require utilities to maintain sufficient records to support the distinction of any expenditures that are

[23] Id. at P 32.
[24] Id.
[25] Id. at P 33.
[26] Id. at P 38.
[27] Id. at P 36.
[28] Id.
[29] Id. at P 37.
[30] Id. at PP 39-40. FERC identified such expenses as including those that are associated with third-party provision of hardware, software, and computing and networking services, as well as subscriptions, service agreements, post-implementation training costs, and ongoing dues for participation by utilities in cybersecurity threat information sharing programs.

afforded incentive-based rate treatment as a regulatory asset.[31] FERC sought comment on whether it would be preferable to permit only 50% of incentive-eligible expenses to be treated as regulatory assets.[32]

Critically, FERC also sought comment on whether it should allow utilities that are already participating in an eligible cybersecurity threat information sharing program (such as CRISP) to seek to recover this incentive.[33]

Performance-Based Rates

Additionally, FERC proposes to consider performance-based rate treatments and sought comment on whether and how the principles of performance-based regulation could apply to utilities with respect to cybersecurity investments.[34]

Specifically, FERC sought comment on widely accepted metrics for cybersecurity performance and whether they could be benchmarks for performance-based rates, or whether new appropriate metrics could be developed.[35] FERC also sought comment on what rate mechanisms could accompany such performance metrics, minding that any proposed mechanisms must rely on cybersecurity performance benchmarks and not expenditures or practices and that proposed mechanisms consider ratepayer impacts.[36]

Proposed Incentive Implementation

ROE Incentive

FERC proposes various ways to determine what the duration of an ROE Incentive should be. FERC proposes to allow an ROE Incentive granted to a utility to remain in effect until the conclusion of the depreciable life of the underlying asset, five years, or when eligibility for the incentive terminates, whichever occurs earliest.[37] For assets with a depreciable life exceeding five years, FERC proposes to terminate the ROE Incentive after the first five years of the asset's service life because, according to FERC, the majority of information technology-related investments have expected useful lives of no longer than five years.[38] FERC, however, sought comment on whether the proposed duration should be shortened to three years.[39]

---

[31] Id. at P 42.
[32] Id. at P 39.
[33] Id. at P 41.
[34] Id. at P 45.
[35] Id.
[36] Id.
[37] Id. at P 46.
[38] Id.
[39] Id.

Regulatory Asset Incentive

The Cybersecurity NOPR also proposes that a utility granted a Regulatory Asset Incentive must amortize the regulatory asset over five years.[40] FERC also proposes that a utility granted the Regulatory Asset Incentive may defer eligible expenses for up to five years from the date of Commission approval of the incentive.[41] That is, eligible expenses could be added to the regulatory asset that is allowed in rate base and amortized over five subsequent years.[42] FERC, however, proposes an exception for cybersecurity threat information sharing programs.[43]

Specifically, because the costs of participating in such threat information sharing programs are distinct from discrete cybersecurity investments, FERC proposes to allow utilities to continue deferring these expenses and including them in rate base for as long as the utility continues incurring costs for its participation in the program, and the program remains eligible for incentives.[44]

Filing Process

The Cybersecurity NOPR also describes the procedures to obtain incentive rate treatment. Utilities will be required to make an FPA Section 205[45] filing to request incentive rate treatment, explaining in detail how it plans to implement the proposed incentive rate treatment, the cybersecurity expenditures for which it seeks incentives, and how its expenditures meet the incentive eligibility criteria.[46] Utilities with transmission formula rates would need to propose conforming revisions to their formula rates, as appropriate, to reflect incentive rate treatment granted.[47] For utilities with stated rates, FERC proposed that they may seek incentives as part of a larger rate case or make a request for single issue ratemaking that the Commission will evaluate on a case-by-case basis.[48] FERC also provided that a utility requesting the ROE Incentive must provide the anticipated cost of the capital investment and identify the tariff or rate schedule under which it will recover the increased ROE.[49] Similarly, a utility requesting the Regulatory Asset Incentive must provide a description of the covered expenses, including whether they are associated with the third-party provision of hardware, software, and computing network services or incurred for training to implement network analysis and monitoring programs, as well as an estimate of the expenses and when it is expected to be incurred.[50]

---

[40] Id. at P 47.
[41] Id. at P 48.
[42] Id.
[43] Id. at P 49.
[44] Id.
[45] 16 U.S.C. § 824d (2018).
[46] NOPR at P 50.
[47] Id. at P 51.
[48] Id. at P 51, n.47.
[49] Id. at P 53.
[50] Id.

Reporting Requirement

Once awarded incentive rate treatment, FERC proposes to require utilities to submit annual informational reports to the Commission by June 1.[51] FERC proposes that the annual filing should detail the specific investments made pursuant to the Commission's approval and the corresponding FERC account for which expenditures are booked.[52]

For recipients of the ROE Incentive, FERC proposes that each annual informational filing describe the parts of its network that it upgraded in addition to the nature and cost of the various investments.[53]

For recipients of the Regulatory Asset Incentive, FERC proposes the annual informational filings describe the expenses in sufficient detail to demonstrate that they are specifically related to the eligible cybersecurity investment underlying the incentives.[54]

Finally, FERC proposes that these annual informational filings will be subject to periodic Commission verification via requests for further informational filings, audits, or other similar means.[55]

[51] Id. at PP 54-55.
[52] Id. at P 55.
[53] Id.
[54] Id.
[55] Id. at P 56.