Cybersecurity Paradigm Shift: The Risks of Net Neutrality Repeal to Energy Reliability, Public Safety, and Climate Change Solutions

CATHERINE J.K. SANDOVAL*

TABLE OF CONTENTS

 Associate Professor, Santa Clara University School of Law, and Former Commissioner, California Public Utilities Commission. This Article was prepared for the *San Diego Journal of Climate and Energy Law* and the Journal's 2018 Climate and Energy Law Symposium, "Looking Beyond Fossil Fuels in the Trump Era."

I. NET NEUTRALITY REPEAL CREATES A "ZERO-DAY" VULNERABILITY FOR THE ENERGY SECTOR THAT UNDERMINES ENERGY RELIABILITY AND CYBERSECURITY

A. The Cybersecurity Hacker-Paradigm Obscures Systemic Threats to Energy Reliability from Internet Service Provider Network Management after Net Neutrality Repeal

This Article contends that the Federal Communications Commission's (FCC) January 2018 repeal of net neutrality rules created a "zero-day" cybersecurity vulnerability for the energy sector and other critical infrastructure.[1] "A zero-day cybersecurity vulnerability is a previously unknown flaw in a computer program that exposes the program to external manipulation."[2] The flaw may also reside in compromised hardware that creates a "back door" into the internet-connected device.[3] This Article argues that cybersecurity has been primarily viewed from a "hacker paradigm" that obscures systemic threats an Internet Service Provider (ISP) can create to energy reliability and cybersecurity through paid priority and other ISP practices.

The FCC's January 2018 *Internet Freedom Order*[4] repealed net neutrality rules the FCC adopted through its 2015 *Open Internet Order* that prohibited ISPs from blocking, throttling, and paid prioritization of internet traffic—"with some limited exceptions for reasonable network management."[5] Unbridling ISPs from enforceable net neutrality rules triggers energy sector cybersecurity risks. These supply chain risks become systemic risks as the energy sector becomes increasingly intertwined with the internet throughout the energy sector's distributed ecosystem. To protect energy reliability, safety, resiliency, renewable integration, just and reasonable rates, and the environment,

---

1. *See* Critical Infrastructures Protection Act of 2001 (CIPA), Pub. L. 107-56, tit. X, § 1016, 115 Stat. 272, 400 (codified as amended at 42 U.S.C. § 5195) (designating sectors including energy, water, and communications as "critical infrastructure," vital to the nation's economy, national security, and well-being).

2. Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, 11 I/S: J. L. & POL'Y FOR INFO. SOC'Y 405, 408 (2015).

3. Alexandre Vernotte et al., *Load Balancing of Renewable Energy: A Cyber Security Analysis*, 1:5 ENERGY INFOMATICS 29 (2018), https://link.springer.com/content/pdf/10.1186%2Fs42162-018-0010-x.pdf [https://perma.cc/2M6U-3NDN] ("Supply chain attacks are also of great concern, i.e., the compromising of the software/hardware vendor with the objective of feeding rogue updates to assets, typically to install a backdoor.").

4. *In the Matter of Restoring Internet Freedom*, 33 F.C.C. Rcd. 311, at ¶¶ 2–4, 220 (2018) (adopted Dec. 14, 2017, released Jan. 4, 2018) [hereinafter FCC, *Internet Freedom Order*].

5. *In the Matter of Protecting & Promoting the Open Internet*, 30 F.C.C. Rcd. 5601, at ¶¶ 114, 126, 150 (2015), https://docs.fcc.gov/public/attachments/FCC-15-24A1.docx [hereinafter FCC, *2015 Open Internet Order*].

the energy sector and its regulators must address cybersecurity risks including those created by ISPs and FCC regulatory decisions.

Cybersecurity and reliability are mandatory standards under federal law for energy sector facilities and services that participate in federal wholesale energy markets and for transmission facilities and services.[6] The Federal Power Act (FPA) delegates to the Federal Energy Regulatory Commission (FERC) responsibility for reliability including cybersecurity and just and reasonable rates,[7] but the Act does not delegate safety authority to FERC—a gap Congress should address. To fill this gap in the critical safety function, states such as California exercise jurisdiction over electric transmission facilities (whether overhead or underground), for the "limited purpose of protecting the safety of employees and the general public."[8] Distribution system energy utilities must also comply with duties imposed by state law requiring safe, reliable service at just and reasonable rates.[9] In twenty-nine states and three territories, state-regulated energy utilities must comply with renewable energy goals.[10]

The Critical Infrastructures Protection Act of 2001 (CIPA) designated the energy sector as "critical infrastructure" vital to the nation's economy, national security, and well-being.[11] The Electricity Policy Act of 2005 (EPAct) amended

---

6. Catherine J.K. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, 9 SAN DIEGO J. CLIMATE & ENERGY L. 1, at 9–10.

7. *See* 16 U.S.C. § 824(d) (2005); 16 U.S.C. § 824o (2005). *See also* Steven Ferrey, *Pentagon Preemption: The 5-Sided Loss of State Energy and Power*, 2014 U. ILL. J.L. TECH. & POL'Y 393, 404 (2014) (discussing FERC jurisdiction over electricity transmission

8. *See e.g.*, CAL. PUB. UTIL. CODE §§ 8037 (electric overhead facilities), 8056 (electric underground facilities); *Decision Adopting Regulations to Reduce Fire Hazards Associated with Overhead Power Lines and Communication Facilities* (D.12-01-032), CAL. PUB. UTIL. COMM'N, at 11, App. B2 (Jan. 12, 2012) (adopting amendments to CPUC General Order 95, Sec. 11, "to formulate, for the State of California, requirements for overhead line design, construction, and maintenance, the application of which will ensure adequate service and secure safety to persons engaged in the construction, maintenance, operation or use of overhead lines and to the public in general.").

9. *See, e.g.*, CAL. PUB. UTIL. CODE § 451 (2019) ("Every public utility shall furnish and maintain such adequate, efficient, just, and reasonable service, instrumentalities, equipment, and facilities, including telephone facilities, as defined in Section 54.1 of the Civil Code, as are necessary to promote the safety, health, comfort, and convenience of its patrons, employees, and the public.").

10. *State Renewable Portfolio Standards and Goals*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 20, 2018), http://www.ncsl.org/research/energy/renewable-portfolio-standards.aspx [https://perma.cc/6TW9-TZES].

11. *See* Critical Infrastructures Protection Act of 2001 (CIPA), Pub. L. 107-56, tit. X, § 1016, 115 Stat. 272, 400 (codified as amended at 42 U.S.C. § 5195) (designating

the FPA to require electric power grid operators to ensure grid reliability.[12] The EPAct defined reliable operation of the "bulk-power system" (BPS) to ensure, "uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."[13]

The bulk-power system is composed of: "(A) facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof); and (B) electric energy from generation facilities needed to maintain transmission system reliability," but it, "does not include facilities used in the local distribution of electric energy."[14] The EPAct delegated to FERC the authority to create mandatory cybersecurity standards for the entities under its jurisdiction. Under FERC Critical Infrastructure Protection (CIP) rules, "responsible entities" under FERC jurisdiction must observe FERC cybersecurity standards and are subject to penalties for their violation.[15] "All bulk power system owners, operators, and users are required to register with [the North American Electric Reliability Organization (NERC)]."[16] A "responsible entity" is a Registered Entity subject to the CIP mandatory standards."[17]

Local energy distribution systems are under the jurisdiction of state public utility or public service commissions, or local municipal power or irrigation district authorities. In 2012, it was estimated that, "from 80 percent to over 90 percent of grid assets are outside NERC-CIP's scope today."[18] States also have a duty to ensure energy utilities under their jurisdiction provide safe, reliable service, at just and reasonable rates.[19] Illinois Public Utilities Commissioner Sherina Maye Edwards observed that, "[a]s utility infrastructure

---

sectors including energy, water, and communications as "critical infrastructure," vital to the nation's economy, national security, and well-being).

12. Sandoval, *supra* note 6, at 9–10 (citing Energy Policy Act of 2005, Pub. L. 109–58, 119 Stat. 594 (codified as amended at 16 U.S.C. 824o, § 215(b) [hereinafter EPAct).

13. *Id.*

14. *Id.*

15. Susan J. Court, *Role of the Federal Energy Regulatory Commission, A Paper Prepared for the 2014 Law + Informatics Symposium on Cyber Defense Strategies and Responsibilities for Industry*, at 8 n.29 (Feb. 7, 2014), http://courtenergy.com/articles/Court_Working%20Paper_Federal%20Cybersecurity%20Law%20and%20Policy.pdf [https://perma.cc/UEZ2-VH47] [hereinafter Court].

16. *NERC CIP Compliance*, N. AM. ELEC. RELIABILITY COUNCIL (Oct. 26, 2018), http://www.complianceguidelines.com/nerc-compliance.htm [https://perma.cc/3W9T-3VT3] [hereinafter NERC, NERC CIP Compliance].

17. Court, *supra* note 15.

18. ELIZAVETA MALASHENKO, CHRIS VILLAREAL, & J. DAVID ERICKSON, CAL. PUB. UTIL. COMM'M, CYBERSECURITY AND THE EVOLVING ROLE OF STATE REGULATION; HOW IT IMPACTS THE CALIFORNIA PUBLIC UTILITIES COMMISSION iii (2012) [hereinafter *CPUC Staff Report*, *Cybersecurity and the Evolving Role of the States*].

19. *See, e.g.*, CAL. PUB. UTIL. CODE § 451 (2019).

becomes increasingly automated, ensuring the security of critical energy infrastructure is becoming a major concern."[20] Further, companies that "own and operate such assets," must address these risks, as well as, "local, state and federal regulators tasked with ensuring the safety, reliability and cost-effectiveness of the services delivered."[21] Ephram Glass and Victor Glass argued that to make the electric grid more resilient against unforeseen attacks on the electric grid's cyber and physical infrastructure, "the [United States] needs to increase distributed generation to ensure no substations are critical to the stability of the electric grid."[22] To protect American energy reliability and safety, FERC, state, and municipal energy sector regulators must address risks to energy sector reliability, cybersecurity, and public safety triggered by the FCC's repeal of net neutrality rules in the 2018 *Internet Freedom Order*. FERC's review of energy grid resiliency and reliability, *Grid Resilience Order*, 162 FERC ¶ 61,012 (2018) ("Resilience Order") AD18-7-000, must consider harms to grid resiliency and reliability that flow from the FCC's removal of legal bars to ISP paid priority, blocking, throttling, and unreasonable interference with traffic.

The internet is increasingly critical for energy sector management and dispatch of distributed energy resources (DERs) necessary to achieve environmental goals and combat climate change. The electric grid and its changing energy generation mix rely on information and communications platforms, including the internet, for grid planning and operation. While a variety of communications services and facilities can be used to plan, manage, and monitor the electric grid and distributed energy ecosystem, the internet creates important tools for grid visibility and control. The internet also exposes the electric grid to cybersecurity vulnerabilities which the energy sector and regulators must address.

State and federal decisions over the past twenty-five years fostered the creation a "smart grid" that uses information and communications technology (ICT), including the internet, to better manage the electric grid and create

20. Commissioner Sherina Maye Edwards et al., *Opportunities and Challenges for State Utility Regulators Part I*, PUB. UTIL. FORT. (Feb. 2017), https://www.fortnightly.com/fortnightly/2017/02/cybersecurity-part-1?authkey=c4869ac2fb271e063b0930630283c52c7aba2cfba161060eadfcc5121603ca5f [https://perma.cc/XW77-QWTX].

21. *Id.*

22. Ephram Glass & Victor Glass, *Are We One Terrorist Attack Away from a Major Nationwide Blackout, What Should We Do?*, RUTGERS BUS. REV. 8 (2018), https://www.rbusinessreview.org/rbr030204 [https://perma.cc/7AAK-SVR6].

new opportunities for energy users and suppliers.[23] Regulatory and private sector investment decisions have embedded the internet into the energy system, just as electricity is embedded into and required for the functioning of the internet. The "Energy-Internet nexus" enables new energy grid management methods that harness communications and information technology to spur reliability, affordability, safety, and climate change solutions. The Energy-Internet nexus fosters integration of DERs such as solar photovoltaic (PV) systems, energy storage, and demand response supported by smart thermostats and other devices connected through the Internet of Things (IoT).

The California Public Utilities Commission (CPUC) decision in the Water-Energy Nexus proceeding recognized the growing importance of communications, including the internet, for the management of energy, water, and renewable energy integration.[24] The CPUC's 2015 Water-Energy Nexus decision recognizes that "access to reliable communications is increasingly critical to optimize water and energy facility operations and management as our state works to forestall climate change, mitigate or adapt to climate change, and to reduce [greenhouse gas] emissions associated with the electric, natural gas, and water sectors."[25] The following year, CPUC observed that the, "[i]nfrastructure and services to provide both voice and internet communications for data management, transportation, and analysis, including narrowband and broadband signals, are critical to water and energy management, the use of resources, and public safety."[26]

Regulatory and investment decisions that fostered the Energy-Internet nexus created path-dependencies that shape grid investments and operation. Smart grid and other state and federal policies created an Energy-Internet nexus that has become central to energy management, resource integration, reliability, and public safety. These policies and investments embed technology, function, and governance systems for the internet and communications technology into the energy sector. This path-dependence creates new opportunities for grid management and integration, but also makes the energy

---

23. *Cyber and Grid Security*, FED. ENERGY REG. COMM'N (FERC), https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp [https://perma.cc/MCQ9-28N7] ("the electric industry is incorporating information technology (IT) systems into its operations–commonly referred to as smart grid–as part of nationwide efforts to improve reliability and efficiency.").

24. *Decision Regarding Tools for Calculating the Embedded Energy in Water and An Avoided Capacity Cost Associated with Water Savings* (D.15-09-023), CAL. PUB. UTIL. COMM'N, at 4–5 (Sept. 25, 2015) [hereinafter CPUC D.15-09-023]. I served as the CPUC's Assigned Commissioner for the Water-Energy Nexus proceeding from 2014-2016 while serving as a CPUC Commissioner, from 2011 to 2017.

25. *Id.*

26. *Decision Updating the Water Energy Nexus Cost Calculator, Proposing Future Inquiry, and Next Steps* (D.16-12-047), CAL. PUB. UTIL. COMM'N, at 27 (Dec. 15, 2016) [hereinafter CPUC D.16-12-047].

sector vulnerable to ISP and communications network management practices and governance.

Smart grid architecture increasingly depends on the internet as, "the main intermediary to the different stakeholders (along with fiber, GPRS [Ground penetrating radar systems] networks from telecom operators)."[27] Internet governance is crucial to the Energy-Internet nexus. Once data traffic crosses from the network of the energy operator or resource across the firewall to the ISP, the traffic is under ISP control.[28] The ISP controls the user's traffic as it crosses the ISP-controlled gateway to the internet.[29] No software patch or firewall protects a user from an ISP whose job it is to transit that user's content to and from the internet.[30] The "hacker paradigm" predominant in the cybersecurity framework obscures risks from ISP network management practices. The FCC's net neutrality repeal allows ISPs to make deals for traffic priority (i.e., paid priority) even if those transactions slow other internet traffic. An ISP's deals with third parties, including parties the ISP does not recognize to have nefarious motives, could slow or stymie energy sector traffic, portions of which depend on public, non-commercial internet access. Cybersecurity strategies to date focused on firewalls, intrusion detection, and other strategies to keep hackers out. Users cannot throw a firewall over their own ISP. The "hacker paradigm" fails to see ISP-induced risks that traditional cybersecurity strategies leave unmitigated.

This Article contends that federal regulators, responsible entities under the FPA, and state energy sector regulators must act to identify and mitigate risks triggered by the FCC's repeal of net neutrality rules. The energy sector's

---

27. Vernotte et al., *supra* note 3, at 18.

28. *Cf.* Charles Kelly & Philip Carden, *Firewalls: Securing NT Networks from Internet Intruders*, IT PRO TODAY (Oct. 31, 1996), https://www.itprotoday.com/security/firewalls-securing-nt-networks-internet-intruders [https://perma.cc/53J6-XG7C] ("[A] network firewall is a hardware/software barrier between a corporate network and the Internet.").

29. Verizon v. FCC, 740 F.3d 623, 646 ("[T]here appears little dispute that broadband providers have the technological ability to distinguish between and discriminate against certain types of Internet traffic.").

30. Jeff Tyson, *How Internet Infrastructure Works*, HOWSTUFF WORKS (Oct. 21, 2018), http://web.stanford.edu/class/msande91si/www-spr04/readings/week1/Howstuff works.htm [https://perma.cc/2TNA-AV2J] ("Every computer that is connected to the Internet is part of a network, even the one in your home. For example, you may use a modem and dial a local number to connect to an Internet Service Provider (ISP). At work, you may be part of a local area network (LAN), but you most likely still connect to the Internet using an ISP that your company has contracted with."). *Cf.* Vernotte et al., *supra* note 3, at 20 (noting that an energy smart grid cybersecurity, "mechanism can be structural/physical, e.g., a more advanced network segregation, and/or software based, e.g., a more frequent patching strategy.").

state and federal legal duties do not allow it to rely on the market and unenforceable ISP promises to protect reliability, cybersecurity, and public safety. An open and neutral internet—the goal of net neutrality—is necessary to protect energy reliability crucial to America's economy, public safety, national security, and deployment of climate change solutions.

B. Article Overview

Following this introduction, section two of this Article discusses the ISP's gatekeeper position on the internet and introduces the "hacker paradigm" and "cat video paradigm" that pervade internet and cybersecurity regulation. Section three provides an overview of federal energy sector reliability standards, highlighting the states' role in energy reliability for the distribution segment of the energy grid. Section four discusses models for energy sector and critical infrastructure cybersecurity governance. Section five provides an overview of mandatory federal cybersecurity standards for the energy sector's BPS. Section six explores the "hacker-focused" paradigm of many cybersecurity standards including the NERC standards FERC enforces for the energy sector. Section seven examines the Energy-Internet nexus, emphasizing the internet's increasing integration into the energy sector. Section eight discusses simulations that test the electric grid for communications-induced faults and cascading failures. Section nine analyzes the consequences of FERC's net neutrality repeal on energy sector reliability, cybersecurity, renewable energy deployment, and public safety.

Finally, section ten recommends that FERC and state public utility commissions conduct grid simulations to test the effect of ISP-induced communications delays on grid reliability and renewable integration. It recommends that state energy regulators initiate proceedings to examine cybersecurity requirements for distribution-level energy resources. Those proceedings should request data from energy sector jurisdictional entities about ISP contracts and conduct, and then consider whether to limit contracts with such entities to ISPs that observe net neutrality. FERC should examine net neutrality repeal as a cybersecurity, reliability and resiliency risk in its Grid Resiliency and Reliability docket. Federal and state law require energy sector participants and regulators to ensure ISPs do not degrade Energy-Internet traffic or violate market manipulation rules and thereby compromise reliability, public safety, just and reasonable rates, the environment, and realization of climate change solutions.

II. ISPS AS GATEKEEPERS TO THE ENERGY-INTERNET NEXUS: THE HACKER PARADIGM AND THE CAT VIDEO PARADIGM FOR INTERNET REGULATION AND CYBERSECURITY

In the internet's ecosystem, an ISP has "gatekeeper" power to control traffic crossing its network. ISPs that provide "last-mile" access to the internet serve as gatekeepers to the internet for subscribers who use the ISP to send traffic through the internet. The D.C. Circuit observed in *Verizon v. FCC*, "[i]nternet users generally connect to these networks [i]nternet "backhaul" networks composed of long-haul fiber-optic links and high-speed routers capable of transmitting vast amounts of data]—and, ultimately, to one another —through local access providers like petitioner Verizon, who operate the 'last-mile' transmission lines."[31] ISPs operate those "last-mile" networks that provide access to the internet, a network of networks. Further, "[w]hen you connect to your ISP, you become part of their network. The ISP may then connect to a larger network and become part of their network. The [i]nternet is simply a network of networks."[32]

The ISP gatekeeper role underscores the importance of governance structures including enforceable legal rules to cabin internet user vulnerabilities to ISP conduct and contracts. The D.C. Circuit in *Verizon v. FCC* described the internet's process:

> To pull the whole picture together with a slightly oversimplified example: when an edge provider such as YouTube transmits some sort of content—say, a video of a cat—to an end user, that content is broken down into packets of information, which are carried by the edge provider's local access provider to the backbone network, which transmits these packets to the end user's local access provider, which, in turn, transmits the information to the end user, who then views and hopefully enjoys the cat.[33]

The D.C. Circuit's cat video example demonstrates how internet communications travel, but does not capture the increasing use of the internet for critical infrastructure communications including energy sector signals necessary for energy reliability. The "cat video paradigm" obscures the internet's importance to energy, public safety, and democracy. The cat video paradigm creates a frame for viewing internet content that diminishes the importance of communications that rely on public internet access. Likewise, the "hacker paradigm" identified above focuses on the cybersecurity dangers

31. Verizon v. FCC, 740 F.3d 623, 628–29 (2014).
32. Tyson, *supra* note 30.
33. Verizon v. FCC, 740 F.3d 623, 629 (2014).

hackers pose, but it obscures other risks such as those arising from ISP network management.

The D.C. Circuit's 2014 decision in *Verizon v. FCC* recognized the gatekeeper function ISPs occupy: "Because all end users generally access the Internet through a single broadband provider, that provider functions as a 'terminating monopolist,' with power to act as a 'gatekeeper' with respect to edge providers that might seek to reach its end-user subscribers."[34] *Verizon v. FCC* establishes that, "this ability to act as a 'gatekeeper' distinguishes broadband providers from other participants in the internet marketplace—including prominent and potentially powerful edge providers such as Google and Apple—who have no similar "control [over] access to the Internet for their subscribers and for anyone wishing to reach those subscribers."[35]

The FCC's 2015 *Open Internet Order* prohibited ISP practices that took advantage of the ISP's position on the internet as the gatekeeper of traffic that crosses an ISP's network as it transits to and from subscribers and other internet endpoints. The California Independent System Operator (CAISO) which oversees large parts of California's grid under FERC jurisdiction observed, "[t]he same companies that support the retail Internet support the increasingly digitally interconnected North American reliability and energy infrastructure.[36]

As the Energy-Internet nexus grows, the risks ISP priority sales have commensurately grown. Paid priority preference for a video game provider, energy sector participant, or third party could delay or degrade other internet signals—including those used for energy management, operations, and recovery. The 2018 net neutrality repeal, the *Internet Freedom Order*, "imposes no eligibility requirements for paid priority buyers—whether foreign or domestic—and fails to analyze public safety and national security consequences of authorizing paid priority without restriction or FCC jurisdiction.[37]

Federal and state regulators and energy operators with cybersecurity obligations must address these risks to protect energy reliability and cybersecurity. Doing so requires recognition of, and attention to, the power

---

34. *Id.* at 646.

35. *Id.*

36. CAL. INDEP. SYS. OPERATOR, 11 BUSINESS PRACTICE MANUAL FOR DIRECT TELEMETRY 31–32 (2018), https://bpmcm.caiso.com/BPM%20Document%20Library/Direct%20Telemetry/BPM_for_Direct_Telemetry_V11_clean.docx [hereinafter BUSINESS PRACTICE MANUAL FOR DIRECT TELEMETRY].

37. Brief of Amicus Curiae in Support of Petitioners at 10, Mozilla Corp., et al. v. FCC, No. 18-1051 (D.C. Cir. 2018) [hereinafter Amicus Brief] (citing *FCC, Internet Freedom Order*, *supra* note 4, ¶¶ 2–4; Catherine Sandoval, *Reply Comments, In the Matter of Restoring Internet Freedom*, WC Docket No. 17-108, Aug. 30, 2017, at 4, 25, 27, 46 [hereinafter Sandoval, *Internet Freedom Reply Comments*].

of ISPs to undermine energy sector statutory reliability and cybersecurity requirements, as well as state law safety, reliability, and environmental goals.

III. ENERGY RELIABILITY, RESILIENCY, AND STATE ENVIRONMENTAL GOALS

A. Energy Sector Reliability Protects Public Safety, Interconnected Infrastructure, and Achievement of Environmental Objectives

The Energy Sector, constituting a mix of privately owned and public entities, is the only sector that must comply with mandatory federal reliability and cybersecurity duties. In addition, many operators of energy resources and facilities must comply with state law duties requiring safe, reliable service, at just and reasonable rates such as California Public Utility Code 451.[38] The FPA delegates to FERC jurisdiction over interstate electric and natural gas facilities and services, mandating FERC ensure reliability including cybersecurity, and just and reasonable rates.[39] The FPA does not specifically delegate safety duties to FERC, a gap in federal jurisdiction filled in part by other federal agencies and in part by the states. California regulates electric transmission and distribution facilities to ensure public and worker safety.[40]

The energy sector's role as a key enabler of the economy, public safety, and national security animate federal energy sector reliability laws adopted in the 2005 EPAct.[41] Using the police power of the state inherent in America's federalist system, many states impose reliability and safety standards on electric utilities to protect and promote the population's well-being and

38. CAL. PUB. UTIL. CODE § 451 (2019); State ex rel. Utils. Comm'n v. Carolina Power & Light Co., 174 N.C. App. 681, 684-85 (N.C. Ct. App. 2005) (noting that North Carolina's Supreme Court "stated that the Utility Commission's purpose [of this regulation] 'was to provide a mechanism through which [the Utility Commission] meaningfully could' . . . . 'take appropriate action . . . to secure and protect reliable service to retail customers in North Carolina.'" North Carolina General Statutes §§ 62–30 and 62–32(b) "give the Utility Commission 'all powers necessary' to regulate public utilities to ensure the citizens of this State are provided with reasonable service."); Rochester v. People's Coop. Power Ass'n, 483 N.W.2d 477, 479 (Minn. 1992) ("In 1974 the legislature enacted what is now chapter 216B, entitled 'Public Utilities,' prefacing the chapter with a 'legislative finding,' announcing its statement of purpose—to provide the retail consumers of natural gas and electric service in this state with adequate and reliable services at reasonable rates. . . ."); MINN. STAT. § 216B.01 (1990)).

39. 16 U.S.C. § 824(d) (2005); 16 U.S.C. § 824 (2005).

40. CAL. PUB. UTIL. CODE §§ 8037 (electric overhead facilities), 8056 (electric underground facilities); CPUC D.12-01-032, *supra* note 8, at 11, App. B2.

41. EPAct, *supra* note 12.

the state's economic, health, educational, and other interests.[42] The 2017-2018 blackout in Puerto Rico left many parts of the island without power for many months and with sporadic power even after repairs were attempted. "The failures of water treatment and delivery following the loss of power in Puerto Rico, illustrate the interconnection between electricity and other critical infrastructure services."[43] Such significant utility failures after a destructive hurricane highlight the societal and economic consequences of power loss over an extended period of time, as well as the imperative of energy sector reliability and safety. Climate change analysis predicts storm intensity will increase as waters warm while drought conditions raise wildfire risk,[44] underscoring the imperative of energy reliability to forestall and address disaster risk.

The electric grid's interconnected design enables its reach to customers and dispatch of distributed energy resources, but also makes it vulnerable to local or even cascading outages. Water systems, gas pipelines, and related infrastructure are interdependent with the electric grid and the energy services it provides. Each of these utility infrastructure systems increasingly depend on the internet for system function and reliability. Mackinnon Lawrence & Jan Vrins observed that "one-off technologies are recombining into

---

42. *See, e.g.*, Duquesne Light Co. v. Barasch, 488 U.S. 299, 307 (1989) ("'[e]very public utility shall furnish and maintain adequate, efficient, safe, and reasonable service and facilities'" and "'[s]uch service also shall be reasonably continuous and without unreasonable interruptions or delay.'") (quoting 66 PA. CONS. STAT. § 1501 (1986)).

43. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 12; U.S. GLOBAL CLIMATE CHANGE RES. PROGRAM, Fourth National Climate Assessment, Vol. II, 47 (2018), https://nca2018.globalchange.gov/ [https://perma.cc/MR44-3M8C] ("In the U.S. Caribbean, Hurricanes Irma and Maria caused catastrophic damage to infrastructure, including the complete failure of Puerto Rico's power grid and the loss of power throughout the U.S. Virgin Islands, as well as extensive damage to the region's agricultural industry.").

44. U.S. GLOBAL CLIMATE CHANGE RES. PROGRAM, *supra* note 43, at 74 ("Increases in greenhouse gases and decreases in air pollution have contributed to increases in Atlantic hurricane activity since 1970. In the future, Atlantic and eastern North Pacific hurricane rainfall and intensity are projected to increase, as are the frequency and severity of landfalling 'atmospheric rivers' on the West Coast."); *id.* at 91 ("conditions conducive to the very large wildfires that have already increased in frequency across the western United States and Alaska since the 1980s."); Terry Dinan, *Projected Increases in Hurricane Damage in the United States: The Role of Climate Change and Coastal Development*, 138 ECOLOGICAL ECON. 186, 186 (2017) ("Climate change is likely to increase the frequency of the most intense categories of hurricanes in some parts of the world, including the North Atlantic Basin, and is expected to increase sea levels, leading to more destructive storm surges when hurricanes occur."). *See also* GOVERNOR NEWSOM'S STRIKE FORCE, WILDFIRES AND CLIMATE CHANGE, CALIFORNIA'S ENERGY FUTURE (Apr. 12, 2019), https://www.gov.ca.gov/wp-content/uploads/2019/04/Wildfires-and-Climate-Change-California%E2%80%99s-Energy-Future.pdf [https://perma.cc/ELN3-MX2B] ("Warmer temperatures, variable snowpack, and earlier snowmelt caused by climate change make for longer and more intense dry seasons, leaving forests more susceptible to severe fire.").

complex hybrid energy ecosystems supported by rapidly evolving technology platforms: integrated DER, transportation-grid nexus, buildings-to-grid, smart cities, energy Internet of Things, and transactive energy, for example."[45]

The Energy-Internet nexus exemplifies infrastructure interdependence that creates new opportunities for grid and resource management as well as new vulnerabilities. The stakes of ISP governance and net neutrality policies are highlighted by policy and management decisions designed to embed the internet into the distributed energy ecosystem's processes and function. The FCC's changes in ISP governance through its 2018 net neutrality repeal also created new cybersecurity, reliability, and safety vulnerabilities for critical infrastructure including the electric, natural gas, and water sectors.

B. Critical Infrastructure; Reliability, Physical Security, and Cybersecurity Regulations

President Clinton's 1996 Executive Order 13010 recognized the need to protect the nation from physical and cyber threats to "critical infrastructure" sectors including energy.[46] Executive Order No. 13010 recognized that, "[c]ertain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."[47] This Executive Order designated as critical infrastructure sectors, "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government."[48]

The Critical Infrastructures Protection Act of 2001 (CIPA) was adopted as part of the U.S.A. Patriot Act following the September 11, 2001, terrorist attack on America.[49] CIPA defines critical infrastructure as those, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or

45. Mackinnon Lawrence & Jan Vrins, *Unleashing Utility Innovation*, PUB. UTIL. FORT. 56, 58 (July 2017).

46. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 7.

47. *Id.* (citing Exec. Order No. 13010, 61 Fed. Reg. 37347, 1996 WL 33673768 (July 15, 1996)).

48. *Id.*

49. *See* Critical Infrastructures Protection Act of 2001 (CIPA), Pub. L. 107-56, tit. X, § 1016, 115 Stat. 272, 400 (codified as amended at 42 U.S.C. § 5195).

safety, or any combination of those matters."[50] Specifically, CIPA, "defines critical infrastructure *not* with reference to the identity of the target, but by the consequences of an attack on it."[51]

In 2005 President George W. Bush signed the Energy Policy Act (EPAct) to promote, "dependable, affordable, and environmentally sound production and distribution of energy for America's future."[52] EPAct amended the FPA to require electric power grid operators to ensure grid reliability and cybersecurity.[53]

Under the FPA, "reliable operation" means, "'operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements,' articulating resilience concepts."[54] Section 215 of the FPA requires FERC to certify an Electric Reliability Organization (ERO) to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. In July 2006, FERC certified the North American Electric Reliability Corporation (NERC) as the ERO authorized to establish bulk transmission system standards for planning, preparation, contingency, and operations.[55] Susan Court, former Director of FERC's Office of Enforcement, noted that since the EPAct's passage, FERC "has approved over 100 mandatory Reliability Standards," including "over 1,000 separate requirements," and NERC, "has registered 1,646 users, owners, and operators for a total of 4,782 functions."[56] FERC may enforce reliability standards, as may NERC, subject to FERC oversight.[57]

---

50. *Id.*

51. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 8 (citing Nicholas Bagley, *Benchmarking, Critical Infrastructure Security, and the Regulatory War on Terror*, 43 HARV. J. ON LEGIS. 47, 51 (2006)).

52. George W. Bush, *Statement on Signing the Energy Policy Act of 2005*, THE AM. PRESIDENCY PROJECT (Aug. 8, 2005), http://www.presidency.ucsb.edu/ws/?pid=64861 [https://perma.cc/QP9A-UB75].

53. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 9–10 (citing EPAct, *supra* note 12).

54. Comments and Responses of PJM Interconnection L.C.C., *Grid Resilience in Regional Transmission Organizations and Independent System Operators*, F.E.R.C. Docket No. AD-18-7-000 (Mar. 9, 2018) at 11 (citing FPA § 215, U.S.C. § 824o(a)(4)), https://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx [https://perma.cc/YX2N-T482] [hereinafter PJM, *FERC Grid Resilience Comments*].

55. Amy L. Stein, *Regulating Reliability*, 54 HOUS. L. REV. 1191, 1217 (2017).

56. Court, *supra* note 15, at 6.

57. Order No. 843, *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 — Cyber Security — Security Management Controls*, 163 F.E.R.C ¶ 61,032 (2018) [hereinafter *FERC Order No. 843*].

NERC developed "Adequate Level of Reliability" standards for design, planning, and operation of the Bulk Electric System (BES). These standards address "Reliable Operation of the BES" over four time frames:

> (1) steady state (the period before a disturbance and after restoration has achieved normal operating conditions); (2) transient (the transitional period after a disturbance and during high-speed automatic actions in response); (3) operations response (the period after the disturbance where some automatic actions occur and operators act to respond); and (4) recovery and system restoration (the time period after a widespread outage through initial restoration to a sustainable operating state and recovery to a new steady state).[58]

These time periods "correspond to the four outcome-based abilities of both the [National Infrastructure Advisory Council] NIAC resilience framework and the [FERC] Commission proposed definition of resilience: (1) robustness; (2) resourcefulness; (3) rapid recovery; and (4) adaptability."[59]

These mandatory federal BES reliability standards complement state reliability standards for the electric grid distribution network. Further, reliability and cybersecurity are critical to achievement of environmental goals and climate change solutions. It is key to keep these frameworks in mind, as energy development, dispatch, and grid management techniques increasingly rely on the open internet to harness renewable resources and minimize the need for fossil-fuels.

C. Energy Sector Environmental Goals Promote Reliability and Resilience

Fossil fuel consumption has been identified as major contributor to CO2 emissions that contribute to climate change.[60] The United Nations

58. Comments and Responses of North American Electric Reliability Corporation (NERC), *Grid Resilience in Regional Transmission Organizations and Independent System Operators*, F.E.R.C. Docket No. AD-18-7-000 (Mar. 9, 2018) at 5–6, https://pjm.com/-/media/documents/ferc/filings/2018/20180309-ad18-7-000.ashx [https://perma.cc/ESM3-SWAN] [hereinafter *NERC Grid Resilience Comments*].

59. Comments of the North American Electric Reliability Corporation (NERC), *Grid Resilience in Regional Transmission Organization and Independent System Operators*, F.E.R.C. Docket No. AD18-7-000 (May 9, 2018), at 5–6, https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Resilience%20Proceeding%20Comments%20(AD18-7).pdf [https://perma.cc/JG5U-HC3D].

60. *See e.g.*, *What Is Climate Change*, ENERGY UPGRADE CAL., https://www.energyupgradeca.org/climate-change/ [https://perma.cc/PP6E-WP2D] ("When fossil fuels are burned, carbon dioxide, methane and other greenhouse gases are released into the air. These greenhouse gases, such as methane, are also released during fossil fuel extraction and transportation.

Intergovernmental Panel on Climate Change (IPCC) issued a report in October 2018 that recommended dramatic efforts to limit global warming to 1.5 degrees over pre-industrial levels, as opposed to the 2 degree warming goal set in the Paris Climate Accord.[61] The IPPC report contends "the consequences of 1°C of global warming through more extreme weather, rising sea levels and diminishing Arctic sea ice, among other changes" highlight the need for swift action to slow global warming and climate change.[62]

Likewise, the State of Massachusetts found that, "the electric sector accounts for approximately twenty percent of [s]tatewide greenhouse gas emissions."[63] By Executive Order, the Governor of Massachusetts in 2017 established, "annually declining aggregate carbon dioxide emissions limits on electricity generating facilities located in the Commonwealth, pursuant to § 3(d)."[64] Further, "[t]wenty-nine states, Washington, D.C., and three territories have adopted [Renewable Portfolio standards (RPS)], while eight states and one territory have set renewable energy goals."[65] Iowa was the first state to establish an RPS, and Hawaii and California have adopted 100% renewable energy standards to be achieved by 2045.[66]

California's energy sector RPS began in 2002 when California Governor Davis signed SB 1078, requiring the state to achieve a twenty percent RPS by 2017.[67] In 2006, Governor Schwarzenegger required twenty percent of electricity retail sales to be fulfilled by renewable energy resources by 2020.[68] Then, in 2011, Governor Brown signed SB X1-2, requiring that thirty-three percent of all electricity come from renewable energy generation resources by 2020. In 2015, California adopted SB 350 which increased

---

Carbon dioxide isn't harmful at natural levels, but too much can act like a layer of plastic wrap around the Earth that lets in heat from the sun but doesn't let it escape. The atmosphere acts like a greenhouse, which is why these emissions are called greenhouse gases."); *California Greenhouse Gas Inventory, 2018 Edition*, CAL. AIR RES. BD., https://www.arb.ca.gov/cc/inventory/data/data.htm [https://perma.cc/B5PU-PYMV].

61. *Summary for Policymakers of IPCC Special Report on Global Warming of 1.5°C Approved by Governments*, INTERGOVERNMENTAL PANEL ON CLIMATE CHANGE (Oct. 6, 2018), http://www.ipcc.ch/ [https://perma.cc/Z42A-HAJM].

62. *Id.*

63. New England Power Generators Ass'n, Inc. v. Dep't of Envtl. Prot., 480 Mass. 398, 405–06 (2018).

64. *Id.* at 403–04 (citing 310 MASS. CODE REGS. § 7.74(1)).

65. *State Renewable Portfolio Standards and Goals*, NAT'L CONF. OF ST. LEGISLATURES (Jan. 20, 2018), http://www.ncsl.org/research/energy/renewable-portfolio-standards.aspx [https://perma.cc/SWC3-BBKB].

66. *Id.*; S.B. 100, ch. 312 (Cal. 2018).

67. S.B. 1078, ch. 516 (Cal. 2002) (amending CAL. PUB. UTIL. CODE § 399.12(b) (Deering 2003)).

68. S.B. 107, ch. 464 (Cal. 2006), http://www.energy.ca.gov/portfolio/documents/documents/sb_107_bill_20060926_chaptered.pdf [https://perma.cc/WM9L-7R4D].

the energy RPS requirements to fifty percent by 2030 to reduce energy sector Greenhouse gas emissions.[69] SB 350 emphasized the integration of demand-side tools to reduce the need to build and run fossil-fueled plants, and it required strategies to reduce the environmental burden of energy on disadvantaged communities.[70] Most recently, in 2018, Governor Brown signed SB 100 which set a goal of one hundred percent renewable energy for all of California's electric generation by 2045.[71]

Climate change also poses threats to the energy sector as a whole, including its infrastructure, reliability, safety, and its ability to ensure just and reasonable rates. In 2014, the Union of Concerned Scientists identified several consequences of climate change for the energy sector including: accelerating sea level rise; increasing wildfires; more frequent and intense heat waves; droughts and reduced water supplies; and elevated water temperatures.[72]

D. Resilience as a Component of Reliability under the Federal Power Act

As the authority over matters of reliability and adequacy, and, "[w]ith the asserted goal of improving electric grid resiliency and reliability, FERC issued a Notice of Proposed Rulemaking (NOPR) on October 10, 2017, proposing a Grid Resiliency Pricing Rule."[73] The "Grid Reliability NOPR cited the 'premature' retirement of several coal-fired and nuclear plants as the basis for its concerns that grid resiliency is threatened."[74] In

69. S.B. 350, ch. 547 (Cal. 2015).

70. *Id.* (citing CAL. HEALTH & SAFETY CODE § 39711 (Deering 2014)). The term disadvantaged communities, "refers to the areas throughout California which most suffer from a combination of economic, health, and environmental burdens. These burdens include poverty, high unemployment, health conditions like asthma and heart disease, as well as air and water pollution, and hazardous wastes." DISADVANTAGED COMMUNITIES, CAL. PUB. UTIL. COMM'N, https://www.cpuc.ca.gov/discom/ [https://perma.cc/CC6P-43HS].

71. S.B. 100, ch. 312 (Cal. 2018).

72. *How Climate Change Puts Our Electricity at Risk*, UNION OF CONCERNED SCIENTISTS (Apr. 2014), https://www.ucsusa.org/global_warming/science_and_impacts/impacts/effects-of-climate-change-risks-on-our-electricity-system.html [https://perma.cc/GK2K-VBZL]. *See also*, U.S. GLOBAL CLIMATE CHANGE RES. PROGRAM, *supra* note 43, at 30 ("Climate change and extreme weather events are expected to increasingly disrupt our Nation's energy and transportation systems, threatening more frequent and longer-lasting power outages, fuel shortages, and service disruptions, with cascading impacts on other critical sectors.")

73. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 28 (citing Grid Resiliency Pricing Rule, 82 Fed. Reg. 46,940, 46,941–42 (proposed Oct. 10, 2017) (to be codified at 18 C.F.R. pt. 35)).

74. *Id.*

January 2018, FERC rejected the United States Department of Energy's (DOE) proposal to divert more funds to coal, nuclear, and other fossil fuel power plants with ninety days fuel on-hand—a proposal that argued adopting such policies would promote grid resiliency and reliability.[75] FERC concluded DOE's proposal was inconsistent with the FPA's threshold requirement for, "a showing that the existing RTO/ISO tariffs are unjust, unreasonable, unduly discriminatory or preferential."[76] Any remedy proposed after such a showing is made must, "be shown to be just, reasonable, and not unduly discriminatory or preferential."[77] DOE's proposal addressed neither of these required legal prongs of FPA analysis.

After rejecting the DOE's proposal, FERC initiated a new proceeding, Docket No. AD18-7-000, "to take additional steps to explore resilience issues in the [Regional Transmission Organizations (RTOs)]/[Independent System Operators (ISOs)]."[78] FERC explained the proceeding aimed:

> (1) to develop a common understanding among the Commission, industry, and others of what resilience of the bulk power system means and requires; (2) to understand how each RTO and ISO assesses resilience in its geographic footprint; and (3) to use this information to evaluate whether additional Commission action regarding resilience is appropriate at this time.[79]

FERC also asked ISOs and RTOs to report on reliability concerns and resilience concepts.[80]

FERC proposed to define resilience as the, "ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event."[81] PJM, a Mid-Atlantic RTO, offered an alternative definition of resilience: the "ability of the system to withstand or quickly recover from events that pose operational risks."[82]

PJM's comments on FERC's resiliency docket asked FERC to clarify whether resilience is anchored in the Congressional definition of reliable operations and just and reasonable rates set forth in FPA section 215.[83]

---

75. *Order Terminating Rulemaking Proceeding, Initiating New Proceeding, and Establishing New Procedures*, 162 F.E.R.C. ¶ 61,020, at ¶¶ 2, 14 (2018).

76. *Id.* at ¶ 14 (citing 16 U.S.C. § 824e(a) (2012)); *see also, e.g.*, Emera Maine v. FERC, 854 F.3d 9, 25 (D.C. Cir. 2017) ("Without a showing that the existing rate is unlawful, FERC has no authority to impose a new rate.")).

77. *Id.*

78. *Id.*

79. *Id.* at ¶ 18.

80. *Id.* at ¶¶ 23–27.

81. *Id.* at ¶ 23.

82. *FERC Grid Resilience Comments*, *supra* note 54, at 12 (citing FPA, section 217, 16 U.S.C. § 824q(b)(3)(B)(4)).

83. *Id.*

NERC argued that resilience is a component of reliability in relation to an event and is thus an implicit feature of NERC's activities under FERC jurisdiction.[84]

This Article agrees with NERC and PJM that resilience, as defined in FERC's proposal, should be interpreted as a component of reliability under FPA section 215.[85] This Article will thus analyze resiliency as a component of FPA and state utility reliability duties.

IV. ENERGY SECTOR CYBERSECURITY GOVERNANCE PROTECTS ENERGY RELIABILITY AND SAFETY

A. Defining Cybersecurity for the Energy-Internet Ecosystem

Federal, state, public, and private sector decisions to integrate the internet into the energy system's operation have enabled new energy resources and opportunities. David M. Driesen observed that, "decisionmaking by institutions is 'path dependent.' Past actions and decisions tend to constrain the range of attractive future decisions."[86] Energy-Internet development and investment reflect path-dependent decisions that embed technologies, governance, and vulnerabilities into the grid, while infusing new grid management options.

The path-dependency of Energy-Internet nexus investments increases ISP incentives to exploit their position at the internet's gateway. The mandatory nature of energy cybersecurity and reliability highlights the need to address vulnerabilities that may compromise reliability, resiliency, just and reasonable rates, and climate change solutions. According to Jeff Kosseff, "[c]ybersecurity focuses not only on the protection of data, but also on the systems and networks of the public and private sector."[87] Kosseff identifies confidentiality, integrity, and availability as the "CIA Triad"—the industry's frame for categorizing cyberattacks:

> Confidentiality refers to the "the prevention of unauthorized disclosure of information." Confidentiality often is associated with data breaches because attackers seek to obtain information without proper authorization. Integrity refers to "the guarantee that the message that is sent is the same as the message received and that the message is not altered in transit" . . . . Availability refers to "the guarantee that information

84. *NERC Grid Resilience Comments, supra* note 58, at 5–6.
85. The appropriate definition of energy sector resiliency is beyond this Article's scope.
86. David M. Driesen, *The Economic Dynamics of Environmental Law: Cost-Benefit Analysis, Emissions Trading, and Priority-Setting*, 31 B.C. ENVTL. AFF. L. REV. 501, 510 (2004).
87. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 995 (2018).

> will be available to the consumer in a timely and uninterrupted manner when it is needed regardless of [the] location of the user." A [Distributed Denial of Service] attack that knocks a popular website offline, for example, is an attack on that site's availability.[88]

The "CIA Triad" forms a lens through which cybersecurity risks and goals are viewed. This lens, like glasses that need a prescription update, embeds a hacker focus that underplays risks from parties who operate the communications systems upon which the organization depends. The hacker focus is a crucial component of this framework. It becomes evident in cybersecurity tests, such as the DOE's Idaho National Laboratory 2007 simulation of a cyber-attack on an energy facility which, "exploited a vulnerability at the facility by altering the timing of a diesel generator's circuit breakers, causing thick smoke to rise from the plant."[89]

Cybersecurity strategies to date sought to prevent cyber-attacks by disconnecting, "critical elements of the electricity industry's infrastructure" through air-gaps and isolation.[90] Amy Stein argues that internet isolation strategies are, "a problematic suggestion as the smart grid initiatives seek to further interconnect the grid."[91] Over the past decade, Energy-Internet integration has gone beyond smart meters and extended the smart grid to behind the meter customer-side resources such as thermostats, batteries, and solar systems. Such integration enables new modes of planning, operating, and repairing the electric grid. It necessarily enables DER visibility that facilities grid operation, dispatch, and adjustments to maintain voltage, frequency, and other grid services. Visibility and control are critical to the energy sector as failures in one part of the energy system can lead to cascading energy reliability issues and blackout.[92] Energy-Internet integration is imperative for the vigilant and adaptive cybersecurity necessary to protect grid reliability and safety.

B. Cybersecurity Governance: Mandates, Cooperation, and Incentive/Risk-Based Models

Cybersecurity governance debates have focused on whether incentive and risk-based cooperative models are preferable to government mandates. Jeff Kosseff argues for a cybersecurity legal framework that combines penalties and incentives to encourage companies to adopt cybersecurity safeguards, rather than one based, "entirely of coercion or entirely of

88. *Id.* (footnotes omitted).
89. Stein, *supra* note 55, at 1230–31.
90. *Id.*
91. *Id.*
92. *See, e.g.*, Chih-Che Sun, Adam Hahn, & Chen-Ching Liu, *Cyber Security of a Power Grid: State-of-the-Art*, 99 ELEC. POWER & ENERGY SYS. 45, 45–56 (2018).

cooperation."[93] Kosseff observed that a "regulatory model based on coercion and deterrence" assumes robust government oversight through, "extensive government monitoring and inspections coupled with penalties for observed violations."[94] Such a system requires penalties for noncompliance sufficient to encourage investment in compliance, even when doing so required firms to "forego potential revenue."[95]

John J. Chung characterizes cybersecurity protection of Critical Infrastructure as a "public good," observing that, "[i]n general, public goods are things or situations that provide a widespread benefit available to all," but "a market economy faces inherent barriers to providing public goods."[96] "[A]ny person providing a public good is unable to capture the full economic benefit or profit of providing the good," creating, "little economic or profit incentive to do so, which results in the less than optimal supply of such goods."[97]

Chung argues, "[m]any companies that operate critical infrastructure tend to underinvest in cyber-defense because of negative externalities, positive externalities, free riding, and public goods problems—the same sorts of challenges the modern administrative state encounters in a variety of other contexts."[98] He further contends that, "[t]he market, by itself, is unable to provide sufficient incentives for an optimal amount of spending on cybersecurity."[99] Notably, Chung is not alone in his contentions.

Michael Garcia, David Forscey, and Timothy Blute contend, "the core challenge for state cybersecurity professionals today is not technical; the cutting edge of cybersecurity is governance."[100] They define governance as the, "formal and informal institutions that [influence how] a group of people determine what to decide, how to decide, and who shall decide."[101] They further note that in, "academic literature and corporate guidelines, cybersecurity governance is commonly described as the process through which humans understand organizational risk, prioritize resources, and establish procedures

93. Kosseff, *supra* note 87, at 1006.
94. *Id.* at 1001–02.
95. *Id.* at 1002.
96. John J. Chung, *Critical Infrastructure, Cybersecurity, and Market Failure*, 96 OR. L. REV. 441, 451 (2018).
97. *Id.*
98. *Id.* at 470.
99. *Id.*
100. Michael Garcia, David Forscey, Timothy Blute, *Beyond the Network: A Holistic Perspective on State Cybersecurity Governance*, 96 NEB. L. REV. 252, 253–54 (2017).
101. *Id.* at 257.

to erect technical defenses against computer-based attacks."[102] However, cybersecurity governance policies must also resist silos and repetition of paradigms tailored to past risks. Adaptive cybersecurity governance must further consider risks introduced by governance of other sectors. Regulation or forbearance from regulation of ISPs who transmit data critical infrastructure uses to execute its functions introduces cybersecurity risks that should be considered in regulatory decision-making and energy system governance and operation.

Beyond those mentioned above, Garcia, Forscey, and Blute argue for an, "expansive role for states in the broader cybersecurity ecosystem, one that obligates state officials to do more than defend state networks."[103] They contend, "[s]tates have a fundamental responsibility to protect constituents, including interstate businesses, from day-to-day cyber attacks and to prepare public and private institutions for a widespread cyber disruption."[104]

The CPUC's 2012 staff report, *Cybersecurity and the Evolving Role of State Regulation; How it Impacts the California Public Utilities Commission*, observed that, "[a]s the State moves forward with grid modernization, utilities must design and implement both cyber and physical security policies that protect public safety, enhance the reliability and resiliency of the grid and protect customer privacy from cyber threats, and do so cost-effectively."[105] In 2016, the CPUC and the California Governor's Office of Emergency Services (Cal OES), "entered into a Memorandum of Understanding (MOU) . . . to coordinate agency efforts in assuring the safety and reliability of utility systems from cyber security threats."[106] This level of state coordination, "requires [CPUC] to focus not just on physical security and system resiliency/ safety of the utility system, but also on cyber threats, because, as reliance on digital technology in utility systems continues to increase, the cyber security of network assets is more critical than ever."[107] In 2017, the CPUC committed to implementing a Staff Cybersecurity Group strategy designed to address the Risk Management pillar of its safety action plan.[108]

States are increasingly recognizing the importance of cybersecurity to energy and other utilities under their jurisdiction. The federalist system

---

102. *Id.* at 254.
103. *Id.*
104. *Id.*
105. *CPUC Staff Report, Cybersecurity and the Evolving Role of the States*, *supra* note 18, at iv.
106. *Id.* at 5.
107. *Id.*
108. CAL. PUB. UTIL. COMM'N, 2017 UPDATE, SAFETY ACTION PLAN AND REGULATORY STRATEGY, IMPLEMENTATION OF THE SAFETY POLICY STATEMENT 2 (2017), http://www.cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Other/2017_Safety_Action_Plan.pdf [https://perma.cc/27GM-VH7E] [hereinafter CPUC, *2017 Safety Action Plan Update*].

of the United States reserves police power to the states to, "legislate with regard to protection of the lives, limbs, health, comfort, and quiet of all persons."[109] The CPUC's comments opposing net neutrality's repeal stressed the statutory obligations of CPUC and California's utilities, "to protect the safety and health of the public. Protection of public safety is a core exercise of a state's police power."[110] States, the federal government, and the energy sector must analyze cybersecurity threats to energy and other critical infrastructure posed by FCC's repeal of net neutrality rules.

V. FEDERAL CYBERSECURITY MANDATES FOR THE ENERGY SECTOR AND STATE LAW ENERGY SECTOR RELIABILITY AND SAFETY DUTIES

A. Recognizing and Protecting Critical Infrastructure

Laws recognizing the importance of critical infrastructure—including energy, water, communications, national security, health care, and other economic sectors—served as the foundation for mandatory energy sector cybersecurity rules. Congress' 2001 adoption of CIPA expressed United States policy, "that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States."[111]

The Homeland Security Act of 2002 established the Department of Homeland Security (DHS) as the coordinator to protect computer systems that support critical infrastructure.[112] The Act tasks DHS with: (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States; (2) recommending measures to protect

109. Sandoval, *supra* note 6, at 68 (citing Gonzales v. Oregon, 546 U.S. 243 (2006)).

110. CAL. PUB. UTIL. COMM'N, Comments, *In the Matter of Restoring Internet Freedom*, WC Docket No. 17-108, at 5, https://ecfsapi.fcc.gov/file/107172199528427/WC%20Docket%20No.%2017-108%20CPUC%20Comments%20on%20Restoring%20Internet%20Freedom.pdf [https://perma.cc/52QC-MVA9] [hereinafter CPUC, Comments, *In the Matter of Restoring Internet Freedom*]. Police power is an attribute of a state's sovereignty and is an essential element of the power to govern, which is reserved to the states. 72 AM. JUR. 2d States, etc. § 21.

111. Sandoval, *supra* note 6, at 8 (citing 42 U.S.C. § 5195c(e)).

112. Homeland Security Act of 2002, Pub. L. No. 107-296 (2002); GOV'T ACCT. OFF. (GAO), CRITICAL INFRASTRUCTURE PROTECTION, DEPARTMENT OF HOMELAND SECURITY FACES CHALLENGES IN FULFILLING CYBERSECURITY RESPONSIBILITIES (2005) [hereinafter, GAO, *Critical Infrastructure Protection*].

key resources and critical infrastructure of the United States; and (3) disseminating, as appropriate, information to assist in the deterrence, prevention, preemption of, or response to terrorist attacks.[113] Homeland Security Presidential Directive 7 (HSPD-7) designates federal agencies as lead points for critical infrastructure sectors, and designates the DOE as the lead for the energy sector including electricity and oil and natural gas.[114]

President George W. Bush's 2003 report, *The National Strategy to Secure Cyberspace*, built on CIPA's requirements to protect the cyber and physical security of critical infrastructure.[115] Per the report, American, "critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping."[116] The report further observed that, "[c]yberspace is their nervous system—the control system of our country."[117] The report recommended public-private partnerships to foster cybersecurity, specifically arguing, "[i]n general, the private sector is best equipped and structured to respond to an evolving cyber threat."[118]

Private sector initiatives, public-private partnerships, and market driven approaches to cybersecurity leave incentive and investment gaps in cyber protection. Market participants, suppliers, insiders, or third parties (including nation-states and adversaries with different incentives or regulatory constructs) may seek to exploit these gaps to increase profits or for ulterior motives. Scholars Eldar Haber and Tal Zarsky argue, "it is undisputable that [critical infrastructures] require proactive protection from cyber attacks" and that "a market-based approach, which has many advantages, cannot provide adequate protection on its own. Providing mere ex post incentives are also insufficient."[119] Haber and Zarsky describe, "three central failings of the market-based approach: *inadequate information sharing, lack of knowledge transfers*, and *underinvestment*."[120] They contend, "the current U.S. CIP approach is misguided and should be thoroughly reexamined," arguing for

113. GAO, *Critical Infrastructure Protection, supra* note 112, at 18–19.
114. *Id.* at 20.
115. The White House, NATIONAL STRATEGY TO SECURE CYBERSPACE 1 (2003) https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf [https://perma.cc/5ZMC-55NE].
116. *Id.* at vii.
117. *Id.*
118. *Id.* at ix.
119. Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. ST. U.L. REV. 516, 573 (2018).
120. *Id.* (emphasis in original).

a larger role of the states in CIP protection, and a centralized agency for CIP protection."[121]

Despite such consequential effects of lackluster cybersecurity frameworks, cybersecurity remains voluntary for all critical infrastructure sectors except for the FERC-jurisdictional energy sector. This Article recommends that the energy sector, state public utility commissions and legislatures evaluate whether cybersecurity should be mandatory for the portions of the energy sector under state jurisdiction. Such a review should also examine state cybersecurity governance to achieve safe and reliable utility service. For the FERC-jurisdictional energy sector, the EPAct of 2005 made cyber security mandatory and subject to FERC enforcement.

B. Mandatory Cybersecurity for the Energy Sector

Integration of communications and information technology, including the internet, into the electric sector renders cybersecurity crucial to public safety, energy reliability, and national security. The Government Accounting Office observed in 2005 that, "[s]ince September 11, 2001, the critical link between cyberspace and physical space has been increasingly recognized."[122] In March 2005, "security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems."[123] Nonetheless, thirteen years later, the energy sector is still fending off hackers.

Mandatory reliability and cybersecurity rules were spurred in large part by the 2003 Eastern blackout that left over 50 million Americans and portions of Ontario Canada without electricity for up to four days, with rolling blackouts for one week in Ontario.[124] Authorities identified a tree which hit a line in Ohio as the initial cause of the blackout.[125] Lack of system and resource visibility, grid operator situational awareness, and control capabilities allowed a local outage to transform into a cascading outage that

121. *Id.*
122. GAO, *Critical Infrastructure Protection*, *supra* note 112, at 14.
123. *Id.* at 11.
124. U.S. CANADA POWER OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA, CAUSES AND RECOMMENDATIONS 1 (2004), http://eta-publications.lbl.gov/sites/default/files/2003-blackout-us-canada.pdf [http://perma.cc/E28P-BFFF].
125. *Id.* at 107–08.

blacked out power to millions.[126] Such incidents are precisely the type that necessitate stronger cybersecurity standards, oversight, and enforcement.

Aptly, the EPAct charged FERC with establishing and enforcing mandatory cybersecurity and reliability standards.[127] EPAct defines "reliability standard" as a requirement, approved by FERC under the Act, "to provide for reliable operation of the bulk-power system," including, "requirements for the operation of existing bulk-power system facilities, including cybersecurity protection."[128] FERC-jurisdictional responsible entities may be ordered to pay fines up to $1 million per day per violation.[129] NERC CIP rules hold responsible entities accountable for supply chain cybersecurity.

EPAct defines a "cybersecurity incident" as, "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."[130] This definition does not limit cybersecurity incidents to those done maliciously, but focuses on the operational consequences of disruption to reliable BES operation like, for example, the 2003 mass blackout in the United States and Canada.

Federal and state regulatory decisions to invest billions to make the energy grid smart through ICT, including the internet, raised the imperative of energy sector cybersecurity. The Energy Independence and Security Act of 2007 (EISA) signed by President George W. Bush spurred federal "smart grid" policies.[131] NIST defined the smart grid as the, "two-way flow of electricity and information to create an automated, widely distributed energy delivery network."[132] The FCC's 2010 National Broadband Plan emphasized, "[c]ommunications are fundamental to all aspects of the smart grid, including generation, transmission, distribution and consumption."[133] ICT including the internet infuses visibility and control into the energy ecosystem, thereby unlocking new energy management and resource options.

---

126. *Id.*
127. EPAct, *supra* note 12.
128. *Id.*
129. NERC, *NERC CIP Compliance*, *supra* note 16; Zhen Zhang, *Cybersecurity Policy for the Electricity Sector: The First Step to Protecting Our Critical Infrastructure from Cyber Threats*, 19 B.U. J. SCI. & TECH. L. 319, 345 (2013).
130. EPAct, *supra* note 12.
131. Sandoval, *supra* note 6, at 16 (citing Pub. L. No. 110-140, 121 Stat. 1492 (2007) (The Energy Independence and Security Act of 2007 (EISA)).
132. *Id.* (citing FCC, CONNECTING AMERICA, THE NATIONAL BROADBAND PLAN 249 (2010), https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf [https://perma.cc/43RZ-6PRX] (citing ELEC. POWER RES. INST. (EPRI), REPORT TO NIST ON THE SMART GRID INTEROPERABILITY STANDARDS ROADMAP (2009), http://www.nist.gov/smartgrid/InterimSmartGridRoadmapNISTRestructure.pdf [https://perma.cc/V3BL-Y3CE])).
133. *Id.*

FERC-jurisdictional energy is the only critical infrastructure sector subject to mandatory federal cybersecurity standards. Other sectors may voluntarily adopt cybersecurity standards.[134] Statutory mandates for cybersecurity are a necessary correlate to federal and state reliability duties. To reap the benefits of ICT investment in energy systems, cybersecurity vulnerabilities must address the changing nature and face of cyber-threats.

C. NERC Critical Infrastructure Protection (CIP) Cybersecurity Standards

Following NERC's formation in 2006, NERC developed proposals and convened workshops that led to the CIP series of standards. In January 2008, FERC Order 706 approved CIP version I which also directed NERC to develop new CIP rules not subject to "reasonable business judgment" and "acceptance of risk" standards.[135] FERC required removal of "reasonable business judgment" and "acceptance of risk" standards recognizing, "the risk involved in the CIP standards, as well as all NERC standards, is risk to the Bulk Electric System, not to the organization itself. No organization can decide to accept risk on behalf of the whole BES."[136] This standard shift recognized the societal values CIP rules seek to protect. Those values take precedence over reasonable business judgment or firm risk-assessment and risk-taking behavior. Regulated entities may not prioritize return-on-investment or assess electric reliability risks as a cost of doing business in place of complying with CIP rules and standards.

The electric grid's interconnected nature and need for balance between energy demand and supply render cybersecurity risks a threat to the entire electric grid, including the people it serves. The electric system is "interconnected and dynamic," and the physics of energy distribution require observance of electrical stability limits.[137] The United States-Canadian report on the 2003 blackout observed that electric grid, "[s]tability problems

134. Zhang, *supra* note 129, at 366 (citing U.S. GOV'T ACCOUNTABILITY OFF., GAO 08-1075R, INFORMATION TECHNOLOGY: FEDERAL LAWS, REGULATIONS, AND MANDATORY STANDARDS FOR SECURING PRIVATE SECTOR INFORMATION TECHNOLOGY SYSTEMS AND DATA IN CRITICAL INFRASTRUCTURE SECTORS 2 (2008)).

135. Order No. 706, Mandatory Reliability Standards for Critical Infrastructure Protection, 122 F.E.R.C. ¶ 61,040 (2008) (to be codified at 18 C.F.R. Pt. 40).

136. TOM ALRICH'S BLOG, *An (Impressionistic) History of NERC CIP* (Jan. 1, 2018), http://tomalrichblog.blogspot.com/2018/01/an-impressionistic-history-of-nerc-cip.html [https://perma.cc/E28P-BFFF].

137. U.S. CANADA POWER OUTAGE TASK FORCE, *supra* note 124, at 8.

can develop very quickly—in just a few cycles (a cycle is 1/60th of a second)—or more slowly, over seconds or minutes."[138] The 2003 outage report further emphasized "[t]he main concern is to ensure that generation dispatch and the resulting power flows and voltages are such that the system is stable at all times" that energy load (demand) matches energy supply.[139]

Under NERC CIP-002, a responsible operator must, "identify critical cyber assets."[140] NERC CIP-003 requires power system operators to, "create security policies to protect all critical cyber assets."[141] CIP-004 requires employee management and training, CIP-005 requires Electronic Security Perimeters, and CIP-006 requires physical security of BES assets.[142] NERC CIP-007 requires, "a network administrator or a responsible entity to ensure that any changes which might occur during a software update or installation of a security patch doesn't affect the overall operations and performance of the critical cyber assets."[143] CIP-008 requires responsible entities to report a cybersecurity incident to the Electricity Sector Information Sharing and Analysis Center,[144] and CIP-009, "requires a recovery plan, the goal of which is to ensure the least possible impact and interruption on system performance."[145]

Additionally, "CIP-005 (Electronic Security Perimeters) and CIP-006 (Physical Security) protect cyber assets from unauthorized intrusions with electronic and physical tools."[146] These NERC rules ultimately require responsible entities to, "control access to critical assets via monitoring devices to detect and alert personnel of attempted or actual unauthorized access."[147] Responsible entities must also conduct an annual vulnerability assessment, including reviewing passwords and network management, and card keys or special locks to protect physical security.[148]

In 2014, NERC promulgated, "[CIP] guidelines referred to as CIP V5, which became binding in July 2016."[149] The standards apply to registered entities according to the function they perform within that system.[150] These

---

138. *Id.*
139. *Id.*
140. BEYOND SECURITY, *NERC-CIP Network Security Requirements*, https://www.beyondsecurity.com/vulnerability_assessment_requirements_nerc-cip.html [https://perma.cc/QK23-FSZ9] [hereinafter NERC-CIP, BEYOND SECURITY].
141. *Id.*
142. Zhang, *supra* note 129, at 347.
143. BEYOND SECURITY, *supra* note 140.
144. Zhang, *supra* note 129, at 349.
145. *Id.*
146. *Id.* at 348.
147. *Id.*
148. *Id.*
149. Stein, *supra* note 55, at 1232; Richard Raysman et al., *The NIST Cybersecurity Framework,* PRAC. L. PRAC. NOTE 5-599-6825 [hereinafter *NIST Cybersecurity Framework*].
150. Susan J. Court, *Federal Cyber-Security Law and Policy: The Role of the Federal Energy Regulatory Commission A Paper Prepared for the 2014 Law + Informatics Symposium*

referenced, "functions include: Balancing Authority, Distribution Provider, Generator Owner, Generator Operator, Interchange Authority, Load Serving Entity, Planning Authority, Purchasing Selling Entity, Reliability Coordinator, Resource Planner, Reserve Sharing Group, Transmission Owner, Transmission Operator, Transmission Planner, and Transmission Service Provider."[151]

On January 21, 2016, FERC Order No. 822 approved seven CIP Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection).[152]

FERC Order No. 829, adopted on July 21, 2016, directed NERC, "to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations."[153] The new standard aimed to, "mitigate the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System."

NERC CIP-013-1 is software and vendor equipment-focused, a cybersecurity lens that may obscure risks from ISPs and the communications system which supplies the electric sector. CIP-013-1 requires responsible entities to report supply chain risks to the industry.[154] FERC ordered NERC and the Critical Infrastructure Protection Committee (CIPC), "to partner with National Laboratory group to conduct current equipment supply chain risk evaluation."[155] Supply chain plans must identify and assess, "BES risk from vendor products and services resulting from procuring and installing vendor equipment and software, and transitions between vendors."[156] FERC also directed NERC to require responsible entities to implement controls

on Cyber Defense Strategies and Responsibilities for Industry, 41 N. KY. L. REV. 437, 443 (2014).

151. *Id.*

152. *FERC Order No. 843*, *supra* note 57, at 4.

153. Order No. 829, *Revised Critical Infrastructure Protection Reliability Standards*, 156 F.E.R.C. ¶ 61,050 (2016).

154. TOBIAS WHITNEY, NERC, CRITICAL INFRASTRUCTURE PROTECTION, SUPPLY CHAIN UPDATE 12 (2008), https://www.nerc.com/pa/comp/Supply%20Chain%20Webinars%20DL/Supply%20Chain%20Webinar.pdf [https://perma.cc/C8HL-MMTK].

155. *Id.* at 15.

156. *Id.*

to mitigate the risk of malicious code that could result from third-party transient electronic devices under Reliability Standard CIP-003-7.[157]

FERC Order 843, adopted in 2018, expressed concern that CIP-003-7 contained a reliability gap in the absence of requirements for the responsible entity to: (1) mitigate any malicious code found during the third-party review(s); or (2) take reasonable steps to mitigate the risks of third party malicious code on its systems, if an arrangement cannot be made for the third-party to do so.[158] FERC observed that without such obligations responsible entities could, "without compliance consequences, simply accept the risk of deficient third-party transient electronic device management practices."[159]

In 2018, FERC updated CIP supply chain cybersecurity standards to address, "four objectives set forth in Order No. 829: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls."[160] FERC observed that while suppliers benefit the energy sector, "the global supply chain also enables opportunities for adversaries to directly or indirectly affect the management or operations of companies that may result in risks to end users."[161] In the 2018 Rulemaking, FERC listed examples of supply chain risks such as, "the insertion of counterfeits, unauthorized production, tampering, theft, or insertion of malicious software, as well as poor manufacturing and development practices."[162] FERC's supply chain risk examples reflect a hacker-focus that obscures systemic supply chain risks such as those arising from ISP governance and net neutrality repeal.

D. Protecting Critical Infrastructure Protection Through PPD-21, 2013

President Obama's 2013 Presidential Executive Order, PPD-21, directed federal agencies to support critical infrastructure cyber and physical security, consistent with CIPA's mandates.[163] PPD-21 identifies, "energy and communications systems as uniquely critical due to the enabling functions

157. *FERC Order No. 843*, *supra* note 57, at 39.

158. *Id.* at 19.

159. *Id.* at 19–20 (*citing* Order No. 706, 122 F.E.R.C. ¶ 61,040 at P 150 (2006) (rejecting the concept of acceptance of risk in the CIP Reliability Standards)).

160. Notice of Proposed Rulemaking, *Supply Chain Risk Mgmt. Reliability Standards*, 162 F.E.R.C. ¶ 61,044 at P 6 (2018).

161. *Id.* at 2.

162. *Id.*

163. Sandoval, *supra* note 6, at 4–5 (citing THE WHITE HOUSE, *Presidential Policy Directive—Critical Infrastructure Security and Resilience* (PPD-21) (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-pressoffice/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/RB88-HZXZ]; DEPT. OF HOMELAND SECURITY, *Critical Infrastructure Sectors*, https://www.dhs.gov/critical-infrastructure-sectors [https://perma.cc/S65Y-3STL] [hereinafter *PPD-21*]).

they provide across all critical infrastructure sectors."[164] PPD-21 specifically designated the following sixteen sectors "critical infrastructure": Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense-Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Water; Transportation Systems; Water and Wastewater Systems.[165] PPD-21 identifies, "energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors."[166] Accordingly, PPD-21 directed the Secretary of Homeland Security to, "develop situational awareness capability for critical infrastructure, requiring action to address evolving threats and consequences."[167] PPD-21 requires DHS response to "evolving threats and consequences,"[168] anticipating that the nature, sources, and results of cyber threats will change.

In 2013, concurrent with the issuance of PPD-21, President Obama promulgated Executive Order 13636*,* Improving Critical Infrastructure Cybersecurity,[169] which directed, "the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) to work with stakeholders and develop a voluntary framework for reducing cyber risks to critical infrastructure."[170] Executive Order 13636 requires cybersecurity policy coordination across government agencies, cybersecurity information sharing between the government and industry.[171] It also requires, "[r]egulatory agencies to: assess their cybersecurity regulations against the Framework [for Improving Critical Infrastructure Cybersecurity] once developed; and create a voluntary program to support adoption of the Framework."[172] NIST's Cybersecurity Framework set a floor for cybersecurity efforts. Ongoing evaluation is necessary to address new cybersecurity risks such as ISP network management practices. The FCC's net neutrality repeal permits ISPs to enter into deals to prioritize certain internet traffic based on opaque paid priority deals, even if doing so slows other internet traffic. Net

164. Sandoval, *supra* note 6, at 11 (citing *PPD-21*, *supra* note 163).
165. *PPD-21*, *supra* note 163.
166. *Id.*
167. *Id.*
168. *Id.*
169. 78 Fed. Reg. 11739, 2013 WL 596302 (Pres.) (July 12, 2013).
170. *NIST Cybersecurity Framework*, *supra* note 149.
171. *Id.*; 78 Fed. Reg. 11739, 2013 WL 596302 (Pres.) (July 12, 2013).
172. *NIST Cybersecurity Framework*, *supra* note 149.

neutrality repeal is an example of an evolving threat NIST's Cybersecurity Framework underestimates.

E. NIST Cybersecurity Framework

Prior to Executive Order 13636, President Obama issued an Executive Order in February 2013 directing NIST to create a cybersecurity framework to reduce cyber risks to critical infrastructure, "incorporating voluntary consensus standards and industry best practices to the fullest extent possible."[173] One year later, on February 12, 2014, NIST issued the *Framework for Improving Critical Infrastructure Cybersecurity*. NIST's Cybersecurity Framework presents a voluntary, "risk-based approach to cybersecurity that provides a methodology for any organization to develop an information security program but does not prescribe concrete security controls."[174] NIST's Framework defined risk management as, "the ongoing process of identifying, assessing, and responding to risk."[175]

The NIST Cybersecurity Framework suggests a core set of activities and outcomes to mitigate cybersecurity threats: Identify, Protect, Detect, Respond, Recover.[176] The Framework has been widely adopted and is often cited as the "'standard' for 'due diligence.'"[177] Several ISOs and RTOs stated in their FERC Resiliency and Reliability docket comments that they comply with NIST's Framework.[178] Scott J. Shackelford et al., argue the Framework's widespread adoption, "is a necessary but not sufficient condition to boosting U.S. CI protection across a range of CI providers with different threat profiles."[179] The Framework is process-oriented and emphasizes security incident detection response, and recovery.[180] NIST's Framework provides

---

173. The White House, Fact Sheet: Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (May 29, 2009), https://fas.org/irp/news/2009/05/cyber-fs.html [https://perma.cc/FX33-33C4].

174. *NIST Cybersecurity Framework*, *supra* note 149.

175. *Id.* at 4.

176. *Id.* at 3.

177. *See, e.g.*, Scott J. Shackelford et al., *From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do About It*, 96 NEB. L. REV. 320, 330 (2017).

178. *See, e.g.*, PJM, *FERC Grid Resilience Comments*, *supra* note 54, at 36.

179. Shackelford et al., *supra* note 177, at 332–33.

180. *NIST Cybersecurity Framework*, *supra* note 149. *See also* Scott J. Shackelford et. al., *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217, 221–22 (2016) (describing criticism of the NIST framework as reactive and not sufficiently proactive) (citing Taylor Armerding, NIST's Finalized Cybersecurity Framework Receives Mixed Reviews, CSO (Jan. 31, 2014), http://www.csoonline.com/article/2134338/security-leadership/nist-s-finalized-cybersecurity-framework-receives-mixed-reviews.html. For more on the benefits of a more proactive approach to cybersecurity, see Amanda N. Craig

"standards, guidelines, and practices to encourage CIP, mainly through public-private partnerships," but does not propose sector-specific rules or requirements.[181] As noted, NIST's Framework has been characterized as a "gold standard" or standard for due diligence for cybersecurity practices "litigation or [for] a regulatory investigation."[182] Accordingly, President Trump issued an Executive Order in 2017 requiring all federal agencies to comply with NIST's Cybersecurity Framework.[183] Still, NIST Framework compliance does not provide a safe harbor to demonstrate compliance with FERC or NERC cybersecurity responsibilities. As discussed below, the NIST Framework may unduly focus on incidents or a cycle of repeated attacks, and miss new threats such as those arising from the net neutrality repeal.

F. Cybersecurity Information Sharing and Reliability Standards

The Energy Modernization Act, subsequent NERC and FERC rules, and federal law all permit and encourage information sharing between market participants about cybersecurity threats. The Cybersecurity Act of 2015 exempted from antitrust scrutiny private entity sharing about, "digital security risks and potential attacks."[184] This Act effectively removed legal barriers to information sharing between competitors to promote proactive responses to cybersecurity threats. The Cybersecurity Act of 2015 also encourages, "the private sector and federal government to work together to identify and defend against cybersecurity threats."[185] One example of the Act's encouraged information sharing includes e-mail-based "NERC

et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 52 AM. BUS. L.J. 721 (2015)).

181. Eldar Haber & Tal Zarsky, *Cybersecurity for Infrastructure: A Critical Analysis*, 44 FLA. ST. U. L. REV. 515, 531 (2017).

182. Scott J. Shackelford et al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things"*, 2017 U. ILL. L. REV. 415, 442 (2017); Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1504–05 (2017) (characterizing the NIST's process-oriented framework as the "gold-standard" model for cybersecurity).

183. *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Exec. Order No. 13,800 § 1(c)(ii), 82 Fed. Reg. 22,391, 22,391–93 (May 11, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-orderstrengthening-cybersecurity-federal-networks-critical-infrastructure/ [https://perma.cc/8DWW-M7WS] [hereinafter *President Trump Executive Order 13,800 on Cybersecurity*]; William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1160 (2019).

184. Stein, *supra* note 55, at 1231–32; Consolidated Appropriations Act, 2016, Pub. L. No. 114–113, 129 Stat. 2242, 2244.

185. Kosseff, *supra* note 87, at 1006.

alerts" that share information among the energy sector about cyber vulnerabilities, threats, and attacks.

In 2017, President Trump issued an Executive Order on Cybersecurity & Critical Infrastructure which declared, "the policy of the executive branch to promote an open, interoperable, reliable, and secure internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy and guarding against disruption, fraud, and theft."[186] Notably, neither the FCC nor FERC cited this Executive Order in the FCC's *Internet Freedom Order* repealing net neutrality, or in the FERC Grid Resiliency docket. In fact, FERC continues to adopt cybersecurity standards that are largely divorced from other federal policies regarding internet and ISP governance.

For example, FERC Order 848 adopted Cyber Security Incident Reporting Reliability Standards in July 2018.[187] These reporting requirements promote information sharing to increase industry, security, and regulatory ability to detect and react to cyber incidents. As such, FERC's reporting requirements have largely focused on incidents. FERC, state regulators, and the energy sector must recognize systemic threats to cybersecurity such as those posed by ISPs unbridled from FCC net neutrality regulation.

G. Cybersecurity and State PUC Initiatives

In 2016, the Michigan Public Service Commission adopted a proceeding on its own motion to, "review issues concerning cybersecurity and the effective protection of utility infrastructure."[188] The State of New York's Reforming Energy Vision (REV) proceeding noted the, "[DOE's] Office of Electricity Delivery and Energy Reliability implemented the Cybersecurity for Energy Delivery Systems (CEDS) program to develop cybersecurity solutions for energy delivery systems. It emphasizes collaboration among governments, industry and others to address the unique environment of energy delivery systems."[189] REV relies on federal cybersecurity programs, while several other states are analyzing whether to adopt their own cybersecurity

186. *President Trump Executive Order 13,800 on Cybersecurity*, *supra* note 183.

187. Order No. 848*, Cyber Security Incident Reporting Reliability Standards*, 164 F.E.R.C. ¶ 61,033 (2018).

188. MICH. PUB. SERV. COMM'N, CASE NO. U-18203, IN THE MATTER OF REVIEW ISSUES CONCERNING CYBERSECURITY AND THE EFFECTIVE PROTECTION OF UTILITY INFRASTRUCTURE, ON THE COMMISSION'S OWN MOTION (2016), 2016 WL 6996044.

189. N.Y. PUB. SERV. COMM'N, CASE 14-M-0101, PROCEEDING ON MOTION OF THE COMMISSION IN REGARD TO REFORMING THE ENERGY VISION, at 21 (2014), 2014 WL 1713082 (citing http://www.energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity [https://perma.cc/J2L5-9CL5]).

rules and initiatives. Accordingly, the State of Maryland in 2015 created a Cybersecurity Council to:

> [C]onduct risk assessments on local infrastructure that federal law or Executive Order 13636 do not cover; assist infrastructure entities not covered by Executive Order 13636 in complying with federal cybersecurity guidance; help private sector cybersecurity businesses in adopting, adapting, and implementing the Framework; and recommend strategic planning measures and any necessary legislative changes.[190]

In February 2017, Idaho's Governor issued Executive Order No. 2017-02, which directed state agencies to immediately adopt and implement NIST's Cybersecurity Framework.[191]

Further, the California Public Utilities Commission (CPUC) issued a staff report on cybersecurity in 2012 which emphasized that, "NERC-CIP" primarily covers only generation and transmission assets that qualify as "critical assets" or "critical cyber-assets."[192] Distribution level assets such as advanced meters and DERS, "do not fall under NERC-CIP but can have a major impact on grid reliability, safety and customer privacy."[193] In 2012, estimates ranged that, "from 80 percent to over 90 percent of grid assets are outside NERC-CIP's scope."[194] The CPUC's 2012 report emphasized that, "NERC-CIP is primarily a compliance-based policy. Compliance is an important component of addressing cybersecurity, but it is not enough to ensure that the rapidly evolving risks are adequately considered and acted upon effectively."[195] Then in 2017, the CPUC committed to implementing a Staff Cybersecurity Group to address the Risk Management pillar of its safety action plan.[196] State-level cybersecurity policies should be calibrated to state reliability, safety, environmental, rate, and other responsibilities for the state's energy jurisdiction.

Illinois Public Utilities Commission (PUC) Commissioner Sherina Maye Edwards observed that "many state regulators are increasing their oversight and involvement, using stakeholder working groups, docketed cybersecurity rulemakings, advanced metering infrastructure (AMI) deployment proceedings,

190. MD. CODE ANN., ST. GOV'T § 9-2901 (West 2018).
191. *NIST Cybersecurity Framework*, *supra* note 149.
192. *CPUC Staff Report, Cybersecurity and the Evolving Role of the States*, *supra* note 18, at iii.
193. *Id.*
194. *Id.*
195. *Id.*
196. CPUC, *2017 Safety Action Plan Update*, *supra* note 108, at 2.

rate cases, audits and reporting requirements."[197] Commissioner Edwards offered several exemplars, including the Pennsylvania PUC which adopted rules that required its regulated utilities to develop continuity plans related to cybersecurity, emergency response, physical security, and business. And "[i]n 2015, the Missouri Public Service Commission opened a docket to examine cybersecurity and physical infrastructure security issues. It requires verbal reporting of 'cybersecurity or infrastructure security events that affect many customers, involve the release of customer proprietary information, or pose a threat to the general public.'"[198] Commissioner Edwards also noted that, "New Jersey['s] Board of Public Utilities recently adopted a set of comprehensive cybersecurity requirements for electric, natural gas and water/wastewater utilities . . . [which] directed [utilities] to create cybersecurity programs that define responsibilities for cyber risk management activities."[199] Thus, New Jersey is establishing, "procedures for identifying and mitigating cyber risk to critical systems through risk assessments and cybersecurity training programs."[200] In 2017, amidst the flurry of state-level action, the National Association of Regulatory Utility Commissioners (NARUC) updated its Cybersecurity Primer for state regulators.[201] NARUC therein emphasized state responsibility for energy reliability and rates, and addressing customer consequences of cybersecurity breach.[202]

State energy cybersecurity initiatives must recognize evolving vulnerabilities. The following section analyzes the "hacker-focus" that frames prevailing cybersecurity paradigms. This limited lens obscures systemic cybersecurity vulnerabilities such as ISP control of internet data passing through an ISP's network.

VI. PREVAILING CYBER THREAT PARADIGMS

A. Cybersecurity Hacker Paradigm Blinders

Cybersecurity must consider the evolving nature, type, and source of threats and vulnerabilities. This Article identifies the "hacker paradigm" prevalent in cybersecurity governance and strategies as a lens that limits the view of cyber risks. CIP rules and the Cybersecurity Framework are rooted in the hacker paradigm, focusing on incident-level attackers. NIST's

197. Commissioner Edwards et al., *supra* note 20.
198. *Id.*
199. *Id.*
200. *Id.*
201. Miles Keogh & Sharon Thomas, CYBERSECURITY: A PRIMER FOR STATE REGULATORS 3.0, NAT'L ASS'N OF REG. UTIL. COMM'RS (Jan. 2017), https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F [https://perma.cc/W4RS-8NNT].
202. *Id.* at 1.

Cybersecurity Framework Core—Identify, Protect, Detect, Respond, Recover[203] —reflects the hacker paradigm wherein a cybersecurity vulnerability is identified, protection measures are taken, networks are monitored, response is initiated, and recovery is achieved. This cycle continues for each subsequent threat. Cybersecurity vulnerabilities created by ISP unbridled power to manage the internet in their business interest, and to sell paid priority or throttle traffic, are systemic vulnerabilities created by the FCC's shift in ISP governance, not threats the five-step Cybersecurity Framework Core can overcome.

The United States DHS's March 2018 warning about hacker probes of the energy grid underscored the importance of cybersecurity to energy reliability and national security:[204] "Hacking and network intrusions are cyber-attacks that attempt to gain unauthorized access to an organization's IT systems, network, or data. Data breaches often occur when an organization loses control over its confidential or sensitive data."[205] DHS warned that hackers may act for a variety of reasons including to, "[s]teal valuable data, such as personal information, trade secrets, or other intellectual property, . . .[m]isuse an organization's systems or network for the hacker's own purposes, . . . [or] [s]abotage or damage an organization's systems or data."[206]

Because hackers often enter networks from the internet,[207] poorly secured connections may permit hacker intrusions. For example, "[i]nsiders may inadvertently or purposely enable hacking and network intrusions by: Sharing their user credentials, especially those that permit remote access, failing to protect computers, network devices, or connections, especially those used to administer the organization's IT systems and network."[208] Alexandre Vernotte et al., observed that threats to electric grid load balancing and, "the smart grid in general arise from the activities of a misbehaving

203. *NIST Cybersecurity Framework*, *supra* note 149, at 3.
204. US-CERT, *Russian Government Cyberactivity Targeting Energy and Other Critical Infrastructure Sector (Alert, TA18-074A)* (Mar. 16, 2018), https://www.us-cert.gov/ncas/alerts/TA18-074A [https://perma.cc/6NGH-9AEB].
205. PRAC. L. INTELL. PROP. & TECH., CYBERSECURITY TECH BASICS: HACKING AND NETWORK INTRUSIONS: OVERVIEW (PRAC. L. PRAC. Note Overview w-003-3498, 2019) [hereinafter *Cybersecurity Tech Basics*].
206. *Id.*
207. *Id.*
208. *Id.*

or a rouge actor in combination with poor design, implementation, or configuration of the system that makes it vulnerable."[209]

Organizational insiders may pose cyber risks through poor practices, fall victim to phishing or other schemes to steal credentials, or behave contrary to the organization's interests. As PJM noted, insiders may "steal or expose data" or "sabotage an organization's resources."[210] NIST also reported, "cybersecurity researchers regularly show that many, if not most, attacks work by exploiting either or both: Individuals, using social engineering methods such as phishing[and] [k]nown, but unaddressed, technical vulnerabilities."[211]

The GAO's 2005 report on CIP discussed typical sources of cyber threat then identified by United States intelligence. These sources were categorized as: bot-network operators (who "take over multiple systems in order to coordinate attacks and to distribute phishing schemes,"[212] spam, and malware[213] attacks); criminal groups (attacking systems for monetary gain); foreign intelligence services (using cyber tools for information-gathering and espionage); hackers (described as those who "break into networks for the thrill of the challenge or for bragging rights in the hacker community," the majority of whom "do not have the requisite expertise to threaten difficult targets such as critical [United States] networks."); insiders (characterized as the "disgruntled organization insider" and outsourcing vendors and employees who accidentally introduce malware into systems); phishers (attempting to steal identities or information for monetary gain); spammers (distributing unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations); spyware and malware authors (seeking to inject computer viruses and worms); terrorists (seeking to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence).[214] GAO's 2005 list recognized that "outsourcing vendors" could introduce malware as insiders.[215] ISPs typically provide internet access, as few firms also act as their own ISP.

---

209. Vernotte et al., *supra* note 3, at 2.
210. *Cybersecurity Tech Basics*, *supra* note 205.
211. *NIST Cybersecurity Framework*, *supra* note 149.
212. GAO, *Critical Infrastructure Protection*, *supra* note 112, at 5 (defining phishing as "the creation and use of e-mails and Web sites that are designed to look like those of well-known legitimate businesses or government agencies, in order to deceive Internet users into disclosing their personal data for criminal purposes, such as identity theft and fraud.").
213. *Id.* (defining malware as "software designed with malicious intent, such as a virus.").
214. *Id.* at 5.
215. *Id.*

GAO's 2005 cybersecurity threat sources list illustrates the hacker or disgruntled insider paradigm prevalent today. Hackers are often portrayed as a loner at home[216]—a characterization that fails to recognize the emergence of hacker collectives. Hackers may work for not only their own motives, but also for economic, political, or other reasons; they may also act as part of a criminal enterprise or even be deployed by foreign intelligence services.[217] For example, a 2017 report from the Oxford Internet Institute identified, "[c]yber troops," as "government, military or political party teams committed to manipulating public opinion over social media."[218]

In 2005, then Federal Bureau of Investigation (FBI) Director Robert Mueller testified that, "although individual hackers do not pose a great threat, hackers intent on stealing information or motivated by money are a concern."[219] Expressing prescient concern, Director Mueller added that, "if this pool of talent is utilized by terrorists, foreign governments or criminal organizations, the potential for a successful cyber-attack on our critical infrastructures is greatly increased."[220] His informed experience and judgment foresaw the link between hackers and foreign governments manifested just one decade later in internet hacks designed to both interfere with the 2016 elections and attack the United States energy sector.[221]

---

216. *See e.g.,* Tal Kopan, *Is Trump Right? Could a 400-Pound Couch-Potato Have Hacked the DNC*, CNN (Sept. 27, 2016), https://www.cnn.com/2016/09/27/politics/dnc-cyberattack-400-pound-hackers/index.html [https://perma.cc/QVZ5-7JV9] (noting that in 2016 then-candidate Donald Trump said in regards to the source of the hack into the Democratic National Committee that "[i]t could be Russia, but it could also be China . . . It could also be lots of other people. It also could be somebody sitting on their bed that weighs 400 pounds.").

217. *See e.g.*, Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44, Title II, 131 Stat. 886 (2017), https://www.congress.gov/bill/115th-congress/house-bill/3364/text?q=%7B%22search%22%3A%5B%22sanctions%22%5D%7D&r=2 [https://perma.cc/82SF-H3CS].

218. Samantha Bradshaw & Philip N. Howard, *Troops, Trolls, and Troublemakers: A Global Inventory of Organized Social Media Manipulation* (Oxford Internet Institute, Computational Propaganda Research Project, Working Paper No. 2017.12, 2017), https://comprop.oii.ox.ac.uk/research/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/ [https://perma.cc/9JB3-LV7R].

219. GAO, *Critical Infrastructure Protection*, *supra* note 112, at 6.

220. *Id.*

221. Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44, Title II, 131 Stat. 886 (2017) (finding "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the United States presidential election."); Brad Heath, *A Mountain of Evidence Points in One Direction: Russia Sought To Sway the 2016 US Election*, USA TODAY (Aug. 3, 2018), https://www.usatoday.com/story/news/2018/08/03/russian-us-election-interference-donald-trump/878910002/ [https://perma.cc/XUR5-VXVQ] ("Prosecutors working for Mueller offered more details on the hacking in July, when a grand jury indicted 12

In regards to the attack on the energy sector, "[i]n May 2017, Russian hackers infiltrated the business systems of [United States] nuclear power plants and other companies in the energy sector in an effort to gather personnel data" that can be, "used for more targeted attempts to compromise infrastructure, including gathering emails, communications about designs, security audits, poorly secured passwords, and known issues."[222] Hackers may use such reconnaissance attacks, "to set up for future, more damaging attacks just based on the proprietary information they're able to steal."[223] This type of attack is an example of an "Advanced Persistent Threat (APT)" through which an attacker, "intrudes into an organization's network . . . and [r]emains resident and undetected for an extended period of time."[224] APTs are particularly alarming because such attacks may steal data or spy on an organization's personnel or activities.[225]

In regards to the election interference attacks, the United States DHS's Computer Emergency Readiness Team (US-CERT) issued a warning on March 16, 2018, of Russian government cyberactivity targeting energy and other critical infrastructure sectors.[226] The alert cautioned that Russian government actions targeted "[United States] Government entities as well as organizations in the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors," conducting network reconnaissance and collecting Industrial Control Systems data.[227]

PJM's comments in FERC's Grid Resiliency docket characterized cyber-attacks as typically originating, "from nation states, terrorists and un-attributable threats."[228] PJM noted "many nation states have increased capability and interest to perform cyber-attacks," and their motives for cyber intrusions vary.[229] Specifically, "[Critical Infrastructure] owners suffer repeated cyberattacks, and some electric utilities report being probed thousands of times each month."[230]

Russian intelligence officers for breaking into Democratic political organizations to steal troves of internal records that they then made public.").

222. Andrew Moshirnia, *No Security Through Obscurity: Changing Circumvention Law to Protect Our Democracy Against Cyberattacks*, 83 BROOK. L. REV. 1279, 1290–91 (2018).

223. *Id.*

224. *Cybersecurity Tech Basics*, *supra* note 205.

225. *Id.*

226. US-CERT, *supra* note 204.

227. *Id.*

228. PJM, *FERC Grid Resilience Comments*, *supra* note 54, at 21.

229. *Id.* at 22.

230. Chung, *supra* note 96, at 476 n.95 (citing Scott J. Shackelford et al., *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995, 2005–06 (2016)).

In addition to nation-state sponsors of cyber threats, PJM noted "[c]ertain actors have expressed their intentions, in recruitment videos or otherwise, to attack the U.S. power grid to damage and disrupt the power grid to effect the general population and create fear," though their capabilities "are not fully known to the electricity industry, making the assessment by an RTO of the likelihood of a cyber-attack and its anticipated impacts more difficult."[231] PJM reported that this, "category represents the most common form of attacks detected on the industry systems in the form of routine reconnaissance by likely cyber criminals searching for software vulnerabilities to exploit."[232]

FERC's 2018 Grid Resiliency docket ordered ISOs and RTOs to report to FERC about several cyber security issues. These include how ISOs and RTOs, "identify and plan for risks associated with high-impact, low-frequency events (e.g., physical and cyber-attacks, accidents, extended fuel supply disruptions, or extreme weather events)."[233] FERC directed ISOs and RTOs to identify any studies, "conducted, are currently in progress, or are planned to be performed in the future to identify the ability of the bulk power system to withstand a high-impact, low-frequency event (e.g., physical and cyber-attacks, accidents, extended fuel supply disruptions, or extreme weather events)."[234] FERC further asked ISOs and RTOs to explain the extent to which each, "consider[ed] whether specific challenges to resilience, such as extreme weather, drought, and physical or cyber threats, affect various generation technologies differently?"[235]

CAISO characterized cyber-attacks as "manmade threats" that can "inflict harm on the power grid," and "occur at any time and without notice," producing "unpredictable" results.[236] CAISO explained, "[i]nformation security incidents that threaten the confidentiality, integrity, and availability of CAISO's systems or information may include, but are not limited to, losing grid visibility, losing energy market systems, data disclosure, changing control variables, losing access to critical operational systems, accessing employee data, or causing financial loss or manipulation."[237]

---

231. PJM, *FERC Grid Resilience Comments*, *supra* note 54, at 22.
232. *Id.* at 23.
233. *Id.* at 21.
234. *Id.* at 34.
235. *Id.* at 47.
236. CAL. INDEP. SYS. OPERATOR CORP., COMMENT LETTER IN RESPONSE TO THE COMMISSION'S REQUEST FOR COMMENTS ABOUT SYSTEM RESILIENCY AND THREATS TO RESILIENCE 12 (Mar. 9, 2018), http://www.caiso.com/Documents/Mar9_2018_Comments-GridResilience_AD18-7.pdf.
237. *Id.*

Hacker intrusions and ISP self-interested network management exemplify man-made threats. PJM noted that man-made threats are "more difficult to quantify because they don't adhere to cyclical weather patterns and cannot be accurately forecasted or projected. Additionally, their effects are discriminate, often targeting the most critical infrastructure, in contrast to indiscriminate and more random effects associated with naturally occurring hazards."[238] Analysis of the ISP's role in the smart grid architecture highlight man-made supply chain and systemic risks the FCC's net neutrality repeal created.

B. Supply Chain Cybersecurity Risks

Prevailing cybersecurity paradigms scrutinize the supply chain through a hacker-focused lens as a hacker target—a means to steal credentials to gain access to the supplier's client. NIST includes in supply chains firms or entities used to design, develop, manufacture, process, handle, and deliver products and services to the end user.[239] NIST's Cybersecurity Framework underscores the importance of "supply chain risk management" (SCRM) to manage cybersecurity risks a supplier has on external parties and the cybersecurity effect external parties have on an organization.[240] NIST identifies a primary objective of cyber SCRM as identifying, assessing, and mitigating products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain.[241]

NIST emphasizes the supply chain as a source of malicious or counterfeit code or functional vulnerability. This focus on one segment of the supply-chain landscape misses ISP technical ability and newly acquired legal authority to introduce functional problems with internet communication due to the FCC's net neutrality repeal order.[242] The first step in NIST's Cybersecurity Framework core is to identify cyber risks. Risk identification should not just look for exposure to hackers, insiders, or traditional supply chain failures. Rather, risk identification must also consider systemic threats including those induced by United States federal policy and ISPs that supply the energy sector with internet access.

ISPs supply last-mile broadband access to subscribers, including energy ecosystem participants and other critical infrastructure. An ISP that deliberately slows or degrades signals used for energy system operation, maintenance,

---

238. PJM, *FERC Grid Resilience Comments*, *supra* note 54, at 20.
239. *NIST Cybersecurity Framework*, *supra* note 149.
240. *Id.*
241. *Id.*
242. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 4 ("The FCC's 2018 '*Internet Freedom*' Order for the *first* time gives ISPs legal permission to erect toll booths between subscribers and content providers.").

planning, and other activities may compromise energy system functionality—a supply chain vulnerability that requires cybersecurity vigilance and reporting.

Vernotte et al., note that smart grid energy resources and participants can use a variety of media to communicate with the internet: "Communication networks between the central control systems and substations can consist of fibre, radio, mobile phone networks (GSM/GPRS), or Power Line Carrier (PLC)."[243] Energy resource scheduling coordinators participating in CAISO's wholesale market can communicate to CAISO through the private Energy Communications Network (ECN) AT&T runs and may subscribe to a private Service Level Agreement that provides Quality of Service (QoS) standards.[244]

ECN-based communication to and from CAISO through AT&T's commercial service is one example of an internet service that would have fallen outside of the coverage of the FCC's net neutrality rules that applied to "Broadband Internet Access Services" (BIAS) offered in the "mass market."[245] The FCC defined "mass market" BIAS to exclude, "enterprise service offerings, which are typically offered to larger organizations through customized or individually negotiated arrangements, or special access services."[246] AT&T offers access to the ECN private network for a monthly fee that varies with the service package selected.[247] CAISO reports that connection to the ECN takes 30-45 business days.[248]

CAISO also allows connection via the public internet to lessen time to establish communication and lower operational costs for participating energy resources.[249] Residential customers may offer their home thermostat, a solar system, a battery, or other facilities as grid resources, accessible through their home internet connection. The FCC's 2015 net neutrality rules applied

243. Vernotte et al., *supra* note 3, at 8.

244. CAL. INDEP. SYS. OPERATOR, SC CERTIFICATION OVERVIEW (May 4, 2018), http://www.caiso.com/Documents/SCCertificationOverview.pdf [https://perma.cc/GQ5J-32D9] [hereinafter CAISO, SC CERTIFICATION OVERVIEW].

245. FCC, *2015 Open Internet Order*, *supra* note 5, ¶ 189.

246. *Id.* It is worth noting that FCC separates enterprise service offerings from BIAS yet treats them as functional equivalents to say that certain users, e.g., emergency services, would not be affected by the potential threats of blocking and throttling because they had access to enterprise offerings.

247. CAISO, SC CERTIFICATION OVERVIEW, *supra* note 244, at 4.

248. *Id.*

249. *ISO New Resource Implementation Process Enhancement*, CAL. INDEP. SYS. OPERATOR (May 18, 2017), http://www.caiso.com/Documents/ISONewResourceImplementationProcessEnhancement.html [https://perma.cc/3ZYG-NPMT] [hereinafter CAISO, *New Resource Implementation Process Enhancement*].

to "mass market" broadband internet access service such as "a service marketed and sold on a standardized basis to residential customers, small businesses, and other end-user customers such as schools and libraries."[250] The 2018 net neutrality repeal opens the door to cybersecurity vulnerabilities for energy resources that rely on mass market broadband. The electric grid relies on and is connected to many resources that communicate through public, mass-market Internet access.

Communications pathways create new opportunities but can also open new threat vectors. "While knowing about the components that constitute the smart grid is important, knowing how these components communicate and for which purpose is essential for performing cyber security analysis, as data flows make for the "highway of hackers," Vernotte et al. observed."[251] ISPs need not hack into an energy operator's network as they control access to and output from the network. FCC allowance of unregulated paid priority deals opened a freeway on-ramp for paid priority deals, and ISP transactions that favor some traffic can slow other internet traffic sharing the same infrastructure.

NIST's Cybersecurity Framework recognizes the difficulty of controlling supplier cybersecurity. Its Framework observed that it may not be possible to impose a set of cybersecurity requirements on the supplier.[252] NIST also promotes informed purchasing as a supply-chain cybersecurity strategy. NIST recommends the "objective should be to make the best buying decision among multiple suppliers given a carefully determined list of cybersecurity requirements. Often, this means some degree of trade-off, comparing multiple products or services with known gaps to the Target Profile," NIST laments.[253]

NIST's Framework assumes that buyers have a choice of suppliers, or that suppliers offer a meaningful choice. The FCC's net neutrality repeal order reported that in 2016, "40% of Americans had the choice of only one provider offering high-speed internet at 25 [Megabits per second] up and 3 down, 45.2% had the choice of two, 5.9% had three, while 8.9% had none."[254] Energy resources are often limited in the choice of communications providers and may have to expend substantial resources to bring communications access to their facility. Lack of competition between ISPs[255] makes it difficult to avoid ISP network management practices that undermine reliability by

250. FCC, *2015 Open Internet Order*, *supra* note 5, ¶ 189.
251. Vernotte et al., *supra* note 3, at 8.
252. Matthew P. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity*, *Version 1.1*., NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 18 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://perma.cc/DY7M-JE77].
253. *Id.*
254. FCC, *Internet Freedom Order*, *supra* note 4, ¶ 125.
255. *Id.* ¶¶ 125–26.

switching to another ISP that does not engage in paid priority or throttle energy users who use exceed their "unlimited" internet plan.

Hong Guo et al. modeled the effect of ISP duopoly competition on content providers in the absence of net neutrality rules.[256] Their model revealed that ISP duopoly competition, where content providers also compete for internet priority through paid priority deals, maintains ISP incentives to seek additional revenues from content providers to avoid being left behind in the queue.[257] FCC's net neutrality repeal induces ISP profit-seeking behavior that can impact energy sector rates, reliability, and safety. Limited ISP competition may deter substitution as a solar panel or smart thermostat cannot readily change ISPs to avoided harmful ISP network management practices.

FERC requires responsible entities to ensure their supply chain's cybersecurity, and it maintains enforcement authority to police rule compliance.[258] A power company agreed to pay a $2.7 million penalty in 2018 for violations of NERC CIP rules after FERC determined the company "failed to properly classify the information with the appropriate sensitivity level," or to, "ensure that the vendor protected the sensitive information after the data was improperly copied from the regulated entity's network."[259] In its analysis, "NERC focused on the gravity of the breach, not only because it would have allowed physical and remote access to the company's system, but also because it threatened the reliability of the entire bulk power system."[260] FERC's ruling against this company underscored its assessment that cybersecurity poses risks to the entire energy system, and thus it is not left to business judgment, firm, or individual risk-taking.

The above FERC ruling is just one exemplar that federal energy sector cybersecurity obligations do not allow the energy sector to take a *post facto* approach to cybersecurity and reliability risks. The DOJ and FCC's brief in defense of the FCC *Internet Freedom Order's* repeal of net neutrality rules argued to the D.C. Circuit that any harms from ISP network management, "are exposed and deterred by market forces, public opprobrium, and

256. Hong Guo et al., *Effects of Competition Among Internet Service Providers and Content Providers On The Net Neutrality Debate*, 41:2 MIS. Q. 353-A29 (June 2017).

257. *Id.*

258. *See*, *e.g.*, *Legal Alert: NERC and Power Company Reach Legal Settlement on Violations of Cybersecurity Standards*, EVERSHEDS SUTHERLAND (Mar. 22, 2018), https://us.eversheds-sutherland.com/NewsCommentary/Legal-Alerts/209814/Legal-Alert-NERC-and-power-company-reach-settlement-on-violations-of-cybersecurity-standards [https://perma.cc/P4CS-UMMK].

259. *Id.*

260. *Id.*

enforcement of the consumer protection laws."[261] DOJ and FCC hopes for market discipline, public scorn, and consumer protection law to restrain harmful ISP conduct do not account for the energy sector's duties to provide safe and reliable service.

The FCC's *Internet Freedom Order* also failed to consider the consequences to energy reliability and the environment from ISP-induced communications delays. The amicus brief I co-authored with Professors Hammond, Byerly, and Chase, my Article *Net Neutrality Powers Energy and Forestalls Climate Change*, and my Reply Comments submitted in the *Internet Freedom* docket, along with critical infrastructure and energy sector legal duties to provide reliable service, reveal the arbitrary and capricious decision-making that formed the *Internet Freedom Order*, and require its vacatur and remand to the FCC to satisfy the APA.[262] As such, ISP gatekeeper access to internet data underscores the imperative of examining the consequences of ISP unbridled network management practices for public safety, energy reliability, just and reasonable rates, and achievement of environmental goals.

C. ISPs Do Not Need to Hack to Gain Access to Data Traversing Their Network to Other Internet Endpoints

ISPs need not hack to gain access to subscriber internet data. ISPs are tasked with transporting data to and from their subscriber to other internet endpoints.[263] Vernotte et al. placed the internet as the central component of smart grid "architecture as it is the main intermediary to the different stakeholders (along with fiber, GPRS networks from telecom operators)."[264] Once the traffic crosses the ISP's network firewall, it becomes part of the greater network under ISP control.[265] The ISP controls the user's traffic as it

---

261. Brief for Respondents at 74–75, Mozilla Corp., et al. v. FCC, No. 18-1051 (D.C. Cir. 2018) [hereinafter *Respondents' Brief*] (citing FCC, *Internet Freedom Order*, *supra* note 4, ¶ 323).

262. Amicus Brief, *supra* note 37, at 8 (citing Michigan v. EPA, 135 S. Ct. 2688, 2710 (2015) (". . . a court may uphold agency action only on the grounds that the agency invoked when it took the action") (citing SEC v. Chenery Corp., 318 U.S. 80, 87 (1943))); Perez v. Mortg. Bankers Ass'n, 135 S. Ct. 1199, 1209 (2015) (quoting FCC v. Fox TV Stations, Inc., 556 U.S. 502, 515 (2009)); Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 6, 73; Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 50–52.

263. *See* Lazaro Gamio, *How Data Travels Across the Internet*, WASH. POST (May 31, 2015), https://www.washingtonpost.com/graphics/national/security-of-the-internet/bgp/ [https://perma.cc/SX3N-MTAN].

264. Vernotte et al., *supra* note 3, at 18.

265. *Cf.* Charles Kelly & Philip Carden, *Firewalls: Securing NT Networks from Internet Intruders*, IT PRO TODAY (Oct. 31, 1996), https://www.itprotoday.com/security/firewalls-securing-nt-networks-internet-intruders [https://perma.cc/53J6-XG7C] ("[A] network firewall is a hardware/software barrier between a corporate network and the Internet.").

crosses the ISP-controlled gateway to the internet.[266] No software patch or firewall protects a user from an ISP whose job it is to transit that user's content to and from the internet.[267]

Suggestions to use a Virtual Private Network (VPN) to obscure the content of internet traffic from the user's ISP "won't protect you from data-throttling that kicks in when you've used too much of your monthly data allotment."[268] When the D.C. Circuit, in *USTA v. FCC,* upheld the FCC's 2015 *Open Internet Order*, it cited the FCC's analysis that, "convincingly detailed how broadband providers' [gatekeeper] position in the market gives them the economic power to restrict edge-provider traffic and charge for the services they furnish."[269]

Without legally enforceable net neutrality rules, internet subscriber cyber-hygiene cannot stop an ISP from blocking, throttling, disadvantaging, interfering with, or degrading traffic that runs through the ISP's network. ISPs already exist inside the internet network. Thus the FCC's net neutrality rule repeal initiated a zero-day cyber vulnerability for the energy sector's reliability.

Kristen E. Eichensehr pointed out that zero-day vulnerabilities present, "national security risks if a foreign government discovers and exploits it against, for example, [United States] critical infrastructure."[270] Paid priority accounts may become a hacker target as favored messages are accelerated, and other traffic may be slowed to accommodate those with priority.[271] Launching paid priority accounts, which impair other traffic during times of likely heavy load, such as hot days or extreme weather events, compounds reliability risks to the energy sector.

The FCC's net neutrality repeal allows ISPs to sell priority to some users, even if doing so degrades other traffic, and to block, throttle, degrade, disadvantage, or interfere with traffic, as long as the ISP discloses that it

266. Verizon v. FCC, 740 F.3d 623, 646 ("[T]here appears little dispute that broadband providers have the technological ability to distinguish between and discriminate against certain types of Internet traffic.").

267. *See* Tyson, *supra* note 30. *Cf.* Vernotte et al., *supra* note 3, at 20 (noting that an energy smart grid cybersecurity, "mechanism can be structural/physical e.g., a more advanced network segregation, and/or software based, e.g., a more frequent patching strategy.").

268. *How to Stop ISP Throttling*, PIXEL PRIVACY, https://pixelprivacy.com/resources/stop-isp-throttling/ [https://perma.cc/AZN7-XU8E].

269. Verizon v. FCC, 740 F.3d at 646.

270. Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 484 (2017).

271. Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 55.

engages in prioritization agreements.[272] I previously warned in *Internet Freedom* docket Reply Comments that paid priority would, "allow ISPs to 'deprioritize' the signals of other Americans to speed ahead those who pay for Internet priority."[273] The FCC's *Internet Freedom Order* permits ISPs to manage internet traffic in their own business interest with no internet user safeguards.[274]

Guo et al. analyze paid priority in a market with duopoly ISP competition and competing content providers vying for internet bandwidth.[275] Under net neutrality rules that prohibit paid priority, ISPs charge consumers fees for internet access, "which are their only revenue source. In the packet discrimination regime, in addition to fixed fees . . . from consumers," they observe that, "ISPs may also charge the [Content Providers] usage-based fees . . ., respectively, for preferential delivery of their content."[276] "In other words, ISPs have two revenue sources in the packet discrimination regime: Internet access fees from consumers and preferential delivery fees from CPs."[277]

Guo et al. then explained, "[w]ithout net neutrality regulation, the competing ISPs still have the incentive to charge CPs for preferential delivery, and in the presence of CP competition, they have the ability to induce CPs to pay for packet prioritization."[278] Their model found that, "some advantaged CPs may benefit from paid prioritization because such arrangements further enforce their dominance in the content market. Paid prioritization, however, always hurts the disadvantaged CPs."[279] Guo et al.'s model illustrates that without enforceable net neutrality rules, ISPs in duopoly local markets can use their gatekeeper position to obtain revenue from content providers to avoid data queuing delays due to ISP network management practices.[280]

This model made no assumptions about the content being sent through the internet. Neither does this model analyze whether the ISP subscriber sending or receiving internet content has any legal duties it executes in part through the use of internet services. The internet's historical "best efforts"

---

272. *See* FCC, *Internet Freedom Order, supra* note 4, ¶¶ 2–4, 220 (repealing FCC rules adopted in 2015 that prohibited ISPs from blocking, throttling, or paid prioritization of Internet traffic except for limited reasonable network management justifications); *cf.* FCC, *2015 Open Internet Order*, *supra* note 5, ¶¶ 215–16.

273. *See* Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 27.

274. FCC, *Internet Freedom Order, supra* note 4, ¶¶ 2–4, 220.

275. Guo et al., *supra* note 256, at 358.

276. *Id.*

277. *Id.*

278. *Id.* at 367.

279. *Id.*

280. *Id.* at 361.

treatment of internet traffic is agnostic to packet content, sender, or recipient.[281] Discriminatory preference for some data packets based on paid priority thwarts "best efforts" for all internet data packets.

ISP Comcast argued for repeal of the paid priority ban arguing that doing so would allow it to sell priority to latency-sensitive applications such as signing for the hearing impaired or autonomous vehicles.[282] AT&T argued that the eliminating paid priority ban would allow it to, "begin implementing isolated paid-prioritization arrangements to support [QoS] for unusually latency-sensitive applications, such as high-definition videoconferencing or massively multiplayer online gaming (MMOG)."[283]

In April 2019 ISP Cox launched a $15 a month "priority routing" service it claims will offer Internet gamers a speed and latency advantage.[284] Cox contends that this service "does not alter speed in any way nor does it prioritize any traffic over others on our network"[285]—a description met with technical doubt. Cox announced this limited trial in Arizona, but it did not disclose any methods it will deploy to measure whether other internet traffic is degraded or affected by the video-gamer priority routing service.

I previously cautioned that an, "ISP's priority deal with a video game provider—whether foreign or domestic—could impact a range of

---

281. FTC, BROADBAND CONNECTIVITY COMPETITION POLICY, at *2, 2007 WL 2506639 (Traditionally, data traffic has traversed the Internet on a "first-in-first-out" and "best-" basis); FCC, *2015 Open Internet Order*, *supra* note 5, at 83 n.148 (concluding ISPs have incentives to use their gatekeeper power in the Internet to extract tolls on Internet users, citing Mozilla's comments that paid priority "represents a visceral deviation from the end-to-end, best efforts history of the Internet, meaning that as a practical matter, it's impossible to understand ex ante the full effects and potential negative externalities that could arise.").

282. Comments of Comcast Corporation, *In the Matter of Restoring Internet Freedom*, WC Docket No. 17-208, at 56 (July 17, 2017), https://ecfsapi.fcc.gov/file/107171777114654/2017-07-17%20AS-FILED%20Comcast%202017%20Open%20Internet%20Comments%20and%20Appendices.pdf [https://perma.cc/MY2Z-UM64]; Jacob Kastrenakes, *Comcast Says It Should Be Able to Create Internet Fast Lanes for Self-Driving Cars*, THE VERGE (July 17, 2017), https://www.theverge.com/2017/7/17/15985114/comcast-paid-prioritization-autonomous-cars [https://perma.cc/5RW3-D68C].

283. Comments of AT&T Services Inc., *In the Matter of Restoring Internet Freedom*, 17-108, at 365 (July 17, 2017), https://ecfsapi.fcc.gov/file/10717906301564/AT%26T%20Internet%20Freedom%20Comments.pdf [https://perma.cc/DT5S-RB5Y].

284. Karl Bode, *This ISP Is Offering a 'Fast Lane' for Gamers. . .For $15 More Per Month*, MOTHERBOARD (Apr. 25, 2019), https://motherboard.vice.com/en_us/article/neabyw/this-isp-is-offering-a-fast-lane-for-gamersfor-dollar15-more-per-month [https://perma.cc/C74E-A3XG].

285. *Id.*

communications to and from the subscriber's account. The ISP's priority transmission of the video game may delay the grid operator's or utility's signal to a demand response aggregator, and the energy resource's reply."[286] ISP paid priority deals with other parties, "may delay a demand response communication with an Internet-connected thermostat or a DER, or a DER's response to a request to provide voltage support. Such conduct undermines electric reliability for the sake of the ISP's profit and the video game's benefit."[287]

Paid priority purchasers may not reveal their motives, affiliations, or true identities to ISPs, as "[t]he FCC Order imposes no limits on who—foreign or domestic—could buy paid priority."[288] Similar to the Russian use of Facebook to perpetrate election interference in 2016 and, as reported by Facebook in June 2018, for the United States mid-term elections,[289] the ISP need not be aware of or sympathetic to the buyer's motives for paid priority to cause harm.

The DOJ and FCC argued in Respondents' brief defending the FCC's *Internet Freedom Order* that the FCC, "reasonably 'determined that replacing the prohibitions on blocking and throttling with a transparency rule implements a lower-cost method of ensuring' that any harms 'are exposed and deterred by market forces, public opprobrium, and enforcement of the consumer protection laws.'"[290] Respondents' brief argued that the FCC's transparency rule provided appropriate "light-touch" regulation, preferable to net neutrality rules.[291]

Nick Feamster argued that net neutrality repeal may provide opportunities to offer service level guarantees to internet users, including non-commercial users.[292] Feamster hoped that FCC network management disclosure rules would provide transparency into ISP practices to allow for informed consumer decision-making and monitoring.[293]

---

286. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 47.

287. *Id.*

288. *Id.* at 4.

289. Sara Frier, *Facebook Finds Ongoing Evidence of Election Interference*, BLOOMBERG (July 31, 2018), https://www.bloomberg.com/news/articles/2018-07-31/facebook-finds-ongoing-evidence-of-election-interference ("Facebook said it notified the U.S. government and deleted dozens of accounts and pages from people using false identities, who were coordinating events and stirring up political unrest. The campaign is similar to the one Russia-linked groups ran around the 2016 presidential elections, though the company doesn't know who's behind it this time.").

290. *Respondents' Brief, supra* note 261, at 74–75.

291. *Id.* at 95.

292. Richard Bennett, *What's the Deal with Software-Defined Networking?*, HIGH TECH FORUM (Feb. 22, 2018), http://hightechforum.org/whats-the-deal-with-software-defined-networking/ [https://perma.cc/3ZXK-NF5V].

293. *Id.*

I previously discussed the limited disclosures the FCC's transparency rule requires: "Tracking the words of the FCC's required disclosure, an ISP's terms of service could state that it engages in a 'practice that directly or indirectly favors some traffic over other traffic, including through use of techniques such as traffic shaping, prioritization, or resource reservation, in exchange for consideration, monetary or otherwise.'"[294] Notably, "FCC's 2018 Order does not require ISPs to disclose the parties to or terms of paid priority transactions, the execution of such deals, or their consequences. Neither does the FCC's Order require ISPs to get their subscriber's consent to paid priority deals."[295] Any disclosures ISPs engage in (e.g., paid priority, traffic shaping), "does not inform consumers, content providers, or regulators of priority deals, or when and how the ISP will launch priority or degrade other service."[296]

The FCC's limited transparency and disclosure rules contribute to "market opacity and lack of transparency about buyer and seller behavior," both of which are hallmarks of a zero-day cybersecurity vulnerability.[297] Mailyn Fidler observed that zero-day "[v]ulnerabilities are most exploitable if kept secret. Zero-days are discovered and not made, so there is no guarantee someone in possession of a vulnerability is the only person who knows about it. The value of secrecy complicates efforts to control the zero-day trade because it contributes to market opacity and lack of transparency about buyer and seller behavior."[298] Information about zero-day vulnerabilities is valuable and may create opportunities and markets for its trade.[299] Lack of FCC disclosure requirements for paid priority deal terms, execution, or their consequences for other internet users creates a secrecy characteristic of zero-day cybersecurity vulnerability information which should not be ignored.

Responsible entity energy operators and regulators cannot rely on limited disclosures that an ISP may engage in, for paid priority or other traffic shaping, or resource reservation techniques to ensure that energy signals are not

294. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 41 (citing FCC, *Internet Freedom Order*, *supra* note 4, ¶¶ 216, 220).
295. *Id.*
296. *Id.*
297. Fidler, *supra* note 2, at 410.
298. *Id.* at 409–10.
299. *Id.* at 410 ("Zero-days are traded in three markets . . . the 'white market' encompasses sales of vulnerabilities between zero-day vulnerability hunters and software vendors or third-party clearinghouses. The 'black market' describes interactions where the buyer or the seller has criminal intent. The 'gray market' involves interactions between vulnerability sellers and government agencies, conducted as legal business deals.").

subject to ISP disadvantage or interference. The FCC's ISP transparency rules are inadequate to protect energy grid reliability.

Neither the energy sector, regulators, nor others with public safety duties should be faced with the Hobson's choice of paying ISPs for protection against the ISP's own degradation of internet traffic, or risking the consequences of paid priority degradation. Unwinding dependence on mass-market internet services is inconsistent with the energy sector's distributed nature that harnesses the public internet to seed the smart grid. Forcing energy market participants to pay for private line, non-mass market communications services such as the ECN private line used to communicate with CAISO raises costs and introduces market entry delays.[300] Paying ISPs for internet priority or safeguards from paid priority delays increases energy costs thereby undermining efforts to adopt just and reasonable rates as required by federal and state statutes. Respondents' brief to the D.C. Circuit in the net neutrality appeal argued that paid priority could facilitate entry of small "edge providers" (i.e., small internet content providers).[301] However, Respondents neither offered an analysis to support this belief, nor considered the range of "edge providers," such as energy operators, their suppliers, regulators, and consumers, who all provide internet content and act to varying degrees as "edge providers." So long as blocking and throttling do not require reasonable network management justifications, any edge provider like an energy provider may be throttled and thereby forced into a prioritization arrangement to provide reliable service to utility customers. This is a frightening reality we can no longer ignore.

Neither Respondents' brief nor the *Internet Freedom Order* analyzed small energy resources and other energy market participants who use the internet to carry out duties imbued with cybersecurity and reliability responsibilities. Paid priority must be addressed as it can undermine the functionality of communications-enabled smart inverters connected to the internet and raise costs for meeting reliability and cybersecurity rules.

A "utility or energy market participant who enters a paid priority deal with an ISP may risk allegations that such a deal makes them a party to energy market manipulation."[302] An energy operator that contracts with an ISP to prioritize its traffic risks disadvantaging other energy resources ranging from energy generators to rooftop solar panels, behind-the-meter batteries, or even electric substations that use the same ISP and internet physical and network resources. Such deals could not only raise costs for

---

300. CAISO, SC CERTIFICATION OVERVIEW, *supra* note 244, at 4.

301. *Respondents' Brief*, *supra* note 261, at 69 (citing FCC, *Internet Freedom Order*, *supra* note 4, ¶¶ 133, 255).

302. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 52.

other energy market participants, but they could also reduce reliability and public safety.

Additionally, "ISP priority for its own energy management signals over those of independent resources could be subject to a FERC market manipulation investigation under the FPA."[303] CAISO requires energy generators to communicate every four seconds, a standard NERC notes is common for many energy resources.[304] Internet priority given to one resource risks slowing other resources and communication to other internet-connected devices used in the energy ecosystem.

I emphasized in comments to the FCC's 2014 *Open Internet* docket and in the *Internet Freedom* docket that:

> FERC forbids "anticompetitive conduct and conduct that threatens market transparency" because it "undermine[s] confidence in the energy markets and damage[s] consumers and competitors. Such conduct might involve the violations of rules designed to limit market power or to ensure the efficient operation of regulated markets." A FERC market participant who bargains to get better Internet speeds or lower prices than its competitors may be engaging in a practice that threatens market transparency and violates market rules.[305]

Even if FERC were to find market manipulation due to paid internet priority agreements, any rate refund would only compensate for rates higher than those which are "just and reasonable."[306] FERC's refund process does not "provide a remedy for harms to safety, reliability, or environmental harm from having to call on more or build more [greenhouse gas]-emitting peaker plants."[307]

Neither does the ability to use private lines or commercial Internet services secure all energy utility, ISO or RTO, or energy resource communications.

---

303. *Id*. (citing *In re* Enron Corp., 326 B.R. 257, 264 (Bankr. S.D.N.Y. 2005) (noting that FPA, 16 U.S.C § 824(e), "provides FERC with broad remedial authority to address anticompetitive behavior" supporting FERC's authority to order disgorgement of money in excess of just and reasonable rates upon a finding of market manipulation during the California Energy crisis of 2000 to 2001)).

304. N. AM. ELEC. RELIABILITY CORP., BALANCING AND FREQUENCY CONTROL 13 (2011), https://www.nerc.com/docs/oc/rs/NERC%20Balancing%20and%20Frequency%20Control%20040520111.pdf [https://perma.cc/4LJ2-ZM4G].

305. Catherine J.K. Sandoval, *Written Statement of Commissioner Catherine J.K. Sandoval Before the Congressional Forum on Net Neutrality, Hosted by Congresswoman Doris O. Matsui*, at 16 (Sept. 24, 2014) (footnotes omitted) [hereinafter *Commissioner Sandoval 2015 Open Internet Ex Parte Comments*].

306. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 52.

307. *Id.*

The 1995 National Science Foundation decision to lift restrictions on the internet to access to "support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work" opened the internet to commercial use, increasing its reach and range of applications.[308] The internet allows every user to communicate with any other user, increasing the network's utility and value. The distributed energy ecosystem embeds the internet's network. Distributed energy networks require that all parts of the system, from generators to customers—including customers who may sometimes act as generators—regulators, suppliers, and others—can reliably communicate.

IoT proliferation illustrates the distributed energy ecosystem's dependence on an open and neutral internet. "We used to think of the home as the grid edge where people consumed electricity but did not produce it. Dr. Mahmoud Daneshmand observed the smart grid era is pushing sensors and, thus, visibility, into the distribution system, where the grid presumably 'ends.'"[309] "[D]igitization and internet of things" are fundamental to smart grid operation, and will be "even more so in the future," Vernotte et al. observe.[310] The smart grid "enables a home or a building to serve as an energy generator, or to decrease or shift energy on demand to aid the grid, save money, prevent blackouts, and protect the environment by reducing [greenhouse gas] emissions."[311] "The need to protect open and neutral Internet access for the energy sector is commensurate with the distributed energy ecosystem's reach," my 2018 Article argued.[312]

"For utilities with millions of customers such as Southern California Edison (SCE), an investor-owned electric utility (IOU) regulated by the CPUC, with over 4.9 million customer connections, negotiating Internet access agreements with multiple ISPs to reach their 14 million customers would be costly, risky, and fraught with uncertainty," my comments to the FCC's 2014 and 2018 net neutrality proceedings observed.[313] Energy reliability, safety, just and reasonable rates, and achievement of environmental objectives to forestall climate change depends on all of us—energy sector customers

---

308. Jane K. Winn, *Crafting A License to Know from A Privilege to Access*, 79 WASH. L. REV. 285, 297 (2004).

309. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 18 (citing Dr. Mahmoud Daneshmand, *Big Challenges for Big Data in the Smart Grid Era*, ECN MAG. (Apr. 4, 2017), https://www.ecnmag.com/blog/2017/04/big-challenges-bigdata-smart-grid-era [https://perma.cc/4CTG-YLCC]).

310. Vernotte et al., *supra* note 3, at 2.

311. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 18.

312. *Id.*

313. Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 50–51 (citing *Commissioner Sandoval 2015 Open Internet Ex Parte Comments*, *supra* note 305, at 2, 3).

and generators, researchers, regulators, suppliers, public safety personnel, and others—not just on entities that can afford or access a commercial internet connection. The ability to use mass market internet services protected by enforceable net neutrality rules such as those adopted in the FCC's 2015 *Open Internet Order* is crucial to energy sector reliability, safety, the environment, national security, and our democracy.

If a responsible entity in the energy sector detected a third-party slowing energy internet signals, delaying system communications, and causing some latency-sensitive or data-rich communications to fail due to delays, they should call Homeland Security and the FBI, and notify the industry via a NERC Alert. DHS and the FBI would coordinate to identify the perpetrator and stop the throttling and traffic degradation. The United States Attorneys' Office would determine if the perpetrator could be prosecuted for cybercrimes or for sabotage of the energy system. The hacker paradigm obscures the risks of paid priority, throttling, or blocking behavior by ISPs authorized by the FCC's repeal of net neutrality rules.

Under FERC cybersecurity rules, responsible entities must ensure supply-chain cybersecurity. ISPs are a key energy sector supplier. Responsible entities are accountable to FERC rules for ISP cybersecurity including ISP-induced cyber vulnerabilities. FERC's grid reliability and resiliency docket should analyze ISP contracts and conduct. States and localities with responsibility for energy providers and resources must also act to ensure that ISP conduct does not undermine energy reliability and resiliency. The Energy-Internet nexus underscores the importance of aligning ISP governance with energy reliability and cybersecurity duties, and the energy system's interconnected nature makes communications failures with energy resources a reliability and safety issue for the entire grid—not just for the energy resource or ISP subscriber.

VII. THE ENERGY-INTERNET NEXUS: GRID COMMUNICATIONS ENABLE RELIABILITY, RESOURCE, AND ENVIRONMENTAL GOALS AT JUST AND REASONABLE RATES

A. The Energy-Internet Nexus

As the GAO reported in 2005, more grid functions are being executed through ICT, a trend which will likely grow. Those communications functions are not just done through closed proprietary, utility-owned networks or commercial plans. Increasingly, energy communications use the internet for some or all of the transport path.

As noted by the GAO, "[s]ince the early 1990s, increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business."[314] In 2017, Rafael Leal-Arcas observed that, "[a]n Internet for energy interconnects the energy network with the Internet, allowing units of energy (locally generated, stored, and forwarded) to be dispatched when and where it is needed."[315] Leal-Arcas's observation does not describe a separate "Internet for energy," but instead it emphasizes the centrality of the internet to energy management. The GAO's 2005 Cybersecurity Report noted, "[w]hile the benefits have been enormous, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support."[316]

The Energy-Internet nexus has grown as electric grid planning, operation, resource dispatch, control, and maintenance increasingly depend on the internet. This is a natural growth because reliable communications are essential to the integration of renewables, demand response, and other resources. As the grid edge blurs to include behind the meter resources such as batteries, smart thermostats, and rooftop solar, many of which are connected to residential Wi-Fi, home and business, governance of mass-market internet connections has become critical to protecting electric reliability and deploying climate change solutions.

B. Electric Grid Functions, Management, Oversight, and Planning Increasingly Rely on Communications and Information Technology, Including the Internet

1. Electric Grid Regulators Rely on the Internet

The internet is crucial to the electric grid's daily function, as well as to the natural gas system that supplies electric plants and natural gas consumers. Regulators including ISOs and RTOs that oversee the BES under FERC jurisdiction rely on the internet to ensure grid reliability and cybersecurity. CAISO, for example, uses, "the Alert, Warning, & Emergency (AWE) Tool as needed to issue Emergency notifications. Subscribers receive these alerts

314. GAO, *Critical Infrastructure Protection*, *supra* note 112, at 1.

315. Rafael Leal-Arcas, *Sustainability, Common Concern, and Public Goods*, 49 GEO. WASH. INT'L L. REV. 801, 877 n.379 (2017) (citing *Internet of Energy for Electric Mobility*, INTERNET OF ENERGY, http://www.artemis-ioe.eu/ [https://perma.cc/E8PU-6Q4T]).

316. GAO, *Critical Infrastructure Protection*, *supra* note 112, at 1.

via email and the ISO Today app."[317] "NERC Alerts" depend on the internet to send emails to "[n]otify the entire industry of an alert via email within minutes" about cybersecurity vulnerabilities.[318]

CAISO also uses the public internet for energy dispatch communications to scheduling coordinators, "representing any generation or participating loads within the ISO control area or planning to import generation at the ISO control area interties."[319] These scheduling coordinators (SC) are the only entities, "authorized to transact business directly with the ISO."[320] In regards to the importance of the internet to CAISO operations, many CAISO products and services require use of web-based applications to submit bids, receive market information, track grid status information, and take part in market simulations.[321]

SCs must decide whether to establish and maintain communications with CAISO through the ECN private network run by AT&T for a monthly fee, with a connection initiation time of 30–45 business days.[322] CAISO also allows SCs to communicate through the public internet with, "little or no cost for setup and maintenance and minimal setup time."[323] CAISO noted, "[i]f the internet carrier selected by an SC has an availability issue, it may affect the SC's ability to communicate with the ISO."[324] Moreover, CAISO imposes no service quality standards on the scheduling coordinator's use of the public internet for communication. CAISO, SCs, market participants, and others must recognize the risks to energy reliability net neutrality repeal triggers.

---

317. CAL. INDEP. SYS. OPERATOR, REAL-TIME COMMUNICATIONS GUIDELINES, PROCEDURE 5110, at 8 (2018), https://www.caiso.com/Documents/5110.pdf [https://perma.cc/RG5G-9VZA].

318. Todd Thompson & Chris Lada, *NERC Alert System, Overview*, N. AM. ELECTRIC RELIABILITY CORP. 6 (2010), https://www.npcc.org/Library/Workshops/20100921TFIST06.pdf [https://perma.cc/5E57-LMCS].

319. CAL. INDEP. SYS. OPERATOR, 10.5 SYSTEMS ACCESS INFORMATION FOR MARKET PARTICIPANTS 10 (Feb. 1, 2019), http://www.caiso.com/Documents/SystemAccessInformation_MarketParticipants.pdf [https://perma.cc/F7UU-YEVR].

320. CAL. INDEP. SYS. OPERATOR, SC CERTIFICATION OVERVIEW, *supra* note 244, at 1.

321. *See* CAL. INDEP. SYS. OPERATOR, 10.5 SYSTEMS ACCESS INFORMATION FOR MARKET PARTICIPANTS (Feb 1, 2019), http://www.caiso.com/Documents/SystemAccessInformation_MarketParticipants.pdf.

322. CAL. INDEP. SYS. OPERATOR, SC CERTIFICATION OVERVIEW, *supra* note 244, at 4.

323. *Id.*

324. *Id.*

2. *The Electric Grid's Distributed Nature and Distributed Energy Resources Rely on the Internet to Achieve Service, Cost, and Environmental Goals*

a. Grid Resource Telemetry Increasingly Depends on the Internet

To promote renewable and DER integration as well as lower cost and market entry barriers, CAISO created options for participating energy generators to use the internet for grid operations telemetry. CAISO requires that generating units and load participants, such as those authorized to dispatch power or to provide load shifting resources such as demand response, "must establish and maintain a data processing gateway between plant facilities and the ISO energy management system for the purpose of generation control and monitoring."[325]

CAISO requires, "direct telemetry of participating generators and load by installing a remote intelligent gateway (RIG) for generating units providing regulation energy or a data processing gateway (DPG) or other ISO-approved technology for resources providing non-regulation ancillary services or supplemental energy."[326] RIGs work in real time to enable CAISO, "to collect data and distribute supervisory control commands to and from generators as well as transfer this data to and from multiple central monitoring and supervisory control sites."[327] CAISO requires data encryption and controls data delivery media to ensure "that a [p]articipating [g]enerator reliably receives ISO [supervisory control and data acquisition (SCADA)] system instructions according to their participation agreements."[328]

In 2016, while the FCC's net neutrality rules were in force, CAISO began allowing participating generators to communicate telemetry through the internet using designated programs to promote security.[329] In 2017, CAISO authorized the company Dispersive Technologies to provide connectivity at the resource owner's site to CAISO's EMS.[330] This option allows communication using, "an Internet Service Provider broadband connection (Ethernet, DSL, cellular IP, satellite IP, or wireless) as the local access to

---

325. *Metering and Telemetry Ensure Accurate Revenue Accounting, Metering and Telemetry Are Mandatory Tools for Ensuring Accurate Revenue Accounting and ISO Operational Visibility*, CAL. INDEP. SYS. OPERATOR, http://www.caiso.com/participate/Pages/MeteringTelemetry/Default.aspx [https://perma.cc/HHR4-WH2H].

326. *Id.*

327. BUSINESS PRACTICE MANUAL FOR DIRECT TELEMETRY, *supra* note 36, at 21.

328. *Id.*

329. *Assigned Commissioner's Ruling Entering Workshop Report into the Record and Seeking Comment* (R.13-12-011), CAL. PUB. UTIL. COMM'N (Oct. 26, 2016), at Attach B, CAISO Presentation, at slide 5 [hereinafter CPUC, *Assigned Commissioner's Ruling R.13-12-011*].

330. CAISO, *New Resource Implementation Process Enhancement*, *supra* note 249.

the public internet. There is no need for resource owners to maintain digital certificates or provision T1 lines for ECN connectivity."[331]

Dispersive Technologies described itself as an, "Internet-based, software-defined network for use by California's energy grid operator to efficiently and effectively connect entities using real-time devices to the grid's energy management system." Dispersive Technologies' software-defined network (SDN) requires "only a standard broadband connection to the public [i]nternet," making it "easier and less expensive to install than other networks. A utility or cogeneration plant can deploy it in days rather than weeks."[332]

Lowering operational and entry costs is critical to enabling dispatch of renewable energy resources. Energy market resources must bid and compete on costs to obtain dispatch orders. The Supreme Court explained in *FERC v. Electric Power Supply Ass'n* that grid operators, "accept the generators' bids in order of cost (least expensive first) until they satisfy the LSEs' [load service entity such as a utility] total demand."[333] Reducing costs to acquire and maintain communications channels suitable to CAISO standards facilitates renewable generation deployment and achievement of environmental goals, including climate change solutions.

Regarding its decision to authorize a public internet connection for participating generators, CAISO reported that "[o]ver time, the reliability of the public [i]nternet has improved but cyber threat to public networks has increased."[334] CAISO reported that Dispersive Technologies features an "integrated firewall" to protect field assets and ensure "highly secure communications."[335] As discussed above in section V(c), firewalls may protect against hackers but will not block ISP network management techniques for internet traffic crossing their network.

---

331. *Dispersive Technologies and California ISO Launch First Software-Defined Network for Critical Infrastructure,* CISTON PR NEWSWIRE (Aug. 1, 2017), https://www.prnewswire.com/news-releases/dispersive-technologies-and-california-iso-launch-first-software-defined-network-for-critical-infrastructure-300497529.html [https://perma.cc/9VLB-6YVF].

332. *Id.*

333. FERC v. Elec. Power Supply Ass'n, 136 S. Ct. 760, 763 (as revised Jan. 28, 2016) (citing Order No. 745, *Demand Response Compensation in Organized Wholesale Energy Markets*, 134 F.E.R.C. ¶ 61187 (2011). *See e.g.*, *Market Processes and Products*, CAL. INDEP. SYS. OPERATOR, http://www.caiso.com/market/Pages/MarketProcesses.aspx [https://perma.cc/GCV2-XUAB] (describing CAISO market using bids to meet energy needs).

334. BUSINESS PRACTICE MANUAL FOR DIRECT TELEMETRY, *supra* note 36.

335. *Distributed Energy Resource Provider*, CAL. INDEP. SYS. OPERATOR, http://www.caiso.com/participate/Pages/DistributedEnergyResourceProvider/Default.aspx [https://perma.cc/WN36-38FX].

b. The Internet Enables Demand Response, Load Reduction and Shifting as an Energy Resource

In 2016, FERC approved a new type of ISO market participant called a Distributed Energy Resource Aggregator (DERA).[336] CAISO allows DERS and DERAs to participate in its wholesale energy market through the energy resources they control or aggregate through contracts. "Distributed energy resource providers are market participants who own or operate an aggregation of distributed energy resources in order to participate in the wholesale market."[337]

CAISO reported that prospective DERA market participants sought the public internet instead of the ECN to provide telemetry to CAISO and reduce barriers to entering ISO markets.[338] CAISO allows DERAs to connect to its grid operations through the public internet using the Dispersive Technology SDN.[339]

c. Four Second Grid Communications: Telemetry Requirements in the CAISO Market

CAISO imposes speed requirements on participating generator telemetry to ensure grid visibility, dispatch, reliability, and control. Under CAISO rules, a "[p]articipating [g]enerator must be able to accept and begin processing direct digital control (DDC) signals (Set Points) within the ISO time standard (two-second maximum from ISO's EMS to output of the Real-Time Device)". This "two-second maximum includes any Generator or third-party communication equipment located between the ISO and the Participating Generator."[340] Further, "the plant controller must receive the signal from the Real-Time Device within the ISO time standard (an additional two seconds from output of the Real-Time Device to plant controller)."[341] These time signals and "time standards also apply in the return direction, resulting in a total maximum of eight seconds, round trip, for the signal to travel from the ISO EMS to the plant controller and back."[342]

CAISO's two-second time standard for participating generators for the sending or receiving of signals (that is, four-seconds per completed dispatch and receipt) allows grid visibility, and the ability to initiate grid controls if needed. Participating generators may be located on a residential or

336. BUSINESS PRACTICE MANUAL FOR DIRECT TELEMETRY, *supra* note 36.
337. *Distributed Energy Resource Provider*, *supra* note 335.
338. BUSINESS PRACTICE MANUAL FOR DIRECT TELEMETRY, *supra* note 36.
339. *Id.*
340. *Id.*
341. *Id.*
342. *Id.*

commercial rooftop and connected to that user's Wi-FI, which runs on the public internet. Energy generators may be located at a solar "farm," a plot of land with a cluster or solar panels and controls, a parking lot, or other urban, suburban, or rural location. The distributed location of energy resources illustrates the imperative of addressing ISP network management practices to protect energy reliability and cybersecurity.

d. Seconds Count for Grid Communications, Reliability, and Safety

NERC noted that most, "SCADA systems poll sequentially for electric system data, with a typical periodicity of four seconds."[343] In the CAISO market, "DER facilities larger than 1 MW in size must communicate 3 data points with the utility every 4 seconds: voltage, real power, and reactive power."[344] "Facilities larger than 9.9 MWs must communicate every 4 seconds the three data points above, as well as the following statuses: plant on, plant off, and circuit breaker status."[345] Data can be transported to the utility or grid operator over various media that in 2016 ranged, "from plain old telephone lines to Voice Over Internet Protocol or cellular services."[346]

Communications provide visibility into grid assets and enable control measures that can prevent localized or cascading outages. NERC determined that lack of visibility contributed to the 2011 cascading blackout that began in Arizona, spread to northern Mexico, and then blacked out all of San Diego and Imperial counties, as generators tripped off and load leaned on other sites.[347] A line worker's error in Arizona caused a line in Imperial County, California to overload and seek an alternate route for power in San Diego. "IID's 42 kv system started to collapse within 40 seconds of initial 500 kv line trip."[348] Within eleven minutes of the error in Arizona and cascading blackouts, protection breakers in front of the San Onofre Nuclear Power plant disconnected when it sensed a surge in load.[349] This grid separation

343. N. AM. ELEC. RELIABILITY CORP., BALANCING AND FREQUENCY CONTROL, *supra* note 304.
344. *See* CPUC D.16-12-047, *supra* note 26, at 18.
345. *Id.*
346. *Id.*
347. W. ELEC. COORDINATING COUNCIL (WECC), MODULE 9: PRINCIPLES OF POWER SYSTEM OPERATION 135 (June 2015), https://www.wecc.biz/Administrative/=INTRO_MOD_9-Grid%20Ops=rev2015-June.pdf [https://perma.cc/J88J-E9YT] (noting lack of information sharing between entities contributed to cascading outage and loss of load).
348. *Id.* at 138.
349. *Id.* at 141.

prevented the great Western blackout from spreading into Orange County, Los Angeles, and beyond. Increased communication and visibility would have helped to prevent this cascading outage from spreading into San Diego County and other regions.

e. Grid Communications Including Fault Detection Relayed Through the Internet to Protect Reliability and Public Safety

The CPUC Water-Energy Nexus December 2016 decision noted that under then-existing standards, "many DER assets connected to the distribution grid sized at 99 MW, aggregated together, do not currently communicate with the utility or California Independent System Operator (CAISO) at all, which masks generation and load."[350] In "grid fault situations, facilities trip off, but load remains. As the grid comes back online, there may be large power swings to consider and manage for the safety of communities and the grid. Today that management is largely done by controls on the electric grid, rather than through communications signals."[351]

CPUC's decision concluded that, "[e]nabling communications that provide visibility would offer much-needed information about load conditions. Communications-based controls would reduce risks and costs associated with such events."[352] At the CPUC's October 26, 2016 Water-Energy-Telecommunications Nexus workshop, participants discussed communications requirements for energy resources and their grid consequences. Energy generators and major facilities such as substations must have a "Class A telecom signal" used for the, "direct transfer trip protection scheme" that maintains electric system safety and reliability.[353] Class A signals must "work before, during, and after a fault."[354] "Propagation delay of the Class A telecom signal of 5-10 cycles is tolerable though grid stability can be impacted by less than 3 cycles."[355]

The United States electric grid operates at 60Hz (Hertz) or 60 cycles per second.[356] Applying the math, 5–10 cycles normally travels the electric grid operating at 60 cycles per second in less than one-quarter of a second. Communications delays exceeding 5–10 cycles may trip off energy resources

---

350. CPUC D.16-12-047, *supra* note 26, at 18–19.
351. *Id.* at 19.
352. *Id.*
353. CPUC, *Assigned Commissioner's Ruling R.13-12-011*, *supra* note 329, at 3.
354. *Id.*
355. *Id.*
356. *60 Hz*, POWER SYS. CONTROLS, https://www.pscpower.com/60hz/ [https://perma.cc/5LXL-AKL4]. A 60Hz electrical system means that it does 60 cycles of frequencies per second. Marshall Brain, *How Power Grids Work*, CLARK SCI. CTR., http://www.science.smith.edu/~jcardell/Courses/EGR220/ElecPwr_HSW.html [https://perma.cc/85Y4-K8G4].

to protect grid safety. Similarly, SCADA systems require prompt and consistent communications, and "SCADA at the transmission system requires 3–5 seconds communications of signals. SCADA at the distribution level require less than 30 second communications."[357]

Communications promote reliability, safety, just and reasonable rates, and achievement of environmental goals, each of which is mandated by California law and other state law. The CPUC emphasized that, "California Public Utilities Code [s]ection 451 commands us to ensure water and energy service that is safe and reliable, at just and reasonable rates. That helps achieve our goals of protecting the public and environment."[358] CPUC observed that, "[t]elecommunications service is critical to doing so now, and will be even more critical in the future."[359] These observations also hold true for FERC-jurisdictional, as well as other state-regulated energy resources.

f. Communications-Enabled Smart Inverters Provide Visibility and Enable Grid Control and DER Dispatch

In 2011 California Governor Brown called for the implementation of 12,000 MW of "localized electricity generation" to help the State reach its goal to acquire 33 percent of its energy from eligible renewable energy resources by 2020.[360] The California Energy Commission (CEC) and CPUC expressed concern that, "[h]igh penetrations of these DER systems, located within distribution grids which were designed only for handling customer loads, could adversely affect California utility operations."[361] The CEC and CPUC worked together with a public working group including technical experts to develop strategies and protocols to facilitate DER integration critical to achieving renewable energy goals.

Inverters are used to produce Alternating Current (AC) power used in the United States electric grid from resources such as wind and solar photovoltaic (PV) systems that produce Direct Current (DC) power.[362] Hydroelectric

357. CPUC, *Assigned Commissioner's Ruling, R.13-12-011*, *supra* note 329, at 3.
358. *Id.* at 17–18.
359. *Id.* at 18.
360. *Candidate DER Capabilities: Recommendations for Updating Technical Requirements in Rule 21* (R.11-09-011), CAL. PUB. UTIL. COMM'N, V. 15, at 2 (May 22, 2013).
361. *Id.*
362. *Alternate Decision Instituting Cost Certainty, Granting Joint Motions To Approve Proposed Revisions to Electric Tariff Rule and Providing Smart Inverter Development A Pathway Forward for Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company* (D.16-06-052), CAL. PUB. UTIL.

and biomass generating units, which produce AC power, do not require inverters.[363] The CPUC reported that as of June 2016 in California, "about 90% of small scale renewable generation is connected to the distribution grid through inverters."[364]

Inverters typically have limited communications functionality, communicating only a stop or go signal for energy exports from a solar or wind energy resource. Software applications control most inverters, "and therefore many of their electrical characteristics can be modified through software settings."[365] Thus, "[t]hese software applications can cause the inverters to change the real power output, voltage levels, power factor, and other electrical characteristics, and can be used to improve the power system efficiency."[366]

Communications-enabled smart inverters provide visibility and control that foster reliability, safety, and renewable resource deployment. In its 2016 Long-Term Reliability Assessment, NERC noted many utilities "lack sufficient visibility" of DERs.[367] Lack of visibility results in "lack of situational awareness," a term NERC defines as, "'ensuring that accurate information on current system conditions is continuously available to operators.'"[368] CPUC observed that visibility gained "in person if needed, and control, through grid protections from faults if not through communications, is critical to maintaining electric safety."[369] "The difference between the current grid and the future grid with smart inverters used for hyper local grid protection is an infusion of communications."[370]

Communications capable inverters, "can respond to occasional commands to override or modify their autonomous actions by utilities and/or retail energy providers (REPs)."[371] Because "DER systems can be designed

---

COMM'N (June 23, 2016), http://docs.cpuc.ca.gov/publisheddocs/published/g000/m164/k376/164376491.pdf [hereinafter CPUC D.16-06-052].

363. *Id.*

364. *Id.*

365. *Id.* at 3–4.

366. *Id.* at 4.

367. N. AM. ELEC. RELIABILITY CORP., 2016 LONG-TERM RELIABILITY ASSESSMENT, at vii. (Dec. 2016), http://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/2016%20Long-Term%20Reliability%20Assessment.pdf [https://perma.cc/S5NE-TN4W].

368. FERC, DISTRIBUTED ENERGY RESOURCES, TECHNICAL CONSIDERATIONS FOR THE BULK POWER SYSTEM (Docket No. 18-10-000), at 12 (Feb. 2018), https://www.ferc.gov/CalendarFiles/20180215112833-der-report.pdf [https://perma.cc/Y4G2-WW2X] (quoting N. AM. ELEC. RELIABILITY CORP., REAL-TIME TOOLS SURVEY ANALYSIS AND RECOMMENDATIONS STAFF REPORT 3 (Executive Summary) (2008), https://www.nerc.com/comm/OC/Realtime%20Tools%20Best%20Practices%20Task%20Force%20RTBPTF%2020/Real-Time%20Tools%20Survey%20Analysis%20and%20Recommendations.pdf [https://perma.cc/P349-DDBL]).

369. CPUC D.16-12-047, *supra* note 26, at 19.

370. *Id.* at 19.

371. *Id.*

to include sensors that monitor local conditions of voltage levels, frequency deviations, and temperature, and can receive emergency commands and pricing signals," DER systems may, "modify their power and reactive power output."[372] Communications capabilities can be added to inverters, which allows settings to be updated as needed, or permits scheduling updates on a daily, weekly, and seasonal timeframe.[373]

I authored an Interconnection Decision in June 2016 as a CPUC Commissioner which adopted a process that set a schedule for smart inverter communications and functionality protocols to promote renewable integration.[374] As of November 2017, California required smart inverters and pledged communications protocols would become mandatory for smart inverters in California in early 2019, just six months after the adoption of communications standards.[375]

The CPUC allows smart inverters to communicate through a variety of media including "cellphone channels, AMI networks, private utility networks, communications network of their choice and the Internet."[376] Solar resources may utilize the internet, VPN, or a to communicate with data centers for data exchange, financial risk assessment, grid operations, SCADA, regulatory reporting, and other applications.[377]

Commonly, solar resources at residential and business properties use the premise's Wi-Fi to connect the inverter to the internet, enabling solar panel monitoring.[378] An inappropriately secured inverter presents a cyber risk for the facility owner that could undermine grid reliability, particularly if

372. CAL. PUB. UTIL. COMM'N, APPENDIX A, REDLINE EDITS CORRESPONDING TO COMMENTS OF THE DIVISION OF RATEPAYER ADVOCATES, CANDIDATE DER CAPABILITIES: RECOMMENDATIONS FOR UPDATING TECHNICAL REQUIREMENTS IN RULE 21, V15, at 4 (May 22, 2013), http://docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M076/K851/76851169.pdf [https://perma.cc/TA34-SS86].

373. *Id.*

374. CPUC D.16-06-052, *supra* note 362, at 41.

375. *Id*. at SIWG Rule 21 Phase 2 Recommendations for the CPUC 1–2.

376. *Id*. at SIWG Rule 21 Phase 2 Recommendations for the CPUC 5.

377. PRESENTATION, SUNSPEC ALL., INFORMATION STANDARDS FOR DISTRIBUTED ENERGY 5 (Oct. 2015), https://sunspec.org/wp-content/uploads/2015/10/SunSpecESNAOpen MeetingOct13.pdf [https://perma.cc/CE75-6GL9].

378. Scott Partlin, *3 Ways on How to Communicate with a Solar Inverter*, SMA CORPORATE BLOG 3 (Apr. 6, 2015), https://www.sma-sunny.com/en/3-ways-on-how-to-communicate-with-a-solar-inverter/ [https://perma.cc/Q789-9QZP].

multiple solar resources were compromised.[379] Joel B. Eisen & Felix Mormann observed that "[m]any DERs and devices that control them will be located at customer sites with little or no computer security and with owners who have minimal or no cybersecurity expertise."[380]

Net neutrality repeal compounds DER cyber vulnerability. If DER communications are delayed due to an ISP's traffic management policies or paid priority with other internet users, then grid reliability, safety, and renewable dispatch can be undermined.

VIII. TESTING THE GRID FOR COMMUNICATIONS-INDUCED FAULTS AND CASCADING FAILURES

A. Electric Trips

The electric grid interconnects to and depends on a range of distributed energy resources to support its ability to serve energy load while reducing the grid's carbon emissions. This interconnected design also makes the electric grid vulnerable to outages that may cascade across the grid in seconds. Benjamin Schäfer et al. observed that individual electric line overloads that trip outages can take place in seconds.[381] For example, the 2006 European blackout left fifteen million European households without power.[382] The European Commission attributed the blackout's origin to E.ON Netz, the electricity transmission system operator in Northern Germany, which switched off a high voltage line to let a ship pass underneath the line.[383] The EC found that E.ON Netz did not have proper security procedures and lacked, "the full technical tools to verify that the system operated within the security limits."[384]

This incident led to "overloading of lines and finally to splitting of the Union of Co-ordination of Electricity Transmission network into three zones:

---

379. William Westerhof, *How to Protect Your Solar Inverter From Hackers*, SOLAR QUOTES BLOG 2 (Feb. 19, 2018), https://www.solarquotes.com.au/blog/solar-inverter-security-hackers/ [https://perma.cc/ZUP9-LZDH].

380. Joel B. Eisen & Felix Mormann, *Free Trade in Electric Power*, 2018 UTAH L. REV. 49, 112.

381. Benjamin Schäfer et al., *Dynamically Induced Cascading Failures in Power Grids*, 9:1975 NATURE COMM. 1, 2 (2018), https://www.nature.com/articles/s41467-018-04287-5.pdf [https://perma.cc/437Y-CY97].

382. UNION FOR THE COORDINATION OF TRANSMISSION OF ELEC., FINAL REPORT, SYSTEM DISTURBANCE ON 4, NOVEMBER 2006, at 5–6 (2006), https://www.entsoe.eu/fileadmin/user_upload/_library/publications/ce/otherreports/Final-Report-20070130.pdf [https://perma.cc/YNS6-Y6W6].

383. Press Release, European Commission, Blackout of November 2006: Important Lessons to Be Drawn (Jan.30, 2007) (on file with author at http://europa.eu/rapid/press-release_IP-07-110_en.htm?locale=en [https://perma.cc/JX9L-LD25]).

384. *Id.*

West, East and South-East. The Western zone lacked power and the Eastern zone had too much power."[385] During this event, "33 high-voltage transmission lines tripped within a time period of 1 min and 20 s, with 30 of those lines failing within the first 19 s[econds]."[386] Similarly, the U.S. electric grid is designed to trip facilities to prevent imbalances that could lead to electrical overload, fires, electrocution, and other dangers. In the CAISO grid, "[i]f voltage goes below 80% everything trips off within 2 seconds."[387]

B. Modeling Internet-Induced Electricity Outages

ICT can help reduce the risk of grid fluctuations that exceed the grid's tolerance and time levels.[388] At the same time, electric grid internet use introduces cybersecurity vulnerabilities. Juan Hoyos, Mark Dehus, and Timothy X Brown argue the "transition from analog to digital data acquisition allows the power industry to innovate with new communications technologies and protocols" while posing, "new cybersecurity problems that can affect the stability and reliability of the power grid."[389]

Hoyos, Dehus, and Brown modeled a hack on the Generic Object Oriented Substation Events (GOOSE) protocol, which is used in the electric industry to distribute event data across electric substation networks.[390] GOOSE's main purpose is to carry vital information (alarms, status, and control) between devices. This is important because "[a]ny alteration of these values could can cause an automation breakdown, causing a circuit breaker to miss an operation, bypassing interlocks, or causing physical damages in the field devices like power transformers or circuit breakers."[391] "A GOOSE attack that appears to change the values of generation levels could produce voltage dips, frequency excursions, and cascading problems throughout the Western Electricity Coordinating Council . . . region."[392]

---

385. *Id.*
386. Schäfer et al., *supra* note 381, at 2.
387. CPUC, *Assigned Commissioner's Ruling R.13-12-011*, *supra* note 329, Attach. A, at 6.
388. Schäfer et al., *supra* note 381, at 2 (noting that cascading events will become more likely in the future due to increasing load and additional fluctuations in the grid).
389. Juan Hoyos, Mark Dehus, Timothy X Brown, *Exploiting the GOOSE Protocol: A Practical Attack on Cyber-Infrastructure*, 2012 IEEE GLOBECOM Workshops 1508, http://ecee.colorado.edu/~ekeller/classes/fall2014_advsec/papers/goose_globecomm12.pdf [https://perma.cc/ZU9M-PJ8R].
390. *Id.*
391. *Id.* at 1510.
392. *Id.*

Hoyos, Dehus, and Brown conducted an, "ethical demonstration of security vulnerability in the Digital Energy Laboratory at the University of Colorado Boulder, with details of the equipment and scripts intentionally omitted."[393] Their simulated hack enabled malware to control certain substation equipment that, "has the potential to cause outages that range from a single feeder on up."[394] They recommend several security measures and emphasized "it is of vital importance that the configuration of the network switch and routers be permitted just for trusted traffic and users inside the substation network."[395]

Chih-Che Sun et al. developed and simulated an energy grid cyber-attack at Washington State University's (WSU) Smart City Testbed. In one demonstration, "attackers are assumed to have the knowledge to access multiple substation communication systems. By capturing and analyzing unencrypted GOOSE packets, attackers are able to modify and resend them to trip circuit breakers in targeted substations."[396] "In the first attack scenario, attackers' targets are substations 38, 35, 33 and 32 since these substations connect to generation sources. The attack starts at t [time] =5 s[econds], and the targets are compromised one by one every 5 s[econds]."[397] Then, "[o]nce the last targeted substation (i.e., substation 32) is compromised, this power system collapses due to insufficient power generation."[398] Next, "[a]fter 4 generators are disconnected from the power grid, cascading events are triggered. Finally, a wide area power outage is caused by the coordinated cyber-attacks."[399]

ISOs also use grid simulators to analyze the "impact of data feed losses, data corruption, and dispatcher tool functionality" and to identify potential vulnerabilities.[400] PJM studies have focused on, "identifying vulnerabilities such as the loss of a substation or common mode outages such as the loss of generation fed from common gas infrastructure"[401] PJM has not studied "the effects associated with the loss of multiple substations or critical system components as could be contemplated in a coordinated physical attack" or in a coordinated cyber-attack.[402] This Article recommends ISOs, energy sector participants, and state PUCs should conduct simulations of ISP-induced signal degradations or delays to determine their effect on grid reliability and renewable integration.

---

393. *Id.*
394. *Id.* at 1512.
395. *Id.*
396. Sun et al., *supra* note 92, at 54.
397. *Id.*
398. *Id.*
399. *Id.*
400. PJM, *FERC Grid Resilience Comments*, *supra* note 54, at 19.
401. *Id.* at 35–36.
402. *Id.*

IX. NET NEUTRALITY REPEAL UNDERMINES PUBLIC SAFETY AND ENERGY RELIABILITY

A. The DOJ's and FCC's Defense of its Failure to Consider Public Safety in the Net Neutrality Repeal Mischaracterizes the Record and Overlooks the FCC's Statutory Duties

The DOJ's and FCC's brief defending the FCC's *Internet Freedom Order* against appeal represented to the D.C. Circuit that, "Petitioners did not raise any issues in this proceeding that were distinct to public safety."[403] Respondents' mischaracterize the record in the *Internet Freedom* docket. My search of the FCC's Electronic Comments Filing System (ECFS) for the Internet Freedom docket found 417 filings that mention "public safety" in that proceeding's record.[404]

Respondents overlook the fact that the *Internet Freedom Order* dismissed my comments expressing concern about the consequences of paid priority for national security, public safety, and critical infrastructure including energy. In a footnote the FCC derisively stated "[n]or do we think we need to address assertions that paid prioritization would endanger [United States] national security as they are vague and lack any substantiation whatsoever."[405]

My *Internet Freedom* docket Reply Comments cited federal and state law duties to protect critical infrastructure including the energy sector, CIPA, PPD-21, President Trump's 2017 Executive Order on Cybersecurity, and the Countering America's Adversaries with Sanctions Act (finding that the Russians used the internet to interfere with United States elections) as statutes that require the FCC to consider the impact of net neutrality repeal on public safety and critical infrastructure including the energy sector.[406] In the *Internet Freedom* docket, I filed my 2014 testimony to a Congressional Democratic Committee hearing about the importance of net neutrality

403. *Respondents' Brief*, *supra* note 261, at 96.

404. ECFS Search for filings with the term in full text "lack of competition," for Rulemaking 17-108, conducted on Oct. 27, 2018, https://www.fcc.gov/ecfs/search/filings?proceedings_name=17-108&q=%22public%20safety%22&sort=date_disseminated, DESC.

405. FCC, *Internet Freedom Order*, *supra* note 4, at n.943.

406. *See* Critical Infrastructures Protection Act of 2001 (CIPA), Pub. L. 107-56, tit. X, § 1016, 115 Stat. 272, 400; *PPD-21*, *supra* note 163; Exec. Order No. 13800, 82 Fed. Reg. 22391, § 2(d) (May 16, 2017); *President Trump Executive Order 13,800 on Cybersecurity*, *supra* note 183; Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44, Title II, 131 Stat. 886 (2017), https://www.congress.gov/bill/115th-congress/house-bill/3364/text?q=%7B%22search%22%3A%5B%22sanctions%22%5D%7D&r=2 [https://perma.cc/82SF-H3CS].

to critical infrastructure including energy, which emphasized federal and state energy reliability and safety duties that could be compromised by blocking, throttling, paid priority, and "minimum speed" requirements.[407] That testimony, "discussed in detail why individualized bargaining proposals [for minimum Internet speeds or paid priority] endanger critical infrastructure, which relies on the open Internet for services such as energy demand response to prevent electrical blackouts."[408]

The *2015 Order* considered critical infrastructure sector needs in rejecting proposals to allow paid priority or individualized negotiations for fast internet access with a "minimum speed" guaranteed.[409] The FCC's 2015 decision to reject paid priority cited my comments submitted when I served as a CPUC Commissioner, which asserted that paid priority would increase "barriers to adopting Internet-based applications," such as Internet-enabled demand response deployed to "prevent power blackouts, forestall the need to build fossil-fueled power plants, promote environmental sustainability, and manage energy resources."[410]

Government Petitioners challenging the FCC's *Internet Freedom Order* as arbitrary and capricious under the APA highlighted the importance of net neutrality to public safety, critical infrastructure, and energy reliability. The Government Petitioners' brief argued that "[i]nstant communication between customers, suppliers, energy generators, contractors, regulators, and safety personnel is essential to maintaining a safe and reliable grid, and must thus remain free from blocking or delay due to throttling or deprioritization."[411] Government Petitioners also cited my comments about the importance of the open internet to energy resource management and reliability: "California has relied on demand response services offered by utilities and third parties to directly balance load, manage congestion, and

---

407. Letter from Catherine J.K. Sandoval, Commissioner, California Public Utilities Commission, to Marlene H. Dortch, Secretary, F.C.C., GN Docket No. 14-28, 10-127, Attach. at 14 (filed Oct. 14, 2014) [hereinafter Commissioner Sandoval, *Ex Parte Letter*].

408. *Commissioner Sandoval 2015 Open Internet Ex Parte Comments*, *supra* note 305, at 59 n.266.

409. *FCC, 2015 Open Internet Order*, *supra* note 5, at 49; *id.* at n.254 (citing Commissioner Sandoval *Ex Parte Letter*, *supra* note 407, Attach. at 14 ("[A]ny of the minimum level of access standards the FCC proposes would be insufficient to support the needs of a diversity of Internet users including Critical Infrastructure.")).

410. *Id.* at 6 (citing *FCC, 2015 Open Internet Order*, *supra* note 5, at 55 n. 291. *See also* FERC v. Electric Power Supply Ass'n., 136 S. Ct. 760, 768–69, as revised (Jan. 28, 2016) ("Wholesale demand response . . . pays consumers for commitments to curtail their use of power, so as to curb wholesale rates and prevent [electric] grid breakdowns.")).

411. Brief for Government Petitioners at 24, Mozilla Corp., et al. v. FCC, Case No. 18-1051 (D.C. Cir. Court of Appeals) (Nov. 27, 2018) (citing 42 U.S.C. § 5195c; Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 47).

satisfy state and federal reliability standards."[412] They emphasized that other states, such as Massachusetts, have demand response programs and would be equally affected by net neutrality repeal.[413]

The CPUC's *Internet Freedom* docket comments emphasized that: "States have independent and primary authority, under both energy and telecommunications law, which is to say under both the Federal Energy Regulatory Commission (FERC) and FCC regulatory regimes, to ensure the safety of the energy and communications infrastructure."[414] The CPUC cited the Energy Policy Act of 2005 which provides, "it shall not 'be construed to preempt any authority of any State to take action to ensure the safety, adequacy, and reliability of electric service within that State, as long as such action is not inconsistent with any reliability standard.'"[415]

The CPUC also emphasized that under California Public Utilities Code Section 451, California utilities have an obligation, "to protect the safety and health of the public."[416] The CPUC added that, "without non-discriminatory rules, providers of emergency services or public safety agencies might have to pay extra for their traffic to have priority. If states, cities, and counties were required to pay for priority access, their ability to provide comprehensive, timely information to the public in a crisis could be profoundly impaired."[417]

CPUC's comments in the *Internet Freedom* docket also emphasized, "[p]rotection of public safety" as "a core exercise of a state's police powers."[418] CPUC noted as examples of its exercise of police power the rules CPUC adopted to ensure the safety of all poles and conduit in California by promulgating rules related to overhead electric and communications facilities (General Order 95) as well as underground electric and communications facilities (General Order 128). The CPUC underscored the, "FCC cannot diminish this state police power to protect public safety and welfare,

412. *Id.* at 24 (citing Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 47).

413. *Id.* at 25 (*see, e.g.*, MASS. GEN. LAWS ch. 25, § 21(b) (2019) (mandating energy efficiency plans that include demand response programs); Rockland Elec. Co., Case No. ER16060524 (N.J. Bd. of Pub. Util., Aug. 23, 2017).

414. CPUC, Comments, *In the Matter of Restoring Internet Freedom*, *supra* note 110, at 4–5.

415. *Id.* at n.9.

416. *Id.* at 5.

417. *Id.* at 29.

418. *Id.* at 5.

notwithstanding whether it reclassifies BIAS, or otherwise attempts to preempt state action regarding utility poles."[419]

Although the CPUC cited utility pole regulation as an example of state responsibility under the state police power, its citations to federal and state authority and concern for public safety are not limited to utility poles. CPUC's comments emphasized the state's responsibility for "to ensure the safety of the energy and communications infrastructure."[420] The CPUC also emphasized that, "a free and open [i]nternet is critical to areas such as energy, education, medicine, and public safety."[421] As CPUC's comments demonstrated, the energy sector's distinct public safety concerns about net neutrality repeal arise from federal statutory duties to ensure energy reliability and cybersecurity, as well as state duties to ensure safe, reliable service, at just and reasonable rates, and compliance with environmental mandates.

The CPUC also expressed concern that, "as the *2015 Open Internet Order* discusses, the absence of strong anti-discriminatory rules could undermine critical infrastructure and public safety."[422] Each paragraph CPUC cited from the FCC's 2015 *Open Internet Order* adopting net neutrality rules referenced, as a basis for adopting those rules, my comments filed in the *Open Internet* proceeding, as well as the comments of other parties.[423]

Santa Clara County informed the FCC through an *ex parte* letter filed in December 2017 that, "[s]ince 2010, [Santa Clara] County has invested heavily in developing and implementing systems that provide key public health, welfare, and safety services to the local community over the internet, and has current plans to implement many more such systems."[424] The

---

419. *Id.*

420. *Id.*

421. *Id.* at 27.

422. *Id.* (citing *See, e.g.*, FCC, *2015 Open Internet Order*, *supra* note 5, ¶¶ 114, 126, 150).

423. FCC, *2015 Open Internet Order*, *supra* note 5, ¶ 114 n.254; *id.* ¶ 126 n.291. *See e.g.*, Commissioner Sandoval, *Ex Parte Letter*, *supra* note 407, at 2 (asserting that paid prioritization undermines public safety and universal service, and increases barriers to adopting Internet-based applications such as Internet-enabled demand response communications electric and gas utilities use to prevent power blackouts, forestall the need to build fossil-fueled power plants, promote environmental sustainability, and manage energy resources); FCC, *2015 Open Internet Order*, *supra* note 5, ¶ 150, n.355 (citing Commissioner Sandoval, *Ex Parte Letter*, *supra* note 407, at 14 (asserting the commercial reasonableness rule would deter investment and Internet applications, such as Internet-enabled "Smart beds," which read a patient's vital signs and send aggregated data on available beds to mass casualty and disaster planners who use this information to determine which hospital has an available bed in a burn unit)).

424. Letter from James R. Williams, County Counsel, Santa Clara County, Office of the County Counsel, to Marlene H. Dortch, Secretary, FCC, *Ex Parte Letter*, Restoring Internet Freedom WC Docket No. 17-108, at 1 (Dec. 6, 2017), https://ecfsapi.fcc.gov/file/12079423

County explained that public safety depends on community access to an open and neutral internet: "The County's and County Fire's newly implemented, internet-based services depend, in many cases, on community members' access to broadband internet on nondiscriminatory terms—in other words, they depend on net neutrality principles like those articulated in the Net Neutrality Rules."[425] The County further explained that, "[i]f traffic to and from these systems is blocked, delayed, or subjected to paid prioritization schemes or other discriminatory practices, the County's and County Fire's ability to effectively provide services to the community would be significantly weakened."[426] These services are provided pursuant to Santa Clara County's governmental duties, which it largely fulfills through the internet.[427]

The County emphasized that *post-facto* enforcement through other laws would be insufficient to protect distinct public safety obligations and needs: "Because many of these systems are used in emergency situations and to protect health and safety, after-the-fact action to address internet service provider (ISP) practices is insufficient to address the harm that the County, County Fire, and the community, are likely to suffer."[428] Santa Clara County offered its virtual Emergency Operations Center as an example, explaining the Center is, "used by the County and County Fire to coordinate crisis response [and] relies on contributors' access to the internet on nondiscriminatory terms. Interference with this system would cause irreversible damage."[429]

The Alarm Industry Association and alarm company ADT also submitted comments in the *Internet Freedom* docket. They expressed concerns that

---

20842/2017.12.06%20-%20Comment%20of%20County%20of%20Santa%20Clara%20and%20Santa%20Clara%20County%20Central%20Fire%20Protection%20District.pdf [https://perma.cc/2WVS-2XPY] [hereinafter, *Santa Clara County Internet Freedom ex parte*].

425. *Id.*

426. *Id.*

427. *Id.* at 6 ("Under California's emergency management framework, the County Office of Emergency Services (OES) is the lead emergency management agency for the entire Santa Clara County Operational Area (Op Area)."). California's Standardized Emergency Management System (SEMS), CA Code of Regulations (CCR) Title 19, section 2401, provides the state's emergency management framework. *See* CPUC D.16-12-066, *Decision on Rural Call Completion Issues, Other Call Completion Issues and Call Initiation Issues Including Lack Of 911 Access and Dial Tone*, at 73, CAL. PUB. UTIL. COMM'N (Dec. 1, 2016), http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M171/K301/171301678.pdf. (noting that SEMS divides by governmental level responsibility for incident command). *See id.* at 74 (citing CAL. CODE REGS. tit. 19, § 2403(b) (2016) ("There are five designated levels in the SEMS organization: field response, local government, operational area, regional, and state. Each level is activated as needed.").

428. *Santa Clara County Internet Freedom ex parte*, *supra* note 424, at 2.

429. *Id.*

paid priority would interfere with public safety. The Alarm Industry Communications Committee observed that, through paid-priority, ISPs who compete with the association's members can deprioritize, degrade, or interrupt alarm transmissions, "running contrary to the Commission's statutory obligation to promote network development to support public safety."[430] The Alarm Industry Association emphasized, "[i]n emergency situations, seconds could mean the difference between life and death."[431] State and local laws impose legal obligations on the alarm industry through service standards, including a maximum transmission time for an alarm signal to travel from the premises to the central monitoring station.[432] The ability to comply with state, local, and federal legal obligations to protect public safety, life, and limb, can be compromised by the ISP paid priority, throttling, blocking, and network management practices the FCC's *Internet Freedom* Order authorized.

Given the multitude of comments from various industries impacted by the evolving net neutrality rules, the D.C. Circuit should take a dim view of the DOJ's and FCC's mischaracterization of the record in the *Internet Freedom* docket. Public safety, energy reliability mandates, and environmental risks consequent from the net neutrality repeal were raised in the record and cited by the FCC's 2015 *Open Internet Order* as reasons for adopting net neutrality rules.[433] The APA requires the FCC to explain its divergence from the agency's prior decision.[434] Moreover, the FCC is statutorily mandated to consider public safety in its decision-making, and to articulate its consideration of those issues.[435]

Verizon's July 2018 interference with the Santa Clara County Fire Protection District's internet use during an active firefight provides an example of ISP exercise of throttling power presaged by Santa Clara County's December 2017 *ex parte* comments. The 2015 *Open Internet Order* would have enabled the *Fire District* to file a complaint with the FCC arguing Verizon violated net neutrality rules applicable to mass-

---

430. Alarm Industry Communications Committee, Reply Comments, Restoring Internet Freedom WC Docket No. 17-108, at 5 (Aug. 30, 2017), https://ecfsapi.fcc.gov/file/10830023 2601598/AICC.NN%20Reply%20Comments.v6-FINAL.pdf [https://perma.cc/TW86-YJ4R]. *See also* ADT, Reply Comments Restoring Internet Freedom WC Docket No. 17-108, at 3–4 (Aug. 30, 2017), https://www.fcc.gov/ecfs/filing/10830125808530 [https://perma.cc/ UN8U-MHY3].

431. Alarm Industry Communications Committee, Reply Comments, *supra* note 430, at 5.

432. *Id.*

433. *2015 Open Internet Order*, *supra* note 5, ¶¶ 114 n.254, 126 n.291, 150 n.355.

434. Amicus Brief*, supra* note 37, at 5 (citing Perez v. Mortgage Bankers Ass'n, 135 S. Ct. 1199, 1209 (2015) (quoting FCC v. Fox TV Stations, Inc., 556 U.S. 502, 515 (2009) ("the Commission failed to explain its departure from its previously expressed views, rendering its decision 'arbitrary and capricious' and contrary to law").

435. *Id.* at 4 (citing Nuvio Corp. v. FCC, 473 F.3d 302, 307 (D.C. Cir. 2006). *See also* Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 47.

market Internet services (if used by the *Fire District*) by slowing the unit's Internet speeds to act "more like an AOL dial up modem from 1995," no longer supporting "a modern broadband internet connection," and "hampering operations for the assigned crew."[436] "The *2015 Order* shielded emergency responders using mass-market [i]nternet services through *ex ante* rules *and* an *ex post* enforcement process rooted in FCC jurisdiction."[437] This legal shield also protected the energy sector and other critical infrastructure from ISP blocking, throttling, paid priority, and unreasonable interference or disadvantages. To the extent emergency responders use services not subject to the *2015 Order*, the FCC should examine whether repeal of all net neutrality rules and the FCC's abdication of jurisdiction over ISPs is sufficient to protect government and emergency services, and critical infrastructure.

B. ISP Verizon Throttled the Santa Clara County Fire Protection District's Internet Use During California's Largest Firefight: Public-Safety Zero-Day Vulnerability

In July 2018, while the Santa Clara County, California Fire Protection District (Fire District) was fighting the Mendocino Complex Fire—which evolved into California's largest fire[438]—Verizon throttled the unit's "unlimited" data plan once the Fire District used 25 gigabits of data that month.[439] Verizon slowed the Fire District's internet speeds to act "more like an AOL dial up modem from 1995," no longer supporting "a modern broadband internet connection," and "hampering operations for the assigned crew."[440] Fire District personnel reported, "the department Verizon device is experiencing speeds of 0.2Mbps/0.6Mbps, meaning it has no meaningful functionality."[441] Government Petitioners reported Verizon, "did not cease throttling even when informed that this practice threatened public safety."[442] The amicus brief I co-filed with Professors Hammond, Chase, and Byerly in support

436. Amicus Brief, *supra* note 37, Add. 2–4.
437. *Id.* at 11.
438. Top 20 Largest California Wildfires, CAL. DEP'T OF FORESTRY & FIRE PROT. (Mar. 14, 2019), https://www.fire.ca.gov/communications/downloads/fact_sheets/Top20_Acres.pdf [https://perma.cc/W7TF-5DR7].
439. Amicus Brief, *supra* note 37, at 11 (citing Brief for Gov't Petitioners, *supra* note 411).
440. *Id.* (citing Brief for Gov't Petitioners, *supra* note 411, Add. 11).
441. Amicus Brief, *supra* note 37, at 11.
442. *Id.* at 23.

of Petitioners in the net neutrality appeal observed, "the ISP would not have slowed had the user been watching an ISP's 'zero-rated' entertainment video exempt from ISP data caps."[443]

The CPUC's Water-Energy-Telecommunications Nexus Decision discussed modern firefighters' reliance on real-time geographic information system (GIS) mapping to monitor fires and coordinate emergency response, track information, and save lives.[444] As such, "[n]et neutrality repeal left public safety agencies unable to rely upon GIS and other Internet applications that require more bandwidth than an email, software updates, or cached video."[445]

Fire fighters should not have to fight a fire like its 1995, let alone 1895. The internet is one of the most transformational firefighting tools deployed in the past half century. ISP-induced dial-up speeds rob fire-fighters, all of the agencies with whom they coordinate, and the public of the ability to use high-speed internet applications to more effectively fight, detect, and escape fires and protect public safety.

C. ISPs Have Not Promised to Forswear from Throttling or Paid Priority that Effects the Distributed Energy Ecosystem and Energy Reliability

After Petitioners' brief appealing the *Open Internet Order* disclosed Verizon's throttling of the Fire Protection District's internet speed during the Mendocino Complex Fire, Verizon publicly promised not to slow the data of first responders on the West Coast and Hawaii.[446] Verizon then promised, "in the event of another disaster, it will lift restrictions on public safety customers, providing full network access."[447] Notably, Verizon's promise is triggered only, "in the event of another disaster." Verizon does not define who will determine whether a disaster exists or the time frame after disaster declaration that it will lift restrictions on "public safety customers." Verizon also failed to define who qualified as a "public safety customer." Are energy utilities public safety customers when they support fire-fighters by managing energy resources during a fire fight? Are energy utilities, resources, regulators, and the distributed energy ecosystem "public

443. Amicus Brief, *supra* note 37, at 12.
444. *See* CPUC D.16-12-047, *supra* note 26, at 33–34.
445. Amicus Brief, *supra* note 37, at 12.
446. Wendy Davis, *Verizon Promises to Stop Throttling First Responders*, MEDIA POST (Aug. 24, 2018), https://www.mediapost.com/publications/article/324091/verizon-promises-to-stop-throttling-first-responde.html [https://perma.cc/L559-LNU4].
447. *Verizon Statement on California Wildfire and Hurricane Lane in Hawaii*, VERIZON (Aug. 24, 2018), https://www.verizon.com/about/news/verizon-statement-california-wildfires-and-hurricane-lane-hawaii [https://perma.cc/5YVK-AZ3U].

safety customers" at all times or only during designated emergencies? Verizon's press release promise does not protect daily operation or management for critical infrastructure sectors including energy and water.

Verizon's institutional focus on "public safety customers" ignores the role of the public in protecting public safety. The internet's distributed nature allows the public to post videos of fires, including fire escape routes. These videos can be life-saving for neighbors and first responders. Flood monitoring through internet-enabled river gauges and public posting of videos that inform flood protection districts, first responders, and communities of flood dangers protect life and property. The distributed energy network relies on all of its users, suppliers, researchers, public safety, regulators, and the public to achieve energy reliability, public safety, and environmental goals. Verizon's promise not to throttle "public safety" agencies in a disaster failed to recognize that community internet access is key to public safety.

The DOJ and FCC *Internet Freedom* appeal brief argued that ISPs will quickly respond to problems, citing as an example, Verizon's pledge not to throttle Public Safety customers after disclosure of its dramatic slowing of the Fire District during a major firefight.[448] The FCC argued to the D.C. Circuit that ISPs have no business incentives to "intentionally impair public safety," because doing so will result in "public opprobrium" and "fierce consumer backlash."[449]

The FCC's reliance on *post facto* solutions after the customer publicly reveals ISP network management interference leaves customers, public safety, and energy reliability exposed to ISP conduct. For the energy sector, throttling, paid priority that degrades other users, intentional interference or disadvantage, blocking, or other preferential ISP practices thwart vital energy operations, reliability, and public safety. Whether the ISP's goal was to "intentionally impair public safety" does not excuse the FCC, ISPs, the federal government, or energy regulators from turning a blind eye to the public safety consequences of such actions.

PPD-21 directs the Secretary of Homeland Security to "develop situational awareness capability for critical infrastructure, requiring action to address evolving threats and consequences."[450] ISP reservation of contractual rights to engage in such conduct based on the FCC's net neutrality repeal leave critical

448. *Respondents' Brief*, *supra* note 261, at 95.
449. *Id.* at 95 (citing FCC, *Internet Freedom Order*, *supra* note 4, ¶¶ 264, 323).
450. *PPD-21*, *supra* note 163.

infrastructure including the energy sector vulnerable to the consequences of ISP throttling and traffic interference.

ISPs have not promised to abstain from thwarting energy ecosystem participants. No public promises have been made to responsible entities in the energy system, nor to those who use the public internet for energy system functions such as DERAs, market bidders, ISOs, or energy consumers.

D. ISP Contractual Reservation of Network Management Rights Highlight Cybersecurity Vulnerabilities

ISP Contracts including their Terms of Service reveal that many prominent ISPs reserved rights to engage in paid priority or manage internet traffic in a manner that may pose reliability and cybersecurity risks. The FCC characterized Verizon's throttling of the Fire District as a single incident Government Petitioners highlighted to illustrate net neutrality repeal's public safety risks.[451] Respondent's brief underscored that, "numerous [broadband providers], including the four largest fixed [providers], have publicly committed not to block or throttle the content that consumers choose."[452] Verizon's citation of its contract plans and network management practices in the midst of its insistence that the Santa Clara Fire District had to pay $2.00 a month more and switch to a new play to restore internet speeds underscore that ISP contracts document cyber vulnerabilities.

Government Petitioners' net neutrality appeal brief attached the Declaration of Santa Clara County Fire Protection District Chief Anthony Bowden, including emails to and from Verizon as the Fire District sought to end the throttling during the firefight. An email from Silas Buss of Verizon to Santa Clara fire officials emphasized, "[i]n short, Verizon has always reserved the right to limit data throughput on unlimited plans. All unlimited data plans offered by Verizon have some sort of data throttling built-in, including the $39.99 plan" that Santa Clara subscribed to through its government account.[453] The Fire District and Verizon went back and forth with emails and calls for several days as Verizon insisted that the Fire District had to switch to a different plan for $2.00 a month more, or a more expensive plan.[454]

A brief examination of ISP publicly-available contract terms for internet use reveals ISP's reservations of rights that pose cybersecurity vulnerabilities.[455]

---

451. *Respondents' Brief*, *supra* note 261, at 94.

452. *Id.* at 72 (citing FCC, *Internet Freedom Order*, *supra* note 4, ¶ 264).

453. Government Petitioners Addendum, Brief for Gov't Petitioners, *supra* note 411, Declaration of Fire Chief Anthony Bowden, Add. 8.

454. *Id.* (citing Declaration of Fire Chief Anthony Bowden, Add. 10–11).

455. Thanks to my research assistant, Luke Batty, Santa Clara Law third year student, for his research on ISP contract terms regarding network management promises and policies.

Verizon's network management policies states that it does not block or throttle lawful content but prioritizes under reasonable network management. Verizon also offers prioritization under Dedicated Access plans.[456] The FCC's 2015 *Open Internet Order*'s excluded network management done in the ISP's business interests from the reasonable network management exception to net neutrality rules.[457] The 2018 *Internet Freedom Order* removed that restriction, allowing ISPs to manage the internet in their business interest.[458]

Comcast, according to their Network Management practices page, states that, "Comcast does not discriminate against lawful internet content, applications, services or non-harmful devices."[459] In its Network Management Disclosure, Comcast contends it does not participate in blocking, throttling, affiliated prioritization, or paid prioritization.[460]

Comcast announced in June 2018 that, "it no longer needs to throttle speeds for heavy internet users, ending a network-management technique it has been using since 2008."[461] Comcast also emphasized that it, "reserve[s] the right to implement a new congestion management system if necessary in the performance of reasonable network management and to maintain a good broadband internet access service experience for our customers, and will provide updates here as well as other locations if a new system is implemented."[462] Comcast's explicit reservation of rights to return to throttling traffic of "heavy" internet users, as Comcast may define that, underscores the need for responsible entities and energy regulators to take action to ensure such throttling does not compromise the communication or function of energy signals.

---

456. *Network Management*, VERIZON, https://www.verizon.com/about/our-company/network-management#does-verizon-block-throttle-or-modify-any-specific-protocols [https://perma.cc/S3W9-TNR7].

457. *See* FCC, *2015 Open Internet Order*, *supra* note 5, ¶¶ 215–16 (providing network management must be "primarily motivated by a technical network management justification rather than other business justifications.").

458. FCC, *In the Matter of Restoring Internet Freedom*, *supra* note 4, ¶ 220.

459. *Learn About Our Network Management Practices*, COMCAST, https://www.xfinity.com/support/articles/network-management-information [https://perma.cc/J4SF-5E2Z].

460. *Xfinity Internet Broadband Disclosures*, COMCAST, https://www.xfinity.com/policies/Internet-broadband-disclosures [https://perma.cc/E68R-37TX].

461. Liam Tung, *Comcast: We've Stopped Throttling Speeds for Heavy Internet Users, For Now*, ZDNET (June 14, 2018), https://www.zdnet.com/article/comcast-weve-stopped-throttling-speeds-for-heavy-internet-users-for-now/ [https://perma.cc/V3PH-EQTS].

462. *Id.*

Similarly to Comcast, Charter claims it does not block or throttle lawful content but makes no promises regarding not engaging in paid prioritization.[463] AT&T also claims it does not block or throttle lawful content, nor engage in affiliated or paid prioritization. AT&T states that prioritization may occur in a reasonable network management situation and it will prioritize communications related to emergencies, national security, public safety, and law enforcement. However, AT&T also claims that they may have differing rates, deals, and speeds individually negotiated at points of interconnection.[464]

T-Mobile stated it will engage in content-agnostic throttling in furtherance of reasonable network management. T-Mobile offers prioritization plans based on the customer, who may purchase a prioritized data plan to receive priority during high-traffic and engage in zero-rating programs music and video platforms. Content providers are not charged to be zero-rated, but they must meet certain criteria.[465]

Verizon, Comcast, AT&T, and Charter all phrased their network management practices in terms of what it "does not" do, indicating that is a current practice which may change. Comcast is the only one of these ISPs that states it does not engage in paid priority. As with Comcast's reservation of rights to return to throttling customers who use large amounts of data, its paid priority policy may change. These ISP policy statements are insufficient to assure the distributed energy ecosystem that the ISP will not slow, degrade, or interfere with traffic essential to energy reliability and renewable energy resources.

The 2018 *Internet Freedom Order* cited ISP promises to refrain from "blocking or throttling lawful Internet conduct" and "existing consumer protection and antitrust laws" as sufficient to protect consumers from gatekeeper abuse.[466] The FCC noted, "that if an ISP 'failed to disclose blocking, throttling, or other practices that would matter to a reasonable consumer, the FTC's deception authority would apply.'"[467] The FTC has discretion to bring cases or not. If an ISP's promises do not create a mismatch to its practices, the

---

463. *Network Management Practices*, CHARTER, https://www.spectrum.com/policies/network-management-practices.html [https://perma.cc/E9FC-EKJV].

464. *Network Practices*, AT&T (2019), http://about.att.com/sites/broadband/network [https://perma.cc/YZ6B-PL4Q].

465. *T-Mobile Terms & Conditions*, T-MOBILE, https://www.t-mobile.com/templates/popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions [https://perma.cc/P77H-ETXP]; *Policies Open Internet*, T-MOBILE, https://www.t-mobile.com/responsibility/consumer-info/policies/internet-service [https://perma.cc/V4TS-XQ4S]; T-MOBILE, CONTENT PROVIDER TECHNICAL REQUIREMENTS FOR BINGE ON, https://www.t-mobile.com/content/dam/tmo/en-g/pdf/BingeOn-Video-Technical-Criteria-March-2016.pdf [https://perma.cc/NZZ7-WQL9].

466. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 63.

467. FCC, *Internet Freedom Order*, *supra* note 4, ¶ 141 (footnotes omitted).

case may not fall with the FTC Act's deceptive conduct proscriptions.[468] The *Internet Freedom Order* also fails to discuss the legal principle that antitrust and unfair competition law remedy only *injuries to competition*, a limitation highlighted in my August 2017 Reply Comments to the FCC.[469]

X. RECOMMENDATIONS AND CONCLUSION

A. Simulation of ISP-Induced Delay or Signal Degradation and Failure to Execute

To test the consequences of communications delays or failures due to ISP throttling, paid priority, or other traffic management manipulation, this Article suggests that RTOs, ISOs, states, FERC, and state PUC jurisdictional energy sector participants run grid simulations with national laboratories or university labs such as WSU's Smart City Testbed. As part of the California Energy Systems for the 21st Century (CES-21) initiative directed by the CPUC, a model of the California grid substation was created at the Idaho National Laboratory (INL).[470] This model allows, "real-world trials of advanced software intended to find dangerous hidden malware and trigger immediate countermeasures at computer speeds."[471] Simulations at the INL or other labs would create information and insights into ISP-induced risks for grid reliability and renewable integration. Such simulations should be promptly initiated under existing grid reliability and cybersecurity programs.

Simulations should test whether ISP-induced internet communication delays or failures trip off energy facilities, cause voltage fluctuations or other issues, local or cascading outages. Simulations should also test the length of delays that trigger grid or facility anomalies. Tests should examine whether concentration of internet communication delays compromises grid function.

---

468. Catherine J.K. Sandoval, *Disclosure, Deception, and Deep-Packet Inspection: The Role of the Federal Trade Commission Act's Deceptive Conduct Prohibitions in the Net Neutrality Debate*, 78 FORDHAM L. REV. 641, 645 (2009).

469. Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 63 (citing Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 34 (citing Atl. Richfield Co. v. USA Petroleum Co., 495 U.S. 328, 334 (1990); Brunswick Corp. v. Pueblo Bowl–O–Mat, Inc., 429 U.S. 477, 489 (1977) (holding an antitrust plaintiff must prove injury which reflects the anticompetitive effect either of the alleged violation or of anticompetitive acts made possible by the alleged violation of antitrust laws).

470. Peter Behr, *Cyberdefenses Put to Test at Computer Speed*, E&E NEWS (Oct. 18, 2017), https://www.eenews.net/stories/1060063877 [https://perma.cc/7P7H-D866].

471. *Id.*

Moreover, CAISO should work with national labs to simulate the effect of ISP-induced signal delays on grid communication using the Dispersive Technologies SDN, and other protocols used to communication with CAISO. Simulations should evaluate the effect of ISP network management delays on demand response and other actions that depend on prompt communication. The CAISO market depends on bids sent via the internet. Simulations should model ISP-induced delays on bids for the CAISO market, costs, dispatch, and achievement of environmental goals.

B. State and FERC/NERC Data Requests and Cybersecurity Reliability Rules for Energy Entities Under Their Jurisdiction

State PUCs should initiate proceedings to examine reliability, safety, rate, environmental, and cybersecurity vulnerabilities created by ISP contracts, statements, conduct, and the FCC's *Internet Freedom Order*. State PUCs should also use record inspection authority to require entities under their jurisdiction to disclose ISP offers or requests for payment for priority or QoS guarantees for mass market internet access and make such information public. State PUCs have the legal right to obtain and review utility records and can bring to light such offers to entities under their jurisdiction in order to protect safety, reliability, the public and the environment.[472]

State energy sector regulators should initiate proceedings to examine cybersecurity requirements for distribution-level energy resources. These proceedings should consider whether to require energy utilities and entities under their jurisdiction to limit contracts to ISPs that observe net neutrality in order to promote grid reliability in the distributed energy ecosystem.

On the federal level, FERC should evaluate net neutrality repeal as a reliability and cybersecurity issue in its Grid Resilience Docket No. AD18-7-000. FERC-jurisdictional responsible entities must analyze and address ISP network management contracts and conduct and the FCC's net neutrality repeal as a cybersecurity vulnerability. ISOs and RTOs should engage in the same analysis, focusing on the integration of energy resources, visibility, and management of the energy load that relies on mass-market internet access. These steps are necessary to protect energy reliability, cybersecurity, and public safety.

---

472. *See e.g.*, CAL. PUB. UTIL. CODE § 701 (2019) ("The commission may supervise and regulate every public utility in the State and may do all things, whether specifically designated in this part or in addition thereto, which are necessary and convenient in the exercise of such power and jurisdiction."); *id.* § 313 (2019) (authorizing CPUC to require data and records from an entity under its jurisdiction); *id*. § 314 (2019) (providing CPUC with inspection rights for entities under its jurisdiction).

C. Conclusion

The FPA imposes mandatory reliability and cybersecurity duties on the energy sector. State law imposes duties for entities under public utility jurisdiction to provide safe, reliable, service at just and reasonable rates, and many states require the energy sector to comply with environmental mandates to combat climate change. These legal duties do not permit the energy sector to rely on market incentives or public opprobrium in response to reports of ISP throttling, to address the consequences of net neutrality repeal on energy reliability and cybersecurity.

The repeal of net neutrality protections poses a zero-day cybersecurity vulnerability for critical infrastructure including the energy sector, as well as other internet users. The lack of restrictions on who can buy paid priority, and absence of safeguards for other internet users from traffic degradation, underscore paid priority's risks. Energy sector participants and regulators must consider the specter that foreign adversaries will accelerate their messages and degrade other internet transmissions through paid priority. The energy sector must address this supply-chain vulnerability under FERC and NERC rules, and state laws that require safe and reliable services.

The prevailing cybersecurity "hacker paradigm" has obscured the risks ISPs pose to cybersecurity. ISPs need not hack into a network because ISPs control traffic as it transits their network. Users cannot erect a firewall against their own ISP or address ISP network management practices through security patches. ISPs thus have "gatekeeper" power to control traffic crossing its network. This role underscores the importance of governance structures, including enforceable legal rules to cabin internet user vulnerabilities to ISP conduct and contracts.

The contract model has provided limited protection, particularly for non-commercial users of mass-market internet access services who lack power to negotiate ISP contract terms. Limited choice between ISPs constrains the ability of consumers to circumvent this issue by shopping. The model run by Guo et al. shows that if allowed to charge for paid priority, ISPs facing duopoly competition can use their gatekeeper position to obtain revenue from content providers to avoid data queuing delays due to ISP network management practices.[473] Even if new ISP networks were built or offered through leased facilities, time delays to switch (assuming the new network observed net neutrality) do not resolve daily, immediate

473. Guo et al., *supra* note 256, at 2.

communications needs for energy resources required within two seconds, for a four second roundtrip for CAISO market participants.[474]

The FCC and DOJ argued to the D.C. Circuit in support of the FCC's *Internet Freedom Order* that, "the issues State Petitioners raise about government services are issues that apply to all edge providers, public and private."[475] These statements fail to recognize the duties imposed on the FERC-jurisdictional energy sector to provide reliable service at just and reasonable rates. Nor did respondents recognize state law duties for utilities to provide safe reliable service, at just and reasonable rates, and comply with environmental goals for the energy sector.

The FCC's and DOJ's arguments—that "[b]ecause Petitioners did not raise any issues in this proceeding that were distinct to public safety, there was no need for the *Order* to separately discuss public safety"—distort the record before the FCC in the *Internet Freedom* proceeding. The CPUC's comments, Santa Clara County's *ex parte* letter, the alarm industry, my comments, and over 400 comments submitted to FERC raised public safety issues triggered by net neutrality repeal.

Respondents' brief to the D.C. Circuit effectively condones ISP delay of public safety internet traffic, including energy sector signals. Respondents relied on public scorn, *post facto* antitrust and consumer protection laws, and market forces to protect against ISP interference with internet traffic. This view is inconsistent with public safety and critical infrastructure laws and legal duties. Neither the FCC nor DOJ address the absence of any remedy under antitrust, unfair competition, or consumer protection laws for non-competition harms such as harms to public safety, national security, energy reliability, just and reasonable rates, and achievement of environmental solutions that combat climate change.[476]

These arguments reveal the "cat video paradigm" through which the federal government assumes all internet traffic is not important and can tolerate delays or degradation, even to the point where it does not function. The FCC's failure to consider public safety and critical infrastructure issues addressed by the *2015 Open Internet Order* and the *Internet Freedom* record indicate the *Internet Freedom Order* is arbitrary and capricious under the APA, and should therefore be vacated and remanded to the FCC for reconsideration.

---

474. N. AM. ELEC. RELIABILITY CORP., BALANCING AND FREQUENCY CONTROL, *supra* note 304, at 13.

475. *Respondents' Brief*, *supra* note 261, at 95.

476. *See* Sandoval, *Internet Freedom Reply Comments*, *supra* note 37, at 33 ("ISP self-regulation, antitrust, and unfair competition laws are insufficient to address these threats and offer no remedy for harms to democracy or national security."); Sandoval, *Net Neutrality Powers Energy and Forestalls Climate Change*, *supra* note 6, at 63 ("The *Internet Freedom* Order fails to discuss the legal principle that antitrust and unfair competition law remedy only *injuries to competition . . . .*").

The energy sector, FERC, NERC, and state PUCs should participate in an appeal of the FCC's *Internet Freedom* Order. If the Order is remanded to the FCC, then the aforementioned entities should file comments informing the FCC about the energy sector's use of the internet, as well as reliability and cybersecurity needs and implications of net neutrality repeal for those duties.

State regulators should initiate proceedings to examine the need for distribution level cybersecurity standards. These state-level proceedings should analyze the impact of net neutrality repeal on energy sector reliability, cybersecurity, safety, just and reasonable rates, and the accomplishment of environmental goals.

State and federal regulators, ISOs, RTOs, and the energy sector should partner with national and university laboratories to simulate the effect of internet delays and degraded communications on the electric grid and on renewable integration. Tests on grid models as suggested by this Article can simulate ISP network management on grid assets and function, providing information to protect grid reliability and promote alignment of ISP and energy sector governance.

The distributed energy ecosystem requires an open and neutral internet to support reliability and environmental sustainability. State and federal energy sector reliability duties therefore require prompt action to avoid the zero-day cybersecurity vulnerability triggered by the FCC's net neutrality repeal from cascading into energy reliability issues that compromise safety, just and reasonable rates, and achievement of climate change solutions.