STATE OF CALIFORNIA GAVIN NEWSOM, *Governor*

PUBLIC UTILITIES COMMISSION
505 VAN NESS AVENUE
SAN FRANCISCO, CA 94102-3298

November 7, 2022

VIA ELECTRONIC DELIVERY

Ms. Kimberly D. Bose
Office of the Secretary
Federal Energy Regulatory Commission
888 First Street, N.E., Room 1A, East
Washington, D.C. 20426

Re: FERC Docket No. RM22-19-000: ***Notice of Proposed Rulemaking; Notice Terminating Proceeding, Incentives for Advanced Cybersecurity Investment; Cybersecurity Incentives***

Dear Ms. Bose:

Enclosed for filing in the above-docketed case, please find an original electronic filing of the attached document entitled **"INITIAL COMMENTS OF THE CALIFORNIA PUBLIC UTILITIES COMMISSION AND THE CALIFORNIA DEPARTMENT OF WATER RESOURCES STATE WATER PROJECT**."

Thank you for your cooperation in this matter.

Sincerely,

/s/ JONATHAN PAIS KNAPP
Jonathan Pais Knapp
Attorney

Enclosure

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives Notice of Proposed Rulemaking	Docket Nos.: RM22-19-000

INITIAL COMMENTS OF THE CALIFORNIA PUBLIC UTILITIES COMMISSION AND THE CALIFORNIA DEPARTMENT OF WATER RESOURCES STATE WATER PROJECT

LATIF M. NURANI
AMANDA C. DRENNEN

SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW, Suite 700
Washington, DC 20006
(202) 879-4000
Attorneys for the
California Department of Water Resources

CHRISTINE J. HAMMOND
JONATHAN PAIS KNAPP

505 Van Ness Avenue
San Francisco, CA 94102
Telephone: (415) 703-1626
Email: Jonathan.Knapp@cpuc.ca.gov

Attorneys for the California Public Utilities Commission and the People of the State of California

November 7, 2022

TABLE OF CONTENTS

Page

I. INTERESTS OF CPUC AND CDWR 1

II. INTRODUCTION 3

III. COMMENTS 7

A. California's Major Investor-Owned Utilities Already Participate in CRISP and are Implementing the Kinds of Security Controls that the NOPR Intends to Incentivize. 7

B. The Commission Should Only Grant Incentives for Participation in CRISP to Utilities That Are Not Currently Participating and Should Condition Incentive Awards on Participation in Regional and State Cybersecurity Initiatives. 9

1. Cybersecurity incentives should not reward utilities for actions they are already taking, such as participating in CRISP. 9

2. Cybersecurity incentives for participation in CRISP should be conditioned on utilities working collaboratively in their regions and states with relevant stakeholders on cybersecurity threat detection and mitigation issues. 12

C. The Commission Should Not Provide Incentives to Encourage Internal Network Security Monitoring. 13

1. Public utilities already have ample financial incentive to make prudent cybersecurity investments and allocate sufficient funding to network monitoring. 13

2. The Commission should not deter effective prioritization of utility cybersecurity spending with financial incentives. 15

3. The Commission should direct NERC to expeditiously develop requirements for internal network analysis and monitoring capabilities for medium and high impact BES cyber systems. 19

D. The Commission Should Refine its Proposed Eligibility Criteria. 20

E. The Commission should collaborate with state regulators to comprehensively address cybersecurity rather than granting incentives for enterprise-wide investments. 21

F. The Financial Impact of the Commission's Proposal on Ratepayers Should be Reduced by Appropriately Limiting the Cost and Duration of the Proposed Incentives. 22

1. The Commission has not substantiated the need for a 200-basis point ROE incentive. 22

2. The Commission has not substantiated the need to treat 100% of eligible expenses as a regulatory asset. 23

3. The duration of each of the proposed incentives should be no longer than three years. 25

G. Modifications are Needed to the Incentive Application Process. 27

1. Applicants must bear the burden of establishing that a cybersecurity expenditure identified on the pre-qualified list satisfies the eligibility criteria and that its proposed incentive is needed. 28

2. Application procedures must allow stakeholders adequate time and information to review incentive applications. 30

3. The case-by-case approach should not be adopted. 31

H. Any Additions to the PQ List Should be Conducted Through a New Rulemaking Procedure, and New Items Should be Added Only if Those Items are Appropriate for Incentive Treatment. 32

I. The Commission Should Require Utilities Awarded Cybersecurity Incentives to Submit Aggregated Data and Provide Vetted State Officials the Opportunity to Access It. 34

IV. CONCLUSION 35

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Cybersecurity Incentives Notice of Proposed Rulemaking	Docket Nos.: RM22-19-000

INITIAL COMMENTS
OF THE CALIFORNIA PUBLIC UTILITIES COMMISSION
AND THE CALIFORNIA DEPARTMENT OF WATER RESOURCES
STATE WATER PROJECT

Pursuant to the Commission's Notice of Proposed Rulemaking addressing cybersecurity incentives ("NOPR"),[1] the California Public Utilities Commission ("CPUC") and the California Department of Water Resources State Water Project ("CDWR") submit these Initial Comments.

I. INTERESTS OF CPUC AND CDWR

The CPUC is a constitutionally established agency charged with the responsibility for regulating electric corporations within the State of California. In addition, the CPUC has a statutory mandate to represent the interest of electric consumers throughout California in proceedings before the Commission.[2]

CDWR is an agency of the State of California, headquartered in Sacramento. It is responsible for monitoring, conserving and developing California's water resources,

[1] *Notice of Proposed Rulemaking; Notice Terminating Proceeding, Incentives for Advanced Cybersecurity Investment; Cybersecurity Incentives*, RM22-19-000; RM21-3-000 (Sept. 22, 2022) ("NOPR"); 87 FR 60567 (withdrawing proposed rule published at 86 FR 8309 and specifying initial comments due on November 7, 2022 and reply comments on November 15, 2022).

[2] Cal. Pub. Util. Code § 307(b).

providing flood protection to ensure public safety, and preventing property damage related to water resources. A primary responsibility of CDWR is the construction, operation, and maintenance of the State Water Project, which delivers an average of 2.6 million acre-feet of water per year to twenty-nine public agency water contractors throughout California.

Correspondence and communications concerning these comments should be directed to:

Jonathan Knapp
Public Utilities Commission of the
State of California
505 Van Ness Avenue
San Francisco, California 94102
Phone: (415) 703-1626
Email: jonathan.knapp@cpuc.ca.gov

Simon Hurd
Public Utilities Commission of the
State of California
505 Van Ness Avenue
San Francisco, California 94102
Phone: (415) 703-2503
Email: simon.hurd@cpuc.ca.gov

Pouneh Ghaffarian
Public Utilities Commission of the
State of California
505 Van Ness Avenue
San Francisco, California 94102
Phone: (415) 703-1317
Email: pouneh.ghaffarian@cpuc.ca.gov

Joshua Kim
Public Utilities Commission of the
State of California
505 Van Ness Avenue
San Francisco, California 94102
Phone: (916) 894-5647
Email: joshua.kim@cpuc.ca.gov

James Cho
Public Utilities Commission of the
State of California
505 Van Ness Avenue
San Francisco, California 94102
Phone: (415) 703-5356
Email: james.cho@cpuc.ca.gov

Danjel Bout
Public Utilities Commission of the
State of California
505 Van Ness Avenue
San Francisco, California 94102
Phone: (916) 713-4141
Email: danjel.bout@cpuc.ca.gov

Latif M. Nurani
Amanda C. Drennen
SPIEGEL & MCDIARMID
1875 Eye Street NW, Suite 700
Washington, DC 20006
Phone: (202) 879-4000
Fax: (202) 393-2866
latif.nurani@spiegelmcd.com
amanda.drennen@spiegelmcd.com

Matthew J. Goldman
Deputy Attorney General
CALIFORNIA DEPARTMENT OF JUSTICE
PO Box 944255
Sacramento, CA 94244-2550
Phone: (916) 210-7841
matthew.goldman@doj.ca.gov

Masoud Shafa
CALIFORNIA DEPARTMENT OF WATER RESOURCES
PO Box 942836
Sacramento, CA 94236-0001
Phone: (916) 574-1296
masoud.shafa@water.ca.gov

Robert S. Hedrick
Office of the General Counsel
CALIFORNIA DEPARTMENT OF WATER RESOURCES
PO Box 899
Sacramento, CA 95812-0001
Phone: (916) 902-7287
robert.hedrick@water.ca.gov

II. INTRODUCTION

The CPUC and CDWR (collectively referred to as the "California Parties") appreciate the opportunity to comment on this NOPR and to provide the California Parties' perspective on how narrowly tailored cybersecurity incentives could enhance the security of the bulk power system. The California Parties agree with Commissioner Phillips that "[i]n today's highly interconnected world, the nation's security and economic well-being depends on reliable and cyber-resilient energy infrastructure."[3] The ongoing threat posed to utility infrastructure and the overall grid by cyberattacks emphasizes the need for the Commission to make sound policy decisions that will result in the enhanced cybersecurity of utility assets, not proposals that may deter effective risk mitigation prioritization.

[3] NOPR, Commissioner Phillips concurrence at P 1.

Like Chairman Glick and Commissioners Clements and Christie, the California Parties have significant concerns with the cybersecurity incentives proposed in the NOPR. The California Parties have previously expressed our concerns with the cybersecurity incentives that were proposed in Commission Staff's 2020 Cybersecurity Whitepaper,[4] and the predecessor 2020 Notice of Proposed Rulemaking.[5] The cybersecurity incentives proposed in the instant NOPR differ from these previous proposals and are responsive to the Congressional mandate in the Infrastructure and Jobs Act ("Act").[6] The Act directs the Commission to establish incentive-based rate treatments to encourage utilities to participate in cybersecurity threat information sharing programs and invest in advanced cybersecurity technology.[7] The California Parties share Chairman Glick's and Commissioner Clements' overarching concern that incentives are not the best way to increase the cybersecurity of utility assets,[8] and Commissioner

---

[4] Cybersecurity Incentives Policy White Paper (June 18, 2020), eLibrary No. 20200618-4003 ("Cybersecurity White Paper"). The CPUC filed joint comments with the California Department of Water Resources State Water Project ("CDWR") in response to the Cybersecurity White Paper. *See Comments of the California Public Utilities Commission and the California Department of Water Resources*, Docket No. AD20-19-000 (Aug. 17, 2020), eLibrary No. 20200817-5210 (referred to below as "CPUC/CDWR Initial Comments on Cybersecurity Whitepaper") and *Reply Comments of the California Public Utilities Commission and California Department of Water Resources*, Docket No. AD20-19-000 (Sept. 1, 2020), eLibrary No. 20200901-5350

[5] *Cybersecurity Incentives*, 173 FERC ¶ 61,240 (2020) ("2020 NOPR"). The CPUC and CDWR filed joint comments in response to the 2020 NOPR. *See Comments of the California Public Utilities Commission and the California Department of Water Resources*, Docket No. RM21-3-000, eLibrary No. 20210406-6141 (April 6, 2021), (referred to below as "CPUC/CDWR Initial Comments on 2020 NOPR"); *Reply Comments of the California Public Utilities Commission and the California Department of Water Resources*, Docket No. RM21-3-000, eLibrary No. 20210506-5159 (May 6, 2021) (referred to below as "CPUC/CDWR Reply Comments on 2020 NOPR")

[6] NOPR at P 7 (*citing* Infrastructure and Jobs Act, Pub. L. 117-58, 135 Stat. 429). The Act directs the Commission to establish incentive-based rate treatments to encourage utilities to invest in advanced cybersecurity technology and participate in cybersecurity threat information sharing programs. 16 U.S.C. § 824s-1(c).

[7] 16 U.S.C. § 824s-1(c).

[8] Transcript, Commission Meeting, September 22, 2022 (referred to below as "September 22, 2022

Christie's concern with relying on return on equity ("ROE") adders as incentive mechanisms.[9]

That said, the California Parties support the Commission's establishment of a limited incentive, which could take the form of an ROE adder or regulatory asset treatment of cybersecurity expenditures, to encourage broader participation in the U.S. Department of Energy's Cybersecurity Risk Information Sharing Program ("CRISP").[10] As explained below in Sections III(B) and III(F), such incentives should only be available to utilities that are not currently participating in CRISP, be of limited value and duration, and be conditioned on utilities participating in all applicable regional and state cybersecurity initiatives.

Transcript") at 36:2-16 (when Chairman Glick explains that he has "significant concerns" with relying on incentives to enhance cybersecurity of utility assets because some utilities may not make the necessary investments, and thus, his "preferred option" would be for the Commission to use its "mandatory reliability standard approach" to require utilities to make necessary cybersecurity investments and participate in information sharing groups.); *id*. at 38:13-17 (emphasis added) (when Commissioner Clements emphasizes that "[t]o echo the Chairman's point, I have said in the past that when it comes to cyber security, we should mandate the investments or best practices that will enhance our posture for reliability and security of the power system. And this continues to be the case."); *c.f. id*. at 38:21-25 (where Commissioner Clements states that "[a]s a practical matter, I am interested in what role this proposal might play in helping to fill the gap relative to getting stronger rules in place, because the administrative process doesn't keep up with [the] ever-evolving threat.").

[9] *Id*. at 39:20-25—40:1-6 (emphasis added) (where Commissioner Christie cautions that "[t]he NOPR is going to give them a 200 basis point adder, 200 basis points. That is a lot. I mean, you know, the ROE already is supposed to represent the market cost of equity capital. And now you are going to give them 200 basis points on top of that for doing what they ought to do anyway? I mean there is a reason why these adders over the years have come to be known as FERC candy. They are really sweet for those who get it, but not to consumers who have to pay for it. It is pretty sour to consumers. *So the question is, is a 200 basis point adder even fair? Or is it just more FERC candy? So there are the two things I am concerned about*.").

[10] *See e.g*., NOPR at P 28 (where the Commission proposes two cybersecurity expenditures for initial inclusion on the pre-qualified list of expenditures eligible for incentive treatment: "(1) expenditures associated with participation in the DOE CRISP; and (2) expenditures associated with internal network security monitoring within the utility's cyber systems, which could include information technology cyber systems and/or operational technology cyber systems, and which could be associated with cyber systems that may or may not be subject to the CIP Reliability Standards.").

By contrast, the Commission should not provide monetary incentives to encourage increased spending on internal network security monitoring and cybersecurity investments that would divert from the holistic prioritization of risk, *e.g.*, by giving utilities a profit motive to disproportionately channel investment into monitoring low-impact assets and, potentially, fail to sufficiently prioritize protection of medium- and high-impact assets. Thus, as explained below in Section III(C), the California Parties oppose the NOPR's proposal to provide incentives for expenditures associated with internal network security monitoring within the utility's cyber systems.[11] As Chairman Glick and Commissioner Christie have emphasized, public utilities already have ample financial incentive to make prudent cybersecurity investments and allocate sufficient funding to network monitoring.[12] Instead, the Commission should direct the North American Electric Reliability Corporation ("NERC") to expeditiously develop requirements for internal network analysis and monitoring capabilities for high and medium impact bulk electric system cyber systems in its ongoing rulemaking proceeding in Docket No. RM22-3-000.[13]

---

[11] *Id*.

[12] September 22, 2022 Transcript at 36:21-25—37:1-2 (where Chair Glick observes that "the Federal Power Act does already provide us with the authority to ensure that utilities and other entities are able to recover investments, and that is certainly including investments in cyber security technology and participating in, again, in cyber security information sharing groups. And I think we have a pretty good record of that. And as a matter of fact, we had a technical conference . . . where we had a bunch of utilities come before us . . . and they all said we don't have a problem recovering our costs either at the federal level or the state level."); *id*. at 40:17-19 (where Commissioner Christie posits that "[o]ne might make the case that the formula rate treatment itself is a pretty good incentive, a pretty good incentive right there."); *see also* John Wolfram, Catalyst Consulting, *FERC Formula Rate Resurgence*, 34 Public Utilities Fortnightly July 2020 at 37 (emphasis added) (explaining that transmission formula rates "provide a clear advantage for transmission owners to recover their actual costs as transmission costs rise. . . . *FERC formula rates provide a strong incentive for grid expansion*."); *see* Section III(C)(1) *infra*.

[13] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber*

Beyond these fundamental recommendations, our Initial Comments also address, among other topics, specific questions in the NOPR regarding the Commission's proposed eligibility criteria and evaluation approaches, the cost and duration of the proposed incentives, the potential for expansion of the pre-qualified list of eligible cybersecurity expenditures, and reporting requirements.

III. COMMENTS

A. California's Major Investor-Owned Utilities Already Participate in CRISP and are Implementing the Kinds of Security Controls that the NOPR Intends to Incentivize.

As the California Parties have previously explained, as a result of the Commission's generous cost recovery mechanisms,[14] combined with the CPUC's unwavering support for state jurisdictional cybersecurity investments[15] and establishment of the California Energy Systems for the 21st Century Program ("CES-21"), which "charted an unprecedented level of collaboration among [California's major investor-owned utilities ("IOUs")], national labs, and industry on cybersecurity research,"[16]

Systems, Notice of Proposed Rulemaking, Docket No. RM22-3-000, 87 FR 4173 (Jan. 27, 2022), 178 FERC ¶ 61,038 (2022).

[14] *See* Section III(C)(1) *infra*.

[15] CPUC/CDWR Initial Comments on 2020 NOPR at 5 (citations omitted) (explaining that "the CPUC is a leader in ensuring that its regulated utilities are making prudent investments in cybersecurity for state jurisdictional assets. For example, the CPUC authorized [Pacific Gas and Electric Company ("PG&E")] to invest more than $114 million in cybersecurity capital expenditures and to spend an additional $49 million annually in IT physical and cybersecurity activities for the period 2018-2020.").

[16] *Id*. at 10 (citations omitted) (explaining that "[a]mong other things, the project produced a simulation engine for evaluating impacts of cyberattacks, a physical testbed environment representative of each investor-owned utility's substations, and advanced research into automated threat response systems."); *see also* California Energy Systems for the 21st Century (CES-21) Program Final Report (August 27, 2020), *available at* ces21_final_report_27aug2020.pdf (ca.gov) at 5 (emphasis added) (explaining that the CES-21 program "*charted an unprecedented level of collaboration among the IOUs, national labs, and industry on cybersecurity research*. The program also drew interest from federal departments because of its unique cybersecurity research objectives and agile research approach when Industrial Control System (ICS) cybersecurity and the [Machine-to-Machine Automated Threat Response] concept were nascent. *CES-21 has brought the eyes of the cybersecurity research*

California IOUs have already produced the kind of results that the NOPR seeks to achieve. The NOPR explains that the two cybersecurity expenditures that would be eligible for incentive treatment under the Commission's proposal—"participation in CRISP and internal network security monitoring"—"fall under recommendations" in the National Institute of Standards and Technology ("NIST") "SP 800-53 'Security and Privacy Controls for Information Systems and Organizations' catalog."[17] The major California IOUs already participate in the CRISP program,[18] and each of the IOUs' respective cybersecurity programs incorporates security controls from the NIST Framework.[19] For example, San Diego Gas & Electric Company's ("SDG&E's") cybersecurity program utilizes cybersecurity "risk management frameworks, including but not limited to, the NIST Cybersecurity Framework, Center for Internet Security (CIS-20), and **NIST 800-53**."[20] The major California IOUs are thus already implementing the cybersecurity activities that the NOPR seeks to encourage.

---

world onto California in a very positive and actualized manner. CES-21 has been recognized for its research by the Department of Energy (DOE), Department of Homeland Security (DHS), National Security Agency (NSA), numerous national laboratories, academic institutions, industry organizations, and individual companies.").

[17] NOPR at P 28 fn. 25.

[18] *See e.g.*, PG&E Corporate Sustainability Report 2022, *available at* Public Safety - PG&E Corporate Sustainability Report 2022 (pgecorp.com) (explaining that as part of the utility's commitment to cybersecurity "PG&E participates in the Cybersecurity Risk Information Sharing Program, which is a threat monitoring and intelligence sharing program sponsored by the U.S. Department of Energy.").

[19] CPUC/CDWR Initial Comments on 2020 NOPR at 5-7 (explaining that the major California IOUs' respective cybersecurity programs exceed NERC's Critical Infrastructure Protection ("CIP") standards and incorporate security controls from the NIST Framework).

[20] *Id*. at 6 (*citing* SDG&E, Risk Assessment Mitigation Phase (Chapter SDG&E -10/SCG-9) Cybersecurity, at SDG&E-10/SCG-9-9 (Nov. 27, 2019), https://www.sdge.com/sites/default/files/regulatory/SDG%26E-10_Cybersecurity_FINAL%20.pdf (referred to below as "SDG&E Cybersecurity Risk Mitigation Plan") at page SDG&E-10/SCG-9-9; *see also* SDG&E, SDG&E Smart Grid Deployment Plan: 2011 — 2020, Section 5 Grid Security and Cyber Security Strategy (last accessed Nov. 2, 2022), https://www.sdge.com/sites/default/files/Grid%2520Security%2520Cyber%2520Security%2520Strategy_1.pdf at 163-(explaining that "Company Information Security policies are based on accepted standards and guidelines,

B. The Commission Should Only Grant Incentives for Participation in CRISP to Utilities That Are Not Currently Participating and Should Condition Incentive Awards on Participation in Regional and State Cybersecurity Initiatives.

1. Cybersecurity incentives should not reward utilities for actions they are already taking, such as participating in CRISP.

Providing incentives to utilities that already participate in CRISP,[21] effectively rewarding them for conduct they are already undertaking, would fail to satisfy the Federal Power Act's ("FPA")[22] just and reasonable standard for incentive rates because the incentive would not, in fact, be needed.[23] As Commission Staff recently explained in

---

including . . . the NIST 800 series standards, and cover regulation important to SDG&E, such as NERC CIP Standards and Requirements and many others. The policy framework applies to the Sempra Energy Utilities . . . including SDG&E . . . .").

[21] NOPR at P 41 (asking "whether we should allow utilities who are already participating in an eligible cybersecurity threat information sharing program to seek to recover this incentive.").

[22] 16 U.S.C. § 791a, *et seq*. All further statutory references are to the Federal Power Act unless otherwise specified.

[23] *See e.g*., *City of Detroit, Michigan v. Fed. Power Comm'n*, 230 F.2d 810, 817 (D.C. Cir. 1955), *cert. denied sub nom* (emphasis added) ("[i]f the Commission contemplates increasing rates for the purpose of encouraging exploration and development, or the ownership by pipeline companies of their own producing facilities, *it must see to it that the increase is in fact needed, and is no more than is needed, for the purpose*. . . ."); see *City of Charlottesville, Va. v. Fed. Energy Regul. Comm'n*, 661 F.2d 945, 950 (D.C. Cir. 1981) ("explaining that "[a]n even more particular standard [of judicial review] applies when the Commission seeks, as here, to encourage exploration and development through increased rates to consumers."). This means that the Commission must "calibrate the relationship between increased rates and the attraction of new capital," or other activity that the incentive is designed to induce. *Farmers Union Cent. Exch., Inc. v. FERC*, 734 F.2d 1486, 1503 (D.C. Cir. 1984) (citations and internal quotation omitted) (finding that the Commission approved rates to incentivize additional oil pipeline capacity that merely ensured "creamy returns . . . far more generous" than provided elsewhere without estimating the need for additional capacity or "even attempt[ing] to calibrate the relationship between increased rates and the attraction of new capital. In the absence of such a reasoned inquiry," the D.C. Circuit held that it could not "countenance" the Commission's approval of the increased oil pipeline rates). Further, the Commission must substantiate the relationship between the incentive and the desired action with evidence and findings. *City of Detroit,* 230 F.2d at 818 ("[w]hen [incentive ratemaking] is used the evidence and findings must show that the [resulting] increase in rates . . . is no more than is reasonably necessary for the purposes advanced for any increase. Since there is nothing in these proceedings from which such a conclusion could be drawn, [the increased rates] are fatally defective [and thus do not satisfy the just and reasonable standard].").

relation to potential new cybersecurity incentives,[24] "**an incentive must actually incentivize something that benefits the ratepayer; otherwise, it is not a reasonable use of ratepayer funds**. Provision of incentives without a strong assurance that the investment will benefit the ratepayer may likely be unjust and unreasonable. Therefore, any incentive that the Commission provides [to encourage cybersecurity expenditures] **should incent actions that benefit customers, rather than reward actions that would have been taken anyway**."[25]

The Commission should not allow most utilities across the country that already participate in CRISP,[26] including the major investor-owned electric utilities ("IOUs") in California,[27] to be eligible to recover an incentive for their ongoing participation. Importantly, to participate in CRISP, utilities must pay certain start-up costs by, for example, "[i]nstall[ing] a passive information sharing device ["ISD"] on participant networks outside their firewalls to collect data relating to Internet traffic."[28] Once a

---

[24] FERC Staff Report, Incentives for Advanced Cybersecurity Technology Investment, May 2022 ("2022 FERC Staff Report") at 22; *id*. at 4 (citation omitted) (explaining that "[t]he Infrastructure and Jobs Act, in part, directs the Federal Energy Regulatory Commission . . . to conduct a study, in consultation with certain entities, to identify incentive-based rate treatments, including performance-based rates, for the jurisdictional transmission and sale of electric energy that could support investments in advanced cybersecurity technology and participation by public utilities in cybersecurity threat information sharing programs"); *see* 16 U.S.C. § 824s-1(b) (requiring the Commission to conduct the study "[n]ot later than 180 days after November 14, 2021.").

[25] 2022 FERC Staff Report at 22.

[26] *See e.g*., U.S. Department of Energy, *Energy Sector Cybersecurity Preparedness*, available at https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness (explaining that "[c]urrent CRISP participants provide power to over 75 percent of the total number of continental U.S. electricity subsector customers.").

[27] *See* note 18 *supra.*

[28] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, *Cybersecurity Risk Information Sharing Program*, *available at* Cybersecurity Risk Information Sharing Program (CRISP) (energy.gov).

utility has paid these start-up costs, the main, ongoing expenses associated with participation are the program's relatively small, annual subscription fee and utility staff time devoted to monitoring. Given the security benefits to the utility and the assurance of cost recovery for those small annual costs, there is no indication that utilities require an incentive to continue their voluntary participation in CRISP after they have made the initial start-up investment. Thus, an incentive would only be arguably justified for utilities that do not currently participate in CRISP, and thus, could potentially be induced to pay the requisite start-up costs. Under comparable circumstances, where the Commission failed to explain the need for incentive rate treatment, courts have held that the FPA's just and reasonable standard, which is expressly incorporated into the Act,[29] does not "countenance" the resulting increases to consumer rates.[30]

[29] 16 U.S.C. § 824s-1(e).

[30] *Farmers Union Cent. Exch., Inc. v. FERC*, 734 F.2d 1486, 1503 (D.C. Cir. 1984) (citations and internal quotation omitted) (finding that the Commission approved rates to incentivize additional oil pipeline capacity that merely ensured "creamy returns . . . far more generous" than provided elsewhere without estimating the need for additional capacity or "even attempt[ing] to calibrate the relationship between increased rates and the attraction of new capital. In the absence of such a reasoned inquiry," the D.C. Circuit held that it could not "countenance" the Commission's approval of the increased oil pipeline rates.); *see also Pub. Serv. Comm'n of State of N.Y. v. Fed. Energy Regul. Comm'n*, 589 F.2d 542, 554 (D.C. Cir. 1978) (citations and internal quotation omitted) (explaining that "the Commission has failed to give 'reasoned consideration' to the shaping of its order in an effort to protect consumers from paying substantially more than necessary to bring forth the needed supplies.").

2. Cybersecurity incentives for participation in CRISP should be conditioned on utilities working collaboratively in their regions and states with relevant stakeholders on cybersecurity threat detection and mitigation issues.

Cybersecurity incentives for participation in CRISP—for utilities that are not already participating in the program—should be conditioned on utilities working collaboratively in their regions and states with other utilities and relevant stakeholders on cybersecurity threat detection and mitigation issues. While CRISP provides awareness of the cybersecurity threat landscape on a national level,[31] utilities need to develop a team mentality with other utilities and relevant stakeholders within their respective regions and states to best mitigate threats to the overall grid. As Chairman Glick has astutely observed, "it just takes one weak link in the whole system to potentially cause major catastrophic damage from a reliability perspective."[32] To facilitate increased interaction between utilities and other relevant stakeholders, concerning monitoring, identification, and mitigation of cybersecurity threats, the Commission should require utilities to verify their participation in all applicable regional and state cybersecurity initiatives as a condition for receiving an incentive for participation in CRISP.[33] Examples of such

[31] *See e.g.*, NOPR at P 28 (*citing* U.S. Department of Energy, *Energy Sector Cybersecurity Preparedness*, available at https://www.energy.gov/ceser/energy-sector-cybersecurity-preparedness (explaining that the purpose of CRISP "is to facilitate the timely bi-directional sharing of unclassified and classified threat information and to develop situational awareness tools that enhance the energy sector's ability to identify, prioritize, and coordinate the protection of critical infrastructure and key resources.").

[32] September 22, 2022 Transcript at 36:8-10.

[33] A utility could verify its participation by demonstrating membership in a charter for an applicable task force, attendance at meetings, contribution to working groups, operational coordination, and/or information sharing.

initiatives could include participation in state Cybersecurity Taskforces and State Emergency Response Planning for Cybersecurity threats.[34]

As explained below in Section III(F), the California Parties recommend that any incentive provided by the Commission for participation in CRISP should be of limited value and duration.

C. The Commission Should Not Provide Incentives to Encourage Internal Network Security Monitoring.

1. Public utilities already have ample financial incentive to make prudent cybersecurity investments and allocate sufficient funding to network monitoring.

As Chairman Glick and Commissioner Christie have emphasized,[35] and many commenters,[36] including the California Parties, have previously explained, utilities

---

[34] California's major IOUs actively participate in such initiatives. *See e.g.*, PG&E, Pacific Gas and Electric Company Smart Grid Annual Deployment — 2020, at 93 (last accessed Nov. 2, 2022), https://www.pge.com/pge_global/common/pdfs/safety/how-the-system-works/electric-systems/smart-grid/AnnualReport2020.pdf (emphasis added) ("PG&E participates in multiple forums to ensure that its control design is current, comprehensive and remains in alignment with the standards and industry groups mentioned above. *PG&E also engages with external partners related to cybersecurity and cyber risk management*, including industry bodies, *government-related security forums*, and academia."); Cybersecurity and Protecting the Grid, Edison International, *available at* Cybersecurity | Edison International (emphasis in original) ("Our **partnerships** and close collaboration of shared intelligence across local, state, and federal government, and with other utilities, further strengthens our utility's protective defenses. [Southern California Edison ("SCE")] has a robust best practices sharing forum with its peer utility companies. This sharing not only includes best practices and lessons learned, but also allows our analysts to share threat intelligence among each other. SCE is part of an industry mutual assistance program for analysts to support each other in the event of an emergency.").

[35] *See* note 12 *supra*.

[36] *See e.g.*, 2022 FERC Staff Report at 18-19 (citations omitted) ("The record from the Commission's 2019 technical conference on cybersecurity as well as responses to staff's 2020 Cybersecurity White Paper and the Cybersecurity Incentives NOPR indicate that regulated utilities with cost-of-service rates have consistently been able to recover cybersecurity costs through both Commission-jurisdictional (wholesale) and state-jurisdictional (retail) rates. Numerous parties, including multiple utilities, submitted post-technical conference comments attesting that utilities were already (with no incentive-based rate treatments) making cybersecurity investments that exceeded their applicable requirements."); *see also* Cybersecurity White Paper at 9 n.26-28 (citations omitted) (noting the variety of cost recovery mechanisms the Commission has employed to allow utilities to recover the costs of "prudently incurred security expenditures.").

already have ample financial incentive to make prudent cybersecurity investments and allocate sufficient funding to network monitoring given the Commission's existing cost recovery mechanisms, *e.g.*, through formula rates, the presumption that all expenditures are prudent, and a generous return on equity ("ROE") for transmission investment.[37] Further, the NOPR cites to no *evidence*[38] that incentives are needed to encourage transmission owners to invest in cybersecurity,[39] that transmission owners are underinvesting in cybersecurity,[40] or that state regulators have disallowed recovery of cybersecurity expenditures.[41] Thus, the California Parties submit that apart from the limited financial incentives recommended above to encourage utilities to participate in

[37] CPUC/CDWR Initial Comments on 2020 NOPR at 5-6 (noting that California's three largest IOUs—PG&E, SCE, and SDG&E—"have transmission formula rates, which automatically allow for those utilities to add cybersecurity-related investments to ratebase and to recover cybersecurity-related expenses as they are incurred."); CPUC/CDWR Initial Comments on Cybersecurity Whitepaper at 6 (noting that "the Commission authorizes California's investor-owned utilities ("IOUs") to earn higher ROEs on transmission investments than the CPUC authorizes for state jurisdictional investments [and thus] California's IOUs can earn generous profits for making virtually risk-free investments in transmission cybersecurity.").

[38] The NOPR's justifications for the incentive are conclusory and not based on substantial evidence. *See* NOPR at P 39 (emphasis added) (stating the sole rationale for the proposed Regulatory Asset Incentive in the NOPR as follows: "to encourage investment in cybersecurity, we *believe* that it may be appropriate to allow utilities to defer and amortize eligible costs that are typically recorded as expenses including those that are associated with third-party provision of hardware, software, and computing and networking services."); *id*. at P 36 (emphasis added) (stating the sole rationale for the proposed ROE incentive in the NOPR as follows: "[w]e *believe* that a 200-basis point ROE adder *may be appropriate* to provide a meaningful incentive to encourage utilities to improve their systems' cybersecurity. . . . given the relatively small cost of cybersecurity investments compared to conventional transmission projects, a higher ROE *may be necessary* to affect the expenditure decisions of utilities, without unduly burdening ratepayers.").

[39] *See e.g.*, *Comments of the Industrial Energy Consumers of America*, Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210406-6137 at 6 ("[t]he Commission proposes to provide cybersecurity incentives to utilities on the backs of ratepayers without establishing a record that such incentives are needed or effective.").

[40] *See e.g., Notice of Intervention and Comments of the Michigan Public Service Commission*, Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210406-5459 at 6 ("the Commission does not assert or provide any evidence in the [2020] NOPR that electric utilities are generally underinvesting in prudent cybersecurity protections, or that underinvestment, where it does occur, is due to inadequate financial incentives.").

[41] *See e.g.*, *Comments of the Organization of MISO States,* Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210406-6089 at 4 ("there is no record of state and local regulators refusing cost recovery for utilities reacting aggressively and responsibly to quell cybersecurity threats.").

CRISP in the first instance, no additional financial incentives are needed to ensure utilities sufficiently invest in cybersecurity.

2. The Commission should not deter effective prioritization of utility cybersecurity spending with financial incentives.

The California Parties caution that cybersecurity incentives to encourage internal network security monitoring and cybersecurity investments could divert from the holistic prioritization of risk, *e.g.*, by inducing unnecessary investment in protection of low-impact assets to maximize returns from incentives and thereby draw resources away from potentially more cost-effective and security-enhancing investments to protect medium- and high-impact assets. As explained above in Section III(A), the major California IOUs have cybersecurity programs that include network security monitoring and voluntarily incorporate security controls from the NIST Framework in their respective cybersecurity programs, as do many other utilities throughout the country.[42] Thus, for example, SDG&E's Operational Technology ("OT") cybersecurity controls already include automated and continuous monitoring, *i.e.*, "OT network anomaly detection to identify and prevent potentially malicious network traffic," "monitoring of endpoint technology devices," and "[v]isibility into the status and location of all operational technology through asset management."[43] Electric utilities must undertake these types of internal

---

[42] *See e.g.*, *Comments of Transmission Access Policy Study Group,* Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210406-6050 at 6 (citations omitted) (explaining that "[u]tilities have told investors and state commissions that they are investing in cybersecurity beyond the minimum requirements; their trade associations have made similar public comments," and that these investments have included cybersecurity upgrades to implement the NIST Framework).

[43] SDG&E Cybersecurity Mitigation Plan at pages SDG&E-10/SCG-9-19—SDG&E-10/SCG-9-20.

cybersecurity network monitoring activities to ensure the security of their respective systems and are already doing so.

Further, although the NOPR proposes that to be eligible for incentive-based rate treatment, cybersecurity expenditures must satisfy two criteria, *i.e.*, that the expenditures materially improve cybersecurity *and are not already mandated*,[44] "[t]he ERO Enterprise[45] has [already] shifted from a primarily compliance-focused approach to one that incorporates a more holistic, risk-based approach in pursuit of continuous improvement, innovation, and value-driven efforts."[46] In other words, the ERO Enterprise currently "works with entities to voluntarily adopt secure practices,"[47] and is therefore already fulfilling the purpose of the NOPR by encouraging cybersecurity investment above-and-beyond that required by the CIP Reliability Standards that materially improve cybersecurity. The California IOUs and utilities throughout the country are already implementing the ERO Enterprise's risk-based approach to address

[44] NOPR at P 22.

[45] *Joint Comments of the North American Electric Reliability Corporation and the Regional Entities in Response to Notice of Proposed Rulemaking*, Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210406-6014 (referred to below as "ERO Enterprise Comments") at 1, fn.1 (explaining that "[t]he six Regional Entities include the following: Midwest Reliability Organization ("MRO"), Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council."). The North American Electric Reliability Corporation ("NERC") and the six Regional Entities are collectively referred to in these Reply Comments as the "Electric Reliability Organization Enterprise" or "ERO Enterprise."

[46] ERO Enterprise Comments at 4 (*citing NERC 2020 Annual Report* (Feb. 2021), *available at* https://www.nerc.com/gov/Annual%20Reports/NERC_Annual%20Report_2020.pdf at 10). *See also* Initial Comments of the Edison Electric Institute (April 6, 2021), eLibrary No. 20210406-6054 (referred to below as "EEI Comments") at 2-3 fn.3 (citing *Order on Electric Reliability Organization Risk Based Registration Initiative and Requiring Compliance Filing*, 150 FERC ¶ 61,213 (2015) (explaining that "[f]or years, the Commission has acknowledged and approved NERC's risk-based approach that directs efforts towards activities with a greater potential impact on bulk electric system reliability.").

[47] ERO Enterprise Comments at 4.

cybersecurity that includes voluntary implementation of controls from the NIST Framework.[48]

The Commission's proposal to make internal network monitoring activities eligible for incentive treatment is not only unnecessary,[49] but would also likely be detrimental to the overall cybersecurity of the bulk power system.[50] The availability of incentives for internal network monitoring, *i.e.*, the inclusion of cybersecurity operational expenses as regulatory assets in rate base or the application of an ROE adder to cybersecurity capital expenditures,[51] could induce utilities to spend more on network monitoring to earn a return, or an inflated return, on such investment. The most direct way for utilities to increase their cybersecurity spending on network monitoring would be to allocate resources to the monitoring of low-impact assets, as there are far more low-impact assets than medium- or high-impact assets.[52] This, in turn, could affect utilities'

---

[48] CPUC/CDWR Reply Comments on 2020 NOPR at 5-6.

[49] *See e.g.*, *Initial Comments of the American Public Power Association,* Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210406-6096 (referred to below as "APPA Comments") at 4 (emphasis added) ("[e]ven in circumstances where more robust cybersecurity investment might be beneficial, new incentives would not be just and reasonable *because they are not needed to promote such investment*."); *id*. at 8 (emphasis added) (*citing* Security Investments for Energy Infrastructure Technical Conference, Docket No. AD19-12-000, Written Statement of Kevin G. Wailes (March 26, 2019) at 7 ("[i]n situations where additional cybersecurity efforts would be appropriate, '*[p]ublic utilities already have numerous financial, legal, and reputational incentives to promote physical and cybersecurity*.'").

[50] Financial incentives encouraging spending on transmission assets could also detrimentally channel utility spending away from protecting distribution assets. *See Comments of the New England Conference of Public Utilities Commissioners in Response to Notice of Proposed Rulemaking on Cybersecurity Incentives,* Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210406-6176 at 8 (warning that the "compounding impacts of FERC's [incentive] policies" could also result in the diversion of investment capital away from "necessary and effective" cybersecurity investments in distribution infrastructure in favor of "potentially less-effective transmission cybersecurity investment" that is eligible for incentive treatment.).

[51] NOPR at P 33 (where the Commission proposes two incentives for utilities that make eligible cybersecurity investments: "an ROE adder of 200 basis points that would be applied to the incentive-eligible investments;" and "deferral of certain eligible expenses for rate recovery, enabling them to be part of rate base such that a return can be earned on the unamortized portion.").

[52] *See e.g.*, CPUC/CDWR Initial Comments on 2020 NOPR at 12 (citation omitted) (emphasis added) (explaining

risk prioritization by encouraging cybersecurity spending on *more* low-impact assets, as opposed to ensuring that the *most important* cyber systems, *i.e.*, medium- and high-impact assets, are sufficiently protected.[53]

In addition, as the California Parties and other commenters have previously explained, the nature of the NIST Framework—a flexible, risk-based, voluntary tool that allows for customization based on specific circumstances—makes it inherently inappropriate to serve as the basis for regulatory incentives.[54] Were the Commission to adopt an incentive for internal network monitoring based on the security controls identified in the NIST SP 800-53 "Security and Privacy Controls for Information Systems and Organizations" catalog,[55] transmission owners would be able to seek incentives for

---

that "high impact assets are limited to large control centers, and medium impact assets are a narrowly defined set of large generators, transmission facilities operating above 200 kV, and smaller control centers; in contrast, the low impact category includes *all* [Bulk Energy System] Cyber Systems that are no designated medium or high. *The result is that low impact systems are much more numerous and much more diverse than medium or high impact systems*.").

[53] Many commenters, including the California Parties, expressed similar concern with the Commission's incentive proposal in the 2020 NOPR to award incentives to utilities that applied CIP Reliability Standards designed for medium- or high-impact assets to low-impact assets. CPUC/CDWR Initial Comments on 2020 NOPR at 8, 11-13; *see also e.g., Comments of Alliant Energy Corporate Services, Inc*., Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210406-5575 at 11 ("[i]ncentivizing entities to increase security on low-impact systems provides a financial cost without commensurate customer or BES benefit. Such systems are identified as 'low-impact' because of the limited impact to security on the operation of the BES."); *Comments of the National Rural Cooperative Association,* Docket No. RM21-3-000 (April 6, 2021), eLibrary No. 20210405-5698 at 4-5 (explaining that the "availability of [the] incentive may encourage utilities to divert finite resources to applying CIP standards to low-impact assets instead of high- or medium-impact assets and may limit the tools the utilities employ to increase cybersecurity."). *See* 2020 NOPR at P 27 (where the Commission proposed to grant an ROE adder to transmission owners that make investments to conform their low impact BES systems to medium and/or high impact requirements).

[54] CPUC/CDWR Reply Comments on 2020 NOPR at 18-19; *see also Comments of the Transmission Access Policy Study Group*, Docket No. AD20-19-000 (August 17, 2020), eLibrary No. 20200817-5185 at 7 (citations omitted) (emphasis added) (where TAPS raised this concern in response to the Cybersecurity White Paper, which identified five types of security controls from the NIST Framework that could be considered for incentive treatment, explaining that "the White Paper proposal for granting incentives based on the NIST Framework *is an open invitation to transmission owners to re-package their existing plans into an incentive application*.")

[55] NOPR at P 28 fn. 25.

cybersecurity controls that they were already planning to implement by re-packaging parts of their existing cybersecurity plans into an incentive application based on security controls that could be construed as falling within the "Assessment, Authorization, and Monitoring" category, and/or other related controls or categories.[56]

Given that incentives to encourage utility spending on internal network monitoring are not needed, could have the effect of detrimentally skewing how utilities prioritize spending on cybersecurity, and should not be based on the NIST Framework, the California Parties urge the Commission not to adopt this proposal.

3. The Commission should direct NERC to expeditiously develop requirements for internal network analysis and monitoring capabilities for medium and high impact BES cyber systems.

Instead of making internal network security monitoring costs eligible for incentive treatment, the Commission should simply direct NERC to expeditiously develop requirements for internal network analysis and monitoring capabilities for medium- and high-impact BES cyber systems (though not for low-impact BES cyber systems) in the ongoing rulemaking proceeding in Docket No. RM22-3-000.[57] For all the reasons explained above in Section III(C)(2), this is the optimal regulatory path forward.

---

[56] NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology, U.S. Department of Commerce (Sept. 2020), *available at* Security and Privacy Controls for Information Systems and Organizations (nist.gov)

[57] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Notice of Proposed Rulemaking, Docket No. RM22-3-000, 87 FR 4173 (Jan. 27, 2022), 178 FERC ¶ 61,038 (2022). *See* Comments of CDWR, Docket No. RM22-3-000 (March 28, 2022), eLibrary No. 20220328-5256 at 4 (urging the Commission to "adopt the most cost-effective solutions to protect the Bulk Electric System" and to "not expand the scope of the proposed directive to low impact BES Cyber Systems unless a record is developed in this proceeding that shows the incremental benefits of expanding the directive outweigh the incremental costs.").

D. The Commission Should Refine its Proposed Eligibility Criteria.

The Commission should make two revisions to its proposed eligibility criteria by: (1) defining what constitutes a mandatory cybersecurity expenditure; and (2) not allowing cybersecurity expenditures associated with transmission projects that have been developed outside of independent transmission planning processes to be eligible for incentive treatment.[58] First, the Commission should specify that any cybersecurity expenditure that a utility is obligated to make, *e.g.*, as a condition for a state commission granting a merger, or as the result of an enforcement action, should be ineligible for incentive treatment.[59] Second, to promote competitive markets and help curtail the growing investment in asset repair and replacement projects, the California Parties strongly urge that projects planned outside of independent planning processes, *e.g.*, regional planning processes, should not be eligible for *any* incentives, including cybersecurity incentives.[60]

---

[58] NOPR at P 22 (the Commission proposes that to be eligible for incentive-based rate treatment cybersecurity expenditures must satisfy two criteria: that the expenditures materially improve cybersecurity and are not already mandated); *id*. at PP 20, 22 (where the NOPR seeks comment on these criteria and asks whether the Commission should adopt any additional criteria).

[59] *Id*. at P 20 (asking "whether the Commission should consider an obligation imposed by a state commission as a condition for a merger to be ineligible for an incentive.").

[60] *See e.g., Initial Comments of the California Public Utilities Commission*, Docket No. RM21-17-000 (Oct. 12, 2021) at 2-5, 51 (describing the existing perverse incentives that have resulted in utilities channelling transmission investment into asset repair and replacement projects, and local and other projects exempt from competitive processes and proposing reforms to remedy "this fundamental, systemic problem in the transmission sector," including, among other things, disallowing incentives for any project that has not been developed in an independent planning process.).

E. The Commission should collaborate with state regulators to comprehensively address cybersecurity rather than granting incentives for enterprise-wide investments.

The NOPR proposes to grant incentives for expenditures that are on "enterprise-wide investments"[61] which are principally under the jurisdiction of state commissions. The vast majority of corporate IT system expenses are recovered through state-jurisdictional rates. The NOPR proposes to incentivize only the portion of such investments conventionally allocated to Commission-jurisdictional rates. But to enhance cybersecurity, the entire corporate IT system must be secured, not just the portion that is recovered under Commission-approved rates. By granting incentives for upgrades to state-jurisdictional equipment, the Commission is treading upon the authority of state commissions. Investment in state-jurisdictional assets is a matter that should be left to the states.[62]

At the very least, the Commission should partner with the states on cybersecurity enhancements rather than adopt the NOPR's go-it-alone approach.[63] The proposed incentives to the enhancement of mostly-state jurisdictional corporate IT systems could result in piecemeal and illogical investment because the majority of the upgrades needed

---

[61] NOPR at P 37.

[62] CPUC/CDWR Initial Comments on Cybersecurity Whitepaper at 12 (where the California Parties recommended that "[t]he Commission should not grant any incentives for cybersecurity investments that are subject to state jurisdiction [such as enterprise-wide assets]. Not only would doing so violate the Federal Power Act, it may actually deter or undermine state efforts to improve the cybersecurity of the assets under their jurisdiction."); *id*. at 13 ("if the Commission were to start granting ROE incentives for investments made on state-jurisdictional assets, utilities would be financially motivated to seek higher profits from the Commission rather than participate in . . . state-led, security-enhancing programs. That is precisely the wrong kind of incentive, and the Commission should not adopt it.").

[63] CPUC/CDWR Initial Comments in Response to 2020 NOPR at 10-11 (explaining that the CES-21 program "demonstrates the potential benefits that can accrue to the grid when states and federal agencies work together."); *see* Section III(A) *supra* (describing CES-21 program).

would not be recovered without the approval of the state commissions. Partnering with state commissions would facilitate the kind of holistic approach to cybersecurity that is necessary to secure all of a utility's systems, not just the ones that the Commission regulates.

F. The Financial Impact of the Commission's Proposal on Ratepayers Should be Reduced by Appropriately Limiting the Cost and Duration of the Proposed Incentives.

To the extent the Commission offers any incentives for cybersecurity expenditures,[64] such incentives should be limited in value and duration. Specifically, as explained in more detail below, the Commission should, subject to the requisite showing of need, limit ROE incentives for cybersecurity expenditures to no more than 25- or 50-basis points, allow no more than 50% of eligible expenses to be treated as regulatory assets, and limit the duration of any cybersecurity incentives to three years, with no exceptions.

1. The Commission has not substantiated the need for a 200-basis point ROE incentive.

The Commission has failed to justify its proposal for a 200-basis point adder, which, as Commissioner Christie rightly observes, "is a lot," and, of course, is "on top" of the utility's base ROE, "for doing what they ought to do anyway[.]"[65] Specifically, the NOPR fails to explain *why* the Commission believes the proposed adder is properly

[64] As explained above in Section III(B), the California Parties urge the Commission to only grant cybersecurity incentives to encourage participation in CRISP by utilities that are not already participating, and for no other purpose.

[65] September 22, 2022, Transcript at 39:20-25.

calibrated to induce the desired investment other than to state, in conclusory fashion, that "given the *relatively small cost of cybersecurity investments* compared to conventional transmission projects, a higher ROE may be necessary to affect the expenditure decisions of utilities, without unduly burdening ratepayers."[66] The California Parties respectfully submit, however, that the significant amounts authorized by the CPUC in recent years for state jurisdictional cybersecurity capital expenditures and annual IT physical and cybersecurity activities demonstrates that cybersecurity investments for major IOUs are not "relatively small."[67] Thus, the additional cost of a 200-basis point ROE incentive applied to cybersecurity expenditures would constitute a substantial burden on ratepayers. Instead, the California Parties urge the Commission to establish a ceiling for the value of the adder of no more than 25- or 50-basis points to impose a lesser burden on consumers.[68]

2. The Commission has not substantiated the need to treat 100% of eligible expenses as a regulatory asset.

The Commission has also failed to justify its proposal to allow 100% of eligible cybersecurity expenses[69] to receive incentive treatment as a regulatory asset that is

---

[66] NOPR at P 36 (emphasis added).

[67] *See* note 15 *supra*.

[68] Consistent with the California Parties' recommendation in Section III(G)(1) *infra*, the applicant seeking an incentive must demonstrate that the proposed cybersecurity expenditure satisfies the eligibility criteria and that, if granted, the incentive will result in just and reasonable rates. As part of this demonstration, the applicant should be required to show that the requested value of the an ROE incentive—not to exceed the ceiling of 25- or 50-basis points—"is in fact needed, and is no more than is needed, for the purpose[.]" *City of Detroit, Michigan v. Fed. Power Comm'n*, 230 F.2d at 817.

[69] The NOPR broadly defines potentially eligible cybersecurity expenses to include: third-party provision of

included in transmission rate base, referred to as the "Regulatory Asset Incentive."[70] The NOPR's only rationale for the Regulatory Asset Incentive is its conclusory claim that "to encourage investment in cybersecurity, *we believe* that it *may be appropriate* to allow utilities to defer and amortize eligible costs that are typically recorded as expenses . . . ."[71] Thus, the Commission fails to offer *any* explanation as to *why* its proposal that 100% of eligible expenses should be able to receive incentive treatment is properly calibrated to induce the desired investment. In fact, the NOPR asks whether the allowable percentage should be reduced to 50%.[72] To reduce the burden on consumers from the Regulatory Asset Incentive, the California Parties urge the Commission to allow *no more than* 50% of eligible expenses— subject to the requisite showing of need—to be treated as a regulatory asset included in transmission rate base.[73] Further, the California Parties strongly support the Commission's preliminary finding that costs that are allowed to be deferred as a regulatory asset and included in rate base for determination of the base return, should not be eligible for the additional return associated with the proposed ROE adder.[74]

---

hardware, software, computing, and networking services; internal system evaluations and assessments or analyses by third parties; cybersecurity training expenses; and recurring expenses, such as subscriptions, service agreements, and post-implementation training costs. NOPR at PP 39-40.

[70] NOPR at P 39 (describing the proposed incentive as follows: "[w]e believe that, in limited circumstances, it may be appropriate to allow a utility to defer recovery of certain cybersecurity costs that are generally expensed as they are incurred, and treat them as regulatory assets, while also allowing such regulatory assets to be included in transmission rate base (Regulatory Asset Incentive).").

[71] *Id*. at P 39 (emphasis added).

[72] *Id*.

[73] See e.g., *City of Detroit, Michigan v. Fed. Power Comm'n*, 230 F.2d at 817.

[74] NOPR at P 38.

3. The duration of each of the proposed incentives should be no longer than three years.

The duration of each of the proposed cybersecurity incentives should be no longer than three years,[75] and the Commission should not "make an exception to this sunsetting provision for eligible cybersecurity threat information sharing programs."[76] In the NOPR, the Commission proposes to allow a utility granted a cybersecurity ROE incentive "to receive that incentive *until the earliest of*: (1) the conclusion of the depreciation life of the underlying asset; (2) *five years from when the cybersecurity investment(s) enter service*; (3) the time that the investment(s) or activities that serve as the basis of that incentive become mandatory pursuant to a Reliability Standard approved by the Commission, or local, state, or Federal law; or (4) the recipient no longer meets the requirements for receiving the incentive.[77] The NOPR similarly proposes that "a utility granted the Regulatory Asset Incentive must amortize the regulatory asset over five years."[78] The Commission preliminarily finds that five years is a "reasonable expected life" to serve as the basis for the duration of incentives given that "[t]he vast majority of information technology-related investments feature expected useful lives and corresponding cost-of-serve depreciation rates *of no longer than five years*."[79]

---

[75] *Id.* at P 46 (where the NOPR seeks comment "on whether the proposed duration should be three years instead of five years.").

[76] *Id*. at P 49.

[77] *Id*. at P 46 (emphasis added).

[78] *Id*. at P 47.

[79] *Id*. at P 46 (emphasis added).

The California Parties respectfully submit that given the evolving nature of cybersecurity technology and security controls, a five-year duration could create perverse incentives to keep old technology online in years four and five if a cybersecurity expenditure has not yet been fully depreciated, even if replacing the technology would make the system more secure. Further, as the Commission recognizes, cybersecurity investments typically have short depreciation lives, "of no longer than five years," and, notably, there is no evidence offered in the NOPR that a maximum five-year depreciation period is necessary. Thus, a three-year maximum duration is more likely to result in just and reasonable rates than a five-year period. Given, as explained above, the significant cost of cybersecurity expenditures,[80] a three-year maximum duration will serve to mitigate the compounding year-over-year burden on ratepayers. Lastly, because the depreciable life of cybersecurity expenditures eligible for incentive treatment will almost always be five years or less, and the duration is capped at the shorter of the depreciable life of the asset or when the security control becomes mandatory, a five-year maximum duration would effectively serve no purpose as it would never come into play. For all these reasons, the California Parties urge the Commission to only allow utilities to receive cybersecurity incentives for no longer than three years.

Further, the California Parties strongly support Commissioner Phillips' admonition against "open-ended or permanent cyber incentives."[81] Specifically, as

[80] *See* note 15 *supra*.

[81] NOPR, Commissioner Phillips concurrence, at P 7 ("To be clear, I do not support open-ended or permanent cyber incentives.").

explained above in Section III(B)(1), the California Parties oppose the NOPR's proposal "to make an exception to [the] sunsetting provision for eligible cybersecurity threat information sharing programs," by allowing utilities to continue deferring expenses for participation and including such expenses in their rate base "*for each annual tranche of expenses*, for as long as: (1) the utility continues incurring costs for its participation in the program; and (2) the program remains eligible for incentives."[82] As explained above, once a utility has elected to participate, *i.e.*, "to take part,"[83] in CRISP and has paid the requisite start-up costs, there is no longer a purpose served by incentive treatment given that the utility is able to readily recover all ongoing costs of participation (along with the start-up costs) in transmission rates. To provide incentives in this circumstance—where they are simply not needed to induce prudent spending on an annual subscription to CRISP and associated staff time—would result in unjust and unreasonable rates in violation of the express language of the Act.[84]

G. Modifications are Needed to the Incentive Application Process.

The proposed incentive application process—which would grant utilities a rebuttable presumption of eligibility for cybersecurity expenditures on the PQ List—would not be adequate to allow the Commission to determine whether a requested incentive will (a) improve a utility's cybersecurity posture and (b) result in just and reasonable rates. The Commission should modify the proposal to:

[82] NOPR at P 49 (emphasis added).

[83] Merriam Webster Dictionary, *available at* Participate Definition & Meaning - Merriam-Webster.

[84] 16 U.S.C § 824s-1(e).

- Require each utility to demonstrate that a cybersecurity expenditure from the PQ List will satisfy the eligibility criteria for that utility.
- Require each utility to demonstrate the incentive is just and reasonable, including a demonstration that the incentive is needed.
- Allow stakeholders adequate time and information to review incentive applications.

1. Applicants must bear the burden of establishing that a cybersecurity expenditure identified on the pre-qualified list satisfies the eligibility criteria and that its proposed incentive is needed.

The Commission should not adopt the NOPR's proposal to grant a rebuttable presumption of incentive eligibility for any cybersecurity expenditure on the PQ List. The Commission should adopt the NOPR's proposal to place the burden on an incentive-seeking utility to demonstrate that the incentive rate is just and reasonable, but the Commission should explicitly clarify that the just-and-reasonable demonstration include a demonstration that the utility does, in fact, need the incentive to make the expenditure.

The proposed presumption of eligibility would, in practice, be effectively irrebuttable. The NOPR suggests that the presumption could be rebutted by a protestor (or the Commission acting *sua sponte*) demonstrating that, given a utility's unique circumstances, the expenditure would be mandatory or would not materially improve security. But the NOPR ignores the reality that no protestor (nor the Commission) will have access to the utility-specific information that could be used to make such a demonstration. Since the utility would have no obligation, under the proposed presumption, to put any utility-specific information into the record, and since the utility's cybersecurity posture is (quite correctly) not publicly available, there is no practical way

for a concerned stakeholder to obtain any information that could be used to rebut the presumption.

Instead of granting a rebuttable presumption, the Commission should require each applicant to demonstrate that the cybersecurity expenditure from the PQ List does, in fact, materially improve that utility's cybersecurity posture. The PQ List would serve as a pre-defined set of technologies and information sharing programs that the Commission determines it generally wants to encourage, but individual applications would present utility-specific information to assess whether the specific expenditure meets the eligibility criteria.

In addition to demonstrating its expenditure meets the eligibility criteria, a utility must also bear the burden of demonstrating that the resulting incentive rate is just and reasonable. As discussed in Section III(B)(1) above, an incentive rate is just and reasonable only if "the increase is in fact needed, and is no more than needed, for the purpose."[85] Thus, to demonstrate that its proposed rate is just and reasonable, a utility must include evidence that the requested rate treatment is needed for the utility to make the cybersecurity expenditure. The Commission should make that principle explicit in its final rule.

[85] *See* note 23 *supra*.

2. Application procedures must allow stakeholders adequate time and information to review incentive applications.

In addition to eliminating the proposed rebuttable presumption, the Commission should clarify the incentive application procedures to ensure stakeholders have adequate time and information to meaningfully review and comment on utility incentive requests.

The Commission's usual filing procedures under Section 205 are not sufficient because they neither provide ample time for review given the more complex nature of cybersecurity incentive applications, as compared to applications for incentives under Section 219,[86] nor do the procedures ensure the development of an adequate factual record. The filing procedures under Section 205 provide only twenty-one days for an interested party to intervene and comment and do not ensure the opportunity for discovery or evidentiary hearings. Applications for cybersecurity incentives, however, will be much more fact-intensive and complex to analyze than incentive applications under Section 219 because assessment of an application's projected cybersecurity benefits will require consideration of critical energy infrastructure information.

The NOPR recognizes that incentive requests may include "specific engineering, vulnerability, or detailed design information" about critical infrastructure, and that applicants should seek Critical Energy/Electric Infrastructure ("CEII") treatment of such information.[87] We strongly agree that such information should not be made public. But, at the same time, appropriate individuals who have complied with the Commission's

[86] 16 U.S.C. 824(s) ("Section 219").

[87] NOPR at P 24.

CEII regulations *must* be able to get timely access to that information and have the ability to provide the Commission analysis of whether a cybersecurity expenditure will materially improve a utility's cybersecurity posture. In order to ensure that adequate time and access, the Commission should make clear that all cybersecurity incentive applications will be presumed to raise issues of material fact, and will thus be subject to an evidentiary hearing with an opportunity for discovery. Provided appropriate safeguards are in place, evidentiary hearings and discovery can be conducted in this context—which would provide a critical measure of transparency regarding the use of ratepayer funds—without creating new vulnerabilities in the grid.

3. The case-by-case approach should not be adopted.

The NOPR asks "whether, and if so, how the Commission should implement a case-by-case approach."[88] Under that case-by-case approach, a utility could request an incentive for any expenditure that it claims would materially improve cybersecurity. The Commission would evaluate each request in a separate administrative proceeding, assessing not only utility-specific questions (*i.e.*, whether the expenditure is voluntary for that utility and whether that utility's unique circumstances warrant an incentive for the expenditure), but also questions of general applicability (*i.e.*, whether the proposed technology is consistent with the six sources identified by the NOPR).

The Commission should not adopt such an administratively infeasible case-by-case approach. Individual adjudications are poor vehicles for making generic

[88] *Id.* at P 32.

determinations about whether a cybersecurity technology is "advanced"[89] or whether the technology qualifies under a DHS or DOE framework. Such proceedings generally have less participation from the public, are subject to the Commission's ex parte rules, and are limited to consideration of the specific proposal advanced by a utility.

Not only is the case-by-case approach unworkable, it is also counter-productive. Utilities have regularly informed the Commission that regulatory certainty is needed to facilitate investment in new technologies.[90] But the case-by-case approach would reduce regulatory certainty. An incentive-seeking utility would have no way of knowing in advance whether a particular technology would qualify for an incentive, which would impede the utility's investment decision.[91]

For those reasons, the Commission should not adopt the case-by-case approach contemplated by the NOPR.

H. Any Additions to the PQ List Should be Conducted Through a New Rulemaking Procedure, and New Items

[89] *Id*. at P 2.

[90] *See* Edison Electric Institute, eLibrary No. 20220114-5166 ("The Commission can help address these issues [associated with incentivizing investment in grid-enhancing technologies] by establishing policies that provide regulatory certainty."); Exelon Corp., eLibrary No. 20190528-5161 ("An initiative to revise existing incentives or develop new ones may unintentionally distract resources from what is truly needed to continue making investments in the physical and cyber security of our assets: the regulatory certainty provided by timely and fair Commission action on filings that involve cost recovery and price formation matters.").

[91] In contrast, our proposed approach would give the utility certainty that a particular category of investment—*e.g.* prospective CRISP participation—is likely to warrant an incentive, so long as doing so is voluntary for the utility and would materially improve its cybersecurity posture, which are both within the utility's control.

Should be Added Only if Those Items are Appropriate for Incentive Treatment.

The NOPR asserts that the "Commission would update the PQ List by adding, removing, or modifying cybersecurity expenditures, as needed, via a rulemaking."[92] The NOPR also asserts that "the PQ List will be codified at 35.48(d) of the Commission's regulations."[93] The Commission should confirm, in any final rule, that it will follow its full notice-and-comment procedures for a rulemaking when revising the PQ List.

Notice-and-comment rulemaking is an essential element of the Administrative Procedures Act.[94] It ensures that the public has a full and fair opportunity to weigh in matters of great public importance,[95] which include the security of the grid and rising electricity costs. While regular updating of the PQ List—both to add new technologies and to remove technologies that no longer merit incentives—may be appropriate, the Commission should not seek to expedite the process at the expense of receiving and considering valuable public comment.

The Commission seeks comment in this proceeding on whether additional cybersecurity expenditures should be considered for inclusion on the initial PQ List.[96]

---

[92] NOPR at P 31.

[93] *Id.* at P 25.

[94] *See e.g.*, *Humane Soc'y of the United States v. United States Dep't of Agric.*, 41 F.4th 564, 568–69 (D.C. Cir. 2022) (emphasis added) (explaining that "[e]xcept in limited circumstances" the Administrative Procedures Act's ("APA") rulemaking provision "guarantees the public notice and an opportunity to participate in agency 'rule making.' 5 U.S.C. § 553. The statute defines 'rule making' as an 'agency process for formulating, *amending*, or repealing a rule.' 5 U.S.C. § 551(5). It in turn defines a 'rule' as 'an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy.' 5 U.S.C. § 551(4). *Thus, once an agency makes a rule—that is, once it makes a statement prescribing law with future effect—the APA requires the agency to provide notice and an opportunity for comment before repealing it*.").

[95] *Id*.

[96] NOPR at P 29.

The California Parties do not have any recommended additions at this time (and, as noted above, recommend removing internal network security monitoring from the list). More importantly, the Commission must not add new items to the initial PQ List without giving the public adequate time to comment on such proposals. It would not comply with the spirit or letter of the Administrative Procedures Act to add entirely new items to the initial PQ List without first giving the public notice of the Commission's intent to do so.[97]

When, in the future, the Commission proposes to add new items to the PQ List, we urge the Commission to adhere to the revised eligibility criteria discussed above. Where a new type of expenditure is better implemented through a mandatory standard, as is the case for internal network security monitoring for medium and high impact BES Cyber Systems, the Commission should not adopt incentives for it. New items should be added sparingly, and only after a clear demonstration that adding the item will benefit consumers.

I. The Commission Should Require Utilities Awarded Cybersecurity Incentives to Submit Aggregated Data and Provide Vetted State Officials the Opportunity to Access It.

In addition to the reporting requirements specified in the NOPR,[98] the California Parties urge the Commission to require utilities awarded cybersecurity incentives to submit aggregated data and, consistent with the Commission's CEII regulations, provide vetted state officials access to it. The provision of such data will, in turn, enable the

[97] *Humane Soc'y of the United States v. United States Dep't of Agric.*, 41 F.4th at 568–69.

[98] NOPR at PP 54-56.

relevant state officials to improve the cybersecurity protection of utility assets in their respective states.

IV. CONCLUSION

The California Parties commend the Commission on its efforts to enhance the cybersecurity of the bulk electric system and appreciate the opportunity to submit these Initial Comments.

Dated: November 7, 2022

Respectfully submitted,

By: /s/ *Latif M. Nurani*
Latif M. Nurani

LATIF M. NURANI
AMANDA C. DRENNEN
SPIEGEL & MCDIARMID LLP
1875 Eye Street, NW
Suite 700
Washington, DC 20006
(202) 879-4000
Attorneys for the
California Department of Water Resources

CHRISTINE J. HAMMOND
JONATHAN PAIS KNAPP

By: /s/ *Jonathan Pais Knapp*
Jonathan Pais Knapp

505 Van Ness Ave.
San Francisco, CA 94102
Telephone: (415) 703-1626

Attorneys for the California Public Utilities Commission and the People of the State of California

CERTIFICATE OF SERVICE

I hereby certify that I have on this day caused the foregoing **"INITIAL COMMENTS OF THE CALIFORNIA PUBLIC UTILITIES COMMISSION AND THE CALIFORNIA DEPARTMENT OF WATER RESOURCES STATE WATER PROJECT"** to be served electronically upon each party identified in the official service list compiled by the Secretary of FERC in **Docket No. RM22-19-000.**

Dated at San Francisco, California, this 7th day of November 2022.

/s/ Jonathan Pais Knapp
Jonathan Pais Knapp