UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Security Investments for Energy Infrastructure Technical Conference	Docket No. AD19-12-000

POST- TECHNICAL CONFERENCE COMMENTS OF THE ELECTRICITY CONSUMERS RESOURCE COUNCIL (ELCON)

The Electricity Consumers Resource Council (ELCON) appreciates the opportunity to submit these post-technical conference comments pursuant to the Commission's April 25, 2019 notice in the above-captioned docket. The conference addressed current cyber and physical security practices used to protect energy infrastructure and was intended to explore how federal and state authorities can provide incentives and cost recovery for security investments in energy infrastructure, particularly for the electric and natural gas sectors. The specific topics addressed at the technical conference included: (1) the types of cyber and physical security threats to energy infrastructure, particularly electric transmission, generation, and natural gas pipelines; (2) strategies and best practices for mitigating cyber and physical security threats; (3) how the costs of such investments are or could be recovered; and (4) whether additional financial incentives for making such investments are needed, and if so, how those incentives should be designed.

ELCON is the national association representing large industrial consumers of electricity. ELCON member companies produce a wide range of products from virtually every segment of the manufacturing community. ELCON members operate hundreds of major facilities and are consumers of electricity in the footprints of all organized markets and other regions throughout

the United States. Reliable electricity supply at just and reasonable rates is essential to our members' operations. Accordingly, ELCON has a strong interest in investment in measures to prevent and mitigate security threats provided that the corresponding costs are prudently incurred and represent a proper balancing of costs and benefits. In these comments, ELCON responds to a selection of the questions posed at the technical conference that are more pertinent to the interests of industrial consumers.

INTRODUCTION

The March 28, 2019 technical conference examined whether additional incentives and cost recovery assurances for security investments in energy infrastructure, including generation, transmission, and natural gas pipelines. Some of the conference participants emphasized the need for security investments that *go beyond* those measures already required by mandatory reliability standards, including in infrastructure not subject to those standards.

ELCON's members are industrial consumers that place a particularly high value on electric reliability. We appreciate FERC and DOE's diligence in evaluating the risks to Bulk Electric System (BES) security. Industrial consumers also place a high value on procurement flexibility and are very sensitive to cost impacts. As such, industrial consumers seek to ensure that grid security policy has demonstrated reliability benefits that justify any added costs, rely on incentives instead of standards where appropriate, and preserve procurement flexibility throughout the supply chain.

Industrial consumers recognize the value of ensuring that electricity suppliers have sufficient opportunity to recover prudently-incurred costs – those that represent a proper balancing of costs and benefits -- through just and reasonable rates. Competitive suppliers and consumers internalize threats to service disruption. This incentive alignment with BES security

encourages cost-effective security investments, provided they have adequate information. A worthwhile role for government is to enhance voluntary, risk-informed decisions to improve market outcomes.

Cost-of-service segments face a moral hazard quandary with BES security, which warrants different regulatory oversight than those exposed to market forces. No prudency gauge exists in the absence of a Commission-developed economic framework for grid resilience and security, leaving industrial consumers exposed to billions in annual cost risk without any verification of benefits.

I. CYBER AND PHYSICAL SECURITY, BEST PRACTICES, AND INDUSTRY AND GOVERNMENT ENGAGEMENT

A. Threats to Energy Infrastructure

1. What cyber and physical security threats are most concerning for the energy industry? What critical factors should industry consider when evaluating the risk these threats present and prioritizing risk-mitigating security initiatives to address these threats?

The greatest threats to widespread and sustained outages related to both cyber and physical security are embedded in the transmission and distribution segments.[1] Very few common physical mode failures exist for power generation. Physical risks are very context-specific, suggesting region-specific analysis should comport with a general rather than prescriptive risk framework. For example, the loss of a pipeline is manageable for grid operators in most areas and trending favorably given growing pipeline reticulation. However, a pipeline contingency in ISO-NE may cause the inability to serve 10-15% of load during a cold

[1] For example, see Mukherjee, *et al.*, " A multi-hazard approach to assess severe weather-induced major power outage risks in the U.S.," Elsevier Vol. 175 (July 208) at pp. 283-305 (available at https://www.sciencedirect.com/science/article/pii/S0951832017307767).

winter period.[2] As such, physical security threats may warrant altering the definition of credible contingencies for generation and transmission in a specific, rather than general, context.

Cybersecurity threats present a legitimate network risk for generation. Participants at the technical conference and in a variety of other industry forums flagged social manipulation (*e.g.*, spearfishing for login credentials) as the largest cyber threat. The remedy is robust cyber hygiene, not expensive system upgrades.

Prioritizing risk-mitigation initiatives should account for quantified benefits and costs or, at least, use a cost-efficiency ranking. This exercise may reveal that some lower risks are worth greater priority than some high risks given the expense of mitigation options. It will also reveal that mitigating some risks is not prudent. Costly mitigation that exceeds risk reduction benefits is imprudent and harms consumers.

2. Does industry have adequate resources to evaluate sophisticated threats such as whether adversaries have established access to their networks, whether insider threats exist, or whether supply chain equipment or subcomponents are compromised?

The private sector has extensive experience with addressing supply chain deficiencies, but the defense and intelligence communities may have access to vital information first. Expediting the transfer of the evolving nature of these threats to the private sector would enhance risk-informed decisions. For example, this may improve the quality or responsiveness of third-party validation programs and commercial standards developments.

3. How are interdependencies among energy infrastructure sectors considered in risk management analyses?

---

[2] Resilience and Emerging Issues in Wholesale Electricity Markets, June 2018, at p. 7 (available at https://www.eia.gov/conference/2018/pdf/presentations/david_patton.pdf).

The electricity and natural gas industries have made tremendous progress coordinating operating and planning activities since the Commission prioritized this area earlier this decade. Interdependencies between telecommunications and energy industries is of growing importance as well. Encouraging interagency and private sector coordination is warranted.

4. What are some of the challenges (e.g. staffing or technology), that industry faces, in order to keep current with the threats?

Participants at the technical conference emphasized the need for better information sharing on threats and adversaries' tactics to ensure they can protect their own assets better. One idea mentioned was to get more security clearances in the private sector so intelligence agencies can share classified information, as waiting for information to become declassified may result in more exposed assets.

Under the purview of the Department of Homeland Security, the timeline for security clearance approval can take years and the number granted is often limited by individual company. These constraints make the receipt of possible helpful information restricted to those who have the necessary clearances. This could impact the stakeholder involvement needed to make information sharing and receipt successful.

5. What other current or emerging threats should be addressed? For example, what are some of the types of physical and cyber security threats that Unmanned Aircraft Systems (i.e., drones) can present? What experience has industry had with commercially-available products used to address these issues?

The amount of commercially-available products to manage physical and cyber risk continues to grow considerably. Financial and physical services are available to help address threat mitigation and response. The evolving insurance market indicates progress in industry

risk management pertaining to cyber and physical threats. For example, corporate insurance contracts for cybersecurity liability have evolved rapidly in the last few years.

B. Mitigation Strategies and Best Practices

6. What are some of the best practices that industry uses to ensure effective action against cyber and physical security threats? Are adequate tools available for industry to assess where to apply best practices (e.g., risk management analyses) for cyber and physical security threats? Do these analyses differ between cyber and physical security threats?

Best practices are very dynamic in a rapidly evolving cyber and physical security threat space. This places a premium on rapid information transfer and procurement flexibility. Prescriptive mandatory reliability standards, by nature, are poorly suited for such dynamic problems and in some cases inhibit innovation and adoption of best practices. Generally, best practices are identified and adopted via ongoing exercises customized to specific contexts, rather than generic practices based on a stale snapshot in time.

For example, manufacturers conduct routine internal phishing and other electronic weakness exercises throughout the year to maintain a high level of mindfulness of possible threats. Such ongoing exercises rapidly identify threats and promptly update protective practices over days and weeks. In contrast, standards development processes take years to identify and implement generic practices that are outdated and often less effective than tailored solutions. Voluntary actions drive innovation in best practices, whereas mandatory standards often restrict necessary innovation. As such, best practices are better achieved through permission-less innovation rather than permission-based approval.

The rapid rate of change in computing technology is outpacing the ability of standards development processes. The Critical Infrastructure Protection (CIP) standards are causing mounting costs with six major initiatives forthcoming. Existing CIP standards already constitute the largest category of NERC reliability standards violations, as evidenced by recent quarterly reports of the Compliance Monitoring and Enforcement Program. This regulatory framework is unlikely to prove scalable at an acceptable cost and may prove counterproductive in mitigating some risks.

A cautionary tale of CIP standards inhibiting best practices comes from the application of CIP Version 5 to virtualization. In the mid-2010s, vendors like Cisco and VMware launched next-generation virtualization hardware and software products to protect against sophisticated cyber attacks, including those sponsored by rogue governments. Many entities elected to forego these practices because of compliance uncertainty with CIP standards. NERC has since launched an investigation into virtualization with standards activity starting soon. The result is that the electricity industry lost at least four years on virtualization and has lagged adoption of better practices with lower capital cost compared to other industries, including banking and finance, that have comparable cybersecurity needs.

Similar mistakes may be repeated in emerging areas like supply chain risk, where rigid mandatory reliability standards that encroach on commercial space could undermine best practices. For example, NERC has identified that extending Supply Chain Standards to low impact BES cyber systems may have the unintended effect of increasing the risk of common-mode vulnerabilities by reducing the diversity of vendors.[3] Instead of introducing accidental harm, policy that motivates private sector innovation will drive development and adoption of

[3] NERC, Supply Chain Risks and Recommended Actions (Draft), March 2019, at pp. 19-20 (available at https://rtoinsider.com/wp-content/uploads/Supply-Chain-Report-May-2019.pdf).

best practices throughout the supply chain. For example, growing demand for layers of cybersecurity protection, including down to individual components, is organically driving supply chain innovation as equipment vendors are developing more cost-effective cyber protection features built into their products (e.g., malware detection and elimination and multi-factor component identification). Competitive forces stimulate the creation and adoption of such best practices, but only if cybersecurity policy permits procurement flexibility.

Less prescriptive and more process-based approaches to CIP standards can preserve procurement flexibility but still need to address excessive reporting burdens. For example, CIP standards focusing on process have permitted patch management advances to proliferate swiftly, but tedious and extensive documentation processes should be streamlined to lower the compliance burden. Errors in patch upgrades are inevitable in a vast system, and "zero tolerance" audits do not distinguish between the gradients of performance levels and can impose hefty mitigation plans that exceed the severity of a violation. Risk-based performance benchmarks are a more suitable direction to "right-size" reporting requirements and mitigation plans.

NERC's shift from "zero tolerance" to a risk-based compliance monitoring and enforcement program supports better practices. This has reduced burdens on industry by "right-sizing" efforts according to facility risk factors. The shift also encourages self-reporting of noncompliance, which helps with identification and adoption of best practices. However, this transformation is not complete and opportunities for improvement are considerable.

Beyond standards, tools that enhance threat detection and information sharing have made considerable progress. The Cybersecurity Risk Information Sharing Program and Electricity Information Sharing and Analysis Center are voluntary platforms that augment risk-informed decisions.

7. How does industry validate the effectiveness of, and maintain its mitigation techniques/measures (e.g., red teaming, manufacturers recommendations) for, both physical and cyber protection? What are the processes to confirm the results are addressed? Are these lessons shared with others in the industry?

Infrastructure suppliers and industrial consumers rely heavily on manufacturer recommendations. For example, a primary vendor for gas turbines sends periodic notices to clients and hosts conferences that include discussions on physical vulnerabilities and improvement opportunities.

Industrial consumers have internal supply chain groups with a formal vetting process in place for all physical and cyber vendors to ensure system configuration conformity and integrity. Internal controls exist to ensure compliance with company policy. For example, corporate departments are only permitted to use pre-approved vendors that have already cleared the internal rigorous screening process.

Various forums exist to share lessons learned. One constraint is that corporate cyber and physical threat mitigation practices are commercially sensitive and integrated into customized internal processes that make standardized reporting challenging. Thus, information collection methods must be secure, not overly burdensome, and recognize constraints on the external validity of results as best practices may very on a company-to-company basis. Periodic, voluntary surveys and data requests can be effective for collecting information on current industry practices but should be used for informative purposes to drive better voluntary risk-informed decisions, not development of prescriptive mandatory standards that will become quickly outdated.

8. What resources are available to assist industry in evaluating risk to energy infrastructure and implementing mitigation measures, especially for small to medium size owners and operators?

Information-sharing institutions serve as very helpful resources to guide private sector decisions. Some industrial consumers are members of the E-ISAC, which issues routine reports and bulletins. Some industrials also subscribe to receive alerts from ICS-CERT which is through the Cybersecurity and Infrastructure Security Agency (CISA) sponsored by DHS. This organization is now known as the National Cybersecurity and Communications Integration Center (NCCIC). However, the usefulness of these resources is only as good as the quality and rate that information is shared. Reducing participation barriers in these types of institutions would encourage more risk-informed decisions in the private sector.

Industrial consumers also participate in ISO/RTO working groups tasked with cyber and physical security. The groups are more regionally focused but provide information from a federal perspective that helps aid in sharing of lessons learned, including common mode vulnerabilities across both intra- and inter-regional scales.

Ensuring industry forums provide ongoing information will assist in the availability of current resources to address emerging risks. These provide important informal forums for discussion as well as formal resources including white papers, such as those produced by the Electric Power Research Institute, North American Generator Forum, and the North American Transmission Forum.

9. What training opportunities are available to owners and operators to understand the various risks to their energy infrastructure and the measures taken to mitigate against physical and cyber threats? What training is necessary and not available?

Manufacturers typically require their employees to attend regular trainings on cyber security threats and internal protection measures. Additional training on physical attack scenarios based on defense and intelligence information would improve the understanding of these risks by the private sector.

10. How does industry mitigate key vulnerabilities to address disruptions from a cyber or physical attack or an extreme natural event (e.g. geomagnetic disturbance)? How should spare equipment, sharing programs, contractor and mutual assistance programs, and other processes be considered in addressing disruptions? What role should the federal government play in helping industry prevent and respond to disruptions? What preparations should be made by industry to assure adequate response and recovery effort?

The primary role of government should be to ensure voluntary private sector decisions are risk-informed, consistent with ELCON's prior responses in these comments. Unusual natural events have regularly been incorporated in planning processes and internalized by market participants. For example, hurricanes and extreme cold weather are accounted for in transmission planning and in power plant operators weatherizing their facilities.

The cost of response and recovery efforts – including spare equipment and assistance programs – should be quantified and compared to the benefits. Quantifying the benefits may require additional research on the value of lost load (VOLL) for extended outages. Consumers value the pace of service restoration very differently. For example, the damage to many manufacturing processes from an outage requires a considerable period of repair time during which the manufacturer places little to no value on service restoration. Other end-uses of electricity are often not sensitive to brief service curtailments but highly value rapid recovery (*e.g.*, refrigeration services). This suggests the policy response should explore voluntary service restoration pricing where practicable or, at the least, allocate costs for service restoration to those that value the additional expense.

II. INCENTIVES AND COST RECOVERY FOR SECURITY INVESTMENTS

A. Cost Recovery

2. *Are current cost recovery policies of the federal and state governments affecting the ability of owners and operators of energy infrastructure to invest in cyber and physical security for this energy infrastructure? Do federal and state policies complement or conflict with each other? Are these policies helping or hindering security investments?*

As noted during the technical conference, PUCs often allow cost recovery required by CIP standards. Thus, flaws in CIP standards carry over into retail rate recovery proceedings. This is likely to result in approval of outdated practices that are imprudent costs for consumer to incur, while foregoing prudent practices needed to address a rapidly evolving threat landscape. For example, some entities are avoiding use of cloud-based services because CIP standards deter deployment of some reliable new services.

3. *Do cost recovery policies at the state and federal level facilitate the adoption of best practices for threat mitigation at energy infrastructures? Do they allow for cost recovery for investment to address mitigation of new and emerging threats (e.g., intentional electromagnetic interference and electromagnetic pulse)?*

Industrial consumers recognize the value of ensuring suppliers have sufficient *opportunity* to recover prudent costs. Sometimes the best practice is to forego an expensive practice and leave the risk unhedged. This occurs in every risk management sphere, although this framing rarely exists in the security domain due to the misconception that there is no cost-security tradeoff worth considering. American manufacturing cannot survive endless cost increases intended to mitigate every possible scenario.

Cost recovery for security investments is especially vulnerable to hyperbolized scenarios and red herrings. The emphasize on mitigating risk from a high-altitude electromagnetic pulse (EMP) is a case-in-point. The likelihood of an adversary detonating a nuclear device at high altitude in lieu of inflicting far greater damage with ground detonation has caused some

security experts to largely dismiss the concern. Meanwhile, NERC is forming an EMP task force and eyeing standards likely much more costly than those for geomagnetic disturbances. This demonstrates the severe need for better defense and intelligence information that is reliable and verifiable, otherwise consumers' confidence will erode in the institutions and grid security initiatives addressing valid and invalid pursuits alike.

5. For competitive generators that do not recover their costs through retail rates, are there mechanisms under which they may recover costs for physical or cybersecurity investments other than through their market-based rates?

Security investments are a subset of all investments needed to operate power plants reliably. Competitive generators already have incentive to adopt cost-effective security practices via the opportunity cost of foregone market revenues. If generators lack threat information to make efficient investment decisions it is not an issue for cost recovery.

A key premise of adopting competitive generation is for all costs necessary to operate a power plant reliably to be internalized by its owner, rather than socialized on captive customers. Shifting a segment of competitive generators' costs to cost-of-service would set a deeply problematic precedent. Specifically, carving-out security investment would undercut incentives for innovation and cost control in security investment practices and encourage suppliers to seek ever-expanding definitions of security investments in order to shift the risk burden onto consumers. This would raise costs and undermine grid security in the long-term.

This concern is already evident, as shown in an ISO-NE proposal to shift the recovery of *generator* CIP costs from market-based rates to *transmission* cost-based rates.[4] The costs of compliance with new regulations – CIP or otherwise – is an investment risk that should be

[4] Interconnection Reliability Operating Limit Critical Infrastructure Protection Cost Recovery, May 2019 (available at https://rtoinsider.com/wp-content/uploads/a06_tc_2019_05_16_iso_presentation.pdf).

internalized by competitive generators, not socialized through a new charge on transmission customers.[5] ISO-NE claims that these costs cannot be competitively offered and recovered through energy and capacity markets. This would only be true if market power mitigation measures failed to recognize these expenses as legitimate going-forward costs. If that is the case, then the problem should be addressed in those mechanisms to permit an *opportunity* to recover such legitimate costs. Creating a new mechanism to socialize security costs on consumers in this case will set precedent for other in-kind misguided requests. It will also worsen cyber risk management by introducing the moral hazard of cost-of-service regulation and, with it, deter cybersecurity innovation by removing the incentive of generators to seek more cost-effective internal processes and vendors.

7. What factors should the states be aware of when reviewing cost recovery filings for cyber and physical security investments? Can these factors be included on an industry-wide or multi-state level?

In the technical conference, PUCs expressed concern over how to discern what utility proposals are prudent for physical and cybersecurity protection. For example, PUCs often approve protections consistent with CIP standards, even though these take years for NERC and stakeholders to develop. PUCs may seek better information on the nature of quickly evolving risks than what stale standards development processes provide, which does not require classified details. It may be better suited to a forum for industry best practices. PUCs, as with the Commission, need a better barometer for prudency.

8. Certain events could require significant unbudgeted resources to respond effectively. How should these costs be considered by federal and state authorities for cost recovery?

[5] Cost Allocation for IROL Critical Generator CIP Costs, March 2019, at p. 3 (available at https://rtoinsider.com/wp-content/uploads/a06_tc_2019_05_16_eversource_presentation.pdf).

One option is to explore contingency rules to enable swift capital access in the event of a verified attack. Predetermined cost recovery mechanisms should allocate costs consistent with consumer classifications that cause the need for rapid service restoration.

B. Financial Incentives

9. What type of incentives would be most effective to facilitate investment in cyber and physical security? How could costs for these incentives be recovered?

Market design that accurately reflects the value of lost load (VOLL) is the basis for providing proper incentives to generators for security and other reliability investments. The current level of generation resilience and security is high. The combination of shortage pricing in energy markets and capacity performance payments approximately equals VOLL across the RTO/ISOs. An expert workshop held in 2018 on economic approaches to bulk power system resilience concluded that "resilience is generally not a basis for more administrative constraints on wholesale energy or capacity markets."[6]

The benefits of transmission are typically non-market in nature and thus captured in transmission expansion planning processes. Ensuring these processes use *credible* contingencies is worthwhile. These processes must avoid opening the door to *incredible* contingencies via the injection of unverified security anecdotes. The Commission must emphasize the use of evidence-based criteria if security parameters are to be considered more explicitly.

Generally, additional incentives, such as return on equity (ROE) adders or construction work in progress (CWIP), would not be effective to enhance security investments. Incentives

[6] Palmer, et al., "Economic Approaches to Understanding and Addressing Resilience in the Bulk Power System: A Workshop Summary, Resources for the Future, June 2018, at p. 2 (available at https://media.rff.org/documents/RFF_workshop_summary_final_0.pdf?_ga=2.44033765.15421067.1558363116-588373065.1558363116).

add costs to consumers for infrastructure that would already be built. Any perceived deficiencies in investment result from faults in procurement mechanisms, which incentives do not address. Infrastructure suppliers are already trying to seize opportunities for resilience and security incentives that provide no such incremental benefit. For example, Connecticut and Massachusetts officials approved the Pequonnock Substation Project to boost grid resilience but considered the project owner's request for a 50 basis point ROE incentive adder unnecessary.[7]

10. How could the Commission use its authority under Section 219 of the Federal Power Act to establish incentives for improved cyber and physical security? Are there other ratemaking or accounting changes that would help incent investments in cyber and physical security?

Any review by the Commission of its authority to incent improved security investments and practices should limit its focus to removing administrative barriers to adoption of best practices and ensuring market participants' incentives align with bulk system reliability. The pursuit of additional incentives, such as a transmission adder for projects deemed critical to grid resilience or security, are unnecessary and would impose unjustified costs on industrials and other consumers. Any security benefits should be remunerated through transmission planning processes and market design and not require out-of-market mechanisms or above-market rates of return.

12. What changes could federal and state authorities make to current policies to better incent the adoption of best practices for cyber and physical security at energy infrastructure facilities?

Where entities have the right incentives to manage risk themselves, the policy emphasis should be on evaluating whether they have adequate information. For example, competitive suppliers and manufacturing facilities internalize risk and thus have risk management

[7] Order on Transmission Incentives, Docket No. ER19-1359-000 (available at https://www.ferc.gov/CalendarFiles/20190514153107-ER19-1359-000.pdf).

incentives that align robustly with bulk power system security. The Commission should examine if policy or programs can enhance voluntary risk-informed decisions for these entities. Since best practices evolve rapidly, improved threat diagnostics and expedited information sharing may improve private sector performance.

For entities that do not bear the full consequences of their own risk management practices, a moral hazard problem exists. For example, some literature finds underinvestment aimed at reducing power outages under the monopoly regulation model.[8] At the same time, security is an easy justification for cost-of-service entities to expand rate base. Overall, moral hazard may necessitate a more active role for regulatory oversight of cost-of-service entities to promote prudent security practices and deter imprudent gold-plating. Exploring performance-based oversight tools in lieu of prescriptive mandatory standards may incent better performance and avoid unintended consequences, such as deterring adoption of new practices in order to comport with stale mandatory requirements.

13. How should state and federal authorities prioritize incentives for various security investments? How should such incentives balance the need for improved security with the rate impact on consumers?

This is the most pertinent question posed by the Commission, as it recognizes the cost-security trade-off facing consumers and importance of incenting only prudent security investment. Consumers incur the costs and benefits of a reliable, resilient, and secure grid, but top-down planning apparatuses have generally failed to adopt the consumer perspective. ELCON and some other consumer groups have expressed intense skepticism of certain electricity policies over the last several years promoted in the name of grid resilience and

[8] Lim and Yurukoglu, "Dynamic Natural Monopoly Regulation: Time Inconsistency, Moral Hazard, and Political Environments," August 16, 2016 (available at https://web.stanford.edu/~ayurukog/main_infrastructure.pdf).

security.[9] Some of these proposals could amount to tens of billions of dollars in cost increases with little or no benefit.[10] A core area of concern is that no barometer for prudency exists in the absence of an economic framework to evaluate costs and benefits.

The Commission should embark on developing an economic framework for non-market segments of the bulk power system. Too many practices and projects are already done outside of an economic framework – such as reliability projects not subject to competitive processes – and adding security criteria would likely compound the problem. An economic framework would enhance conventional policy and introduce a prudency instrument for evaluating and prioritizing resilience and security considerations. An economic approach should also strive to enhance risk-informed policy and private sector decisions.

Admittedly, the benefits of high impact, low probability events are difficult to estimate. However, obtaining better information to bolster threat diagnostics would inform the likelihood of an event occurring. Better estimates for extended-outage VOLL would inform the consequences of an event occurring. Altogether, better projections of likelihood and consequences combined with better cost estimates would help establish guardrails for defining efficient risk levels, rather than relying on arbitrary standards.

The basic elements of an economic framework for transmission would be readily transferrable to distribution, which would benefit state regulators. The Commission and states would benefit from jointly examining grid resilience and security through an economic lens and consumer perspective.

---

[9] Hartman and Marquis, "Consumers shouldn't pay for bureaucratic thinking on electricity," Utility Dive, March 8, 2019 (available at https://www.utilitydive.com/news/consumers-shouldnt-pay-for-bureaucratic-thinking-on-electricity/550013/).

[10] For example, see Celebi et al., The Brattle Group, "The Cost of Preventing Baseload Retirements: A Preliminary Examination of the DOE Memorandum," July 2018 (available at https://info.aee.net/hubfs/Brattle_AEE_Final_Embargoed_7.19.18.pdf).

Respectfully Submitted:

Devin Hartman
President and CEO

ELECTRICITY CONSUMERS RESOURCE COUNCIL
1101 K Street, NW, Suite 700
Washington, DC 20005
Email: dhartman@elcon.org
Phone: (202) 682-1390

W. Richard Bidstrup
CLEARY GOTTLIEB STEEN & HAMILTON LLP
2112 Pennsylvania Avenue, NW
Washington, DC 20037
Email: rbidstrup@gmail.com
Phone: (202) 974-1760
Counsel for ELCON

Dated: May 24, 2019

CERTIFICATE OF SERVICE

I hereby certify that I have this day served the foregoing document upon each person designated on the official service list compiled by the Secretary of this proceeding.

Dated at Washington, D.C.: May 24, 2019

/s/ W. RICHARD BIDSTRUP
W. Richard Bidstrup