UNITED STATES OF
AMERICA BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Reliability Technical Conference	Docket No. AD19-13-000

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 respecting the June 27, 2019 Commissioner-led technical conference to discuss policy issues related to the reliability of the Bulk-Power System.

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.

ELCON's members are industrial consumers that place a particularly high value on electric reliability. Accordingly, ELCON has a strong interest in mitigating

Bulk Electric System ("BES") reliability threats provided that the corresponding costs are prudently incurred and represent a proper balancing of costs and benefits. ELCON appreciates FERC's and NERC's diligence in evaluating the risks to BES reliability. 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 reliability 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. In these comments, ELCON responds to a selection of the questions posed to Panels I and II at the technical conference that are more pertinent to the interests of industrial consumers.

Panel I: Status of the Electric Reliability Organization and Reliability

a) What trends and risks from the State of Reliability Report does NERC consider to be the most significant challenges facing BES reliability? How should NERC prioritize these challenges to ensure reliability of the BES is maintained? How have these challenges affected NERC's and Regional Entities' resource requirements and allocations?

Ideally, NERC would prioritize issues based on the potential economic damages that result from loss of load expectations under current region-specific procurement and operating practices. This would require an approach to valuing the benefits of reliability, which admittedly will take considerable development time. In the meantime, NERC would best serve beneficiaries of BES reliability by prioritizing deeper analyses of areas where current procurement practices and operating protocols have the most room for improvement to jointly enhance BES efficiency and reliability.

The value of NERC's analyses as an informative tool increases as organizing electric infrastructure procurement and operating behavior to achieve BES reliability becomes more complex. NERC's reports should aim to inform BES participants, their regulators, and the broader electricity community in a manner that results in organic improvement in the efficiency and reliability of resource procurement and asset management activities. In this way, NERC's reports would help other entities prioritize issues that improve BES reliability that standards cannot address efficiently or altogether. ELCON applauds NERC's new emphasis on achieving impact through informational influence, rather than a "standards-only" approach.

Many NERC metrics are constrained by the inherent limitations of trend analysis, which is useful for comparative analyses in certain contexts but often fails to diagnose the underlying causal factors needed for policy decisions. This is summarized by the common financial disclosure that "past results may not be indicative of future performance." Trend analysis without context can result in false positives, such as flagging a downward trend in installed capacity in a region as problematic when no reliability concern exists because of binding capacity procurement mechanisms. Trend analysis may also provide a false sense of security, especially when it comes to identifying low frequency events where small sample sizes constrain statistical analysis. NERC's growing emphasis on "near misses" may help remedy this for certain types of issues, such as cyberattacks and brief shortages of balancing services.

Better contextualizing NERC's trend analyses would be fruitful. Specifically,

integrating trend analysis results with more region-specific field observations, such as changes in procurement mechanisms or operating protocols, leads to more insightful conclusions. For example, forced outage patterns are a function of various market design elements, entity regulatory status, and regulatory prudency determinations. Better applying empirical analysis to regional contexts would better voluntary responses from Regional Entities, state regulators, and BES entities.

Regulated utilities do not adjust procurement to indications of scarcity without support by state regulators, whereas merchants and industrial consumers alter weatherization, fuel procurement, consumption patterns, and other reliability-enhancing practices in response to price signals. As such, the accuracy of extrapolating forced outage trends hinges heavily on the regulatory climate in some states and market conditions in others. Markets do not signal merchants to incur extra costs to avoid some outages or consumers to alter consumption behavior when there are oversupply conditions. As fundamentals tighten, however, merchant generator outages decrease naturally and consumption shifts to off-peak periods. Trend analysis in markets may indicate a problem when the issue is actually self-correcting. Furthermore, the avoidance of costs to produce an unnecessarily high level of available operating reserves is a boon to consumers, but reliability metrics only display them as a problem.

NERC is correct to flag changes in the resource mix as a reliability policy priority, but this issue must be evaluated in the proper context. Evaluating implausible political scenarios, such as coal and nuclear retirements in excess of what any regional procurement processes would allow, creates misinformation.

Evaluating plausible scenarios would help inform the stakeholders involved with determining the resource mix and encourage reliability-enhancing decisions that are otherwise outside of NERC control. For example, variances in capacity accreditation methods for unconventional resources can significantly impact BES reliability, and utility and regional procurement processes would benefit from enhanced information. In this way, NERC plays an important role by monitoring and informing procurement processes without necessitating standards that restrict procurement flexibility.

Evaluation of the changing resource mix continues to rely on an overemphasis on reserve margins during peak conditions. Peak reserve margins are becoming less indicative of loss of load probability than other indicators. Recent developments in MISO, SPP, and CAISO flag challenges for obtaining balancing service flexibility, much of which occurs during shoulder seasons where there is ample nominal capacity but deficiencies in specific capabilities. For example, MISO recently identified loss-of-load risk outside of the summer for the first time, with the CEO noting that it is time to think about an "availability margin" as opposed to a reserve margin.[1] As such, BES metrics should focus more on coincident performance of resources throughout the year and across the suite of essential reliability services.

Reframing some NERC assessments to examine *opportunities* as well as *risks* to BES reliability would be a welcome development. In particular, new technologies could improve BES reliability and/or lower the economic damages of reliability

[1] A. Cook, "MISO Finds Loss-of-load Risk in Fall, Winter Months," RTO Insider (Aug. 13, 2019) (available at https://rtoinsider.com/miso-loss-of-load-risk-fall-winter-months-141110/).

events. The prospect of differentiating reliability services is very important to industrial consumers. For example, a brief service curtailment may be viewed indifferently by an arc furnace operator but cause tens of millions in damages to a refiner. An opportunity is approaching to cease treating all firm load uniformly and instead treat load consistent with consumer preferences. NERC could open the door to this by segmenting firm load in its metrics based on the value those end-uses place on reliability. Holding the number and duration of total firm load curtailments constant, but reallocating customer outages under a differentiated versus undifferentiated reliability construct could easily lower the aggregate economic damages by over an order of magnitude.

Ideally, NERC would evaluate new technologies and reliability concepts through an economic lens. As Bushnell *et al.* (2017) note, NERC "should consider the impact of new technologies on both planning and operational standards in a way that better accommodates economically efficient reductions or curtailments in load."[2] Reliability organizations, including NERC, must play an active role in order to increase the diversity in approaches to resource adequacy and reliability, as some of these activities would violate existing NERC standards.[3]

b) How should NERC address the risk of high-impact, low-frequency events such as gas pipeline contingencies and electromagnetic pulses? What additional steps, if any, should NERC be taking to address these types of threats?

NERC must approach high-impact, low-frequency ("HILF") events through a

[2] J. Bushnell, *et al*., "Capacity Markets at a Crossroads," Energy Institute at HAAS (April 2017), at p. 5 (available at https://hepg.hks.harvard.edu/files/hepg/files/wp278updated.pdf).
[3] *Id.* at p. 53.

verifiable, quantifiable lens. HILF events have been the primary category of "resilience" concerns raised in other forums. Industrial consumers have expressed major concerns at both state and federal levels about the inability to quantify the speculative benefits of mitigating HILF events. Most attempts to define and quantify these concepts have "relied upon ad hoc definitions that do not have much underlying rigor".[4] The result is a severe lack of prudency gauge to decide if the benefits of mitigating a HILF event outweigh the costs. ELCON reiterates its stance from prior comments that the Commission should develop an economic framework to evaluate HILF events, which will help NERC and other parties respond appropriately.[5]

An economic framework for HILF events would evaluate whether any unique market failures exist that require changes to market design. Common mode failures may require special attention in narrow market design improvements, such as redefining system contingencies and associated capacity accreditation.[6] These are very region-specific and do not lend themselves to uniform policy prescriptions. Pipeline contingencies fall under this purview. 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 I5O-NE may cause the inability to

[4]Pacific Northwest National Laboratory, Electric Grid Resilience and Reliability for Grid Architecture (Nov. 2017) at p. 1 (available at https://gridarchitecture.pnnl.gov/media/advanced/Electric_Grid_Resilience_and_Reliability.pdf).

[5] *See* Post-Technical Conference Comments of ELCON on Security Investments for Energy Infrastructure Comments, Docket No. AD19-12-000 (May 24, 2019).

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

serve 10-15% of load during a cold spell.[7] NERC can assist in evaluating such conditions, but HILF events are poorly suited to remedy via uniform, mandatory standards.

The continued pursuit of mandatory reliability standards to mitigate an EMP attack is a clear example of the credibility problem associated with injecting unsubstantiated security scenarios into civilian energy infrastructure policy. Depending on its use, experts have noted that EMP is "not a risk apart from nuclear strikes" and that far easier and less expensive attack options exist at the power-plant level.[8] Simply put, an adversary with the means to deploy a high altitude EMP would also possess the means to inflict far worse damage that renders EMP concerns obsolete. A logical adversary without EMP capability would pursue alternative means of reaching the same or a more severe result.

Energy and security staff at the Energy Department and Capitol Hill routinely downplay or dismiss EMP concerns in private, yet the public call to address the issue remains. Whether EMP or otherwise, industrial consumers cannot afford to mitigate every possible attack scenario, and the Commission should only define HILF attack scenarios that are highly credible within the defense and intelligence communities, such as various cyberattack scenarios. Standards development with respect to extremely low probability events, such as EMP, must be especially cost-conscious.

---

[7] D Patton Presentation to 2018 Energy Conference of the U.S. Energy Information Administration, 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).

[8] M. Pearl, We Asked a Military Expert How Scared We Should Be of an EMP Attack (May 2015) (available at https://www.vice.com/en_ca/article/kwxq4v/we-asked-a-military-expert-how-scared-the-us-should-be-of-an-emp-attack-508).

e) What new steps is the Electricity Information Sharing and Analysis Center (EISAC) taking to further assist the industry to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents? Are there additional actions the Commission could take to further encourage participation in E-ISAC's information sharing activities?

Information-sharing institutions serve as very helpful resources to guide private sector decisions. Reducing participation barriers in these types of institutions would encourage more risk-informed decisions in the private sector. NERC leadership has indicated a stronger emphasis on improving voluntary information sharing under E-ISAC, which is a very welcome direction for security policy from the perspective of industrial consumers.

Some industrial consumers are members of the E-ISAC, which issues routine reports and bulletins. Some industrial consumers also subscribe to receive alerts from ICS-CERT which is through the Cybersecurity and Infrastructure Security Agency ("CISA") sponsored by DHS. However, the usefulness of these resources is only as good as the quality and timeliness of the information that is provided.

Improving the quality and rate of E-ISAC information and lowering the costs of E-ISAC participation would encourage companies to join E-ISAC. E-ISAC is still fine-tuning operations trade-offs, such as how to balance expediency with quality in alerts. E-ISAC continues to add staff and refine strategic direction and implementation, which are opportunities to improve services that entice industry participation. E-ISAC efforts are improving collaboration within and between industries through both routinized practices and periodic exercises, such as GridEx V. E-ISAC data is limited now, but should improve as implementation progresses.

E-ISAC's strategic goals of engagement, information sharing, and analysis are

on-point and can greatly help industrial consumers and other entities manage their cybersecurity risks. E-ISAC is initiating outreach to prospective members and Commission inquiry on the feedback received would be welcome to reveal how greater participation could be achieved. ELCON has offered its assistance to NERC and E-ISAC on engagement with large consumers and is discussing next steps with E-ISAC leadership. Commission encouragement to improve E-ISAC data and metrics refinement, across all strategic goals, would be beneficial.

f) In what ways can the Commission, NERC, and the Regional Entities work together to identify and address evolving threats to maintain and improve reliability and security of the BES? When should the Commission and/or NERC conclude that a new or modified standard is necessary to address an identified threat?

Greater scrutiny of the proper role of standards is critical as the ERO Enterprise evolves. As a matter of policy instrument choice, mandatory standards are more appropriate for issues where best practices are obvious and relatively static and uniform behavior change is desirable. Where these conditions are met, standards can improve information access, lower transactions costs, and enhance reliability at reasonable cost. In other contexts, standards can impose major costs with little reliability benefit and infringe on industry procurement flexibility.

Sometimes mandatory standards are not needed or are even counterproductive to improving BES reliability. This is clearly the case for dynamic best practices, such as cybersecurity protections, where critical infrastructure protection (CIP) standards have deterred adoption of best practices. Standards are also inefficient or counterproductive when applied to entities with motives aligned with BES reliability. For example, NERC compliance concerns deter forms of

reliability-enhancing self-supply in the industrial community, including cogeneration, microgrids, and energy storage development.

A favorable cost-benefit analysis should be at least one precondition to the development of any new standard above a major cost threshold. For uniform unit-specific standards, the net benefits of uniform behavior change would need to outweigh alternative options. Alternative actions are often outside of NERC's control, such as changes to market design and state procurement processes. This means NERC should first thoroughly understand how these processes function before pursuing standards development. Furthermore, these processes could be improved with NERC serving an informational and collaborative role in lieu of standards.

A clear application of this is fuel security and cold weather preparation. Whether the reliability benefits outweigh the extra costs to firm fuel supplies or weatherize equipment is region and often sub-region specific. For example, a system requiring 100 GW of winter resources and 150 GW of nominal capacity does not need tens of GWs of capacity to incur extra costs in order to meet system reliability needs. In this case, uniform performance across the fleet would be inefficient and a poor fit for standards.

A more tangible action is the July 2019 joint FERC/NERC report on the January 2018 Southern cold weather event that recommended the development of weatherization standards without calculating the cost or the effect on loss of load

probability.[9] As such, consumers do not know if the recommendation will leave them better or worse off. Physical procurement standards would intrude upon merchants' market-driven responses to cold weather preparation and encroach upon state prudency reviews of weatherization costs. However, cost-benefit and other information could enhance market participant and state regulatory decision-making. Any requirement that generation owners develop weatherization plans must emphasize that uniform practices across the fleet are not necessary, but rather the portfolio of assets should be optimized to maximize the benefits less costs of weatherization practices. Information from FERC and NERC on the incremental effect of weatherization on loss of load probability would at least help states and other actors translate into benefits that they can compare against the cost of more robust weatherization.

Generally, extending physical standards into the fuel security and weatherization space restricts procurement flexibility and intrudes upon regionally-tailored responses in the form of wholesale market design and/or state procurement processes. The states and regional reliability coordinators would benefit from NERC tools that provide better awareness and could inform changes to procurement processes, which NERC does not hold authority over in any event.

Improving the alignment of state procurement with future regional operating conditions is very important to BES reliability. This invites a role for improved

[9] 2019 FERC and NERC Staff Report, The South Central United States Cold Weather Bulk Electric System Event of January 17, 2018 (July 2019) (available at https://www.ferc.gov/legal/staff-reports/2019/07-18-19-ferc-nerc-report.pdf).

information rather than top-down standards. For example, comparing state surveys of fuel procurement practices to regional operating conditions is a valuable endeavor, as the MISO experience indicates, which helps state prudency review processes. In restructured areas, changes to capacity performance and energy price formation have demonstrably increased the alignment of merchant generators' fuel procurement and weatherization behavior with the reliable operation of the system (e.g., PJM). Neither context requires additional standards, which would raise costs and contention among stakeholders.

Panel II: The Impact of Cloud Based Services and Virtualization on BES Operations, Planning and Security

b) What are the security and operational concerns associated with the increased use of virtualization in utility environments that must comply with the NERC CIP Reliability Standards? How can the NERC CIP Reliability Standards adapt to the increased use of virtualization?

CIP, especially with respect to cloud and virtualization services, is a case where the appropriateness, nature, and stringency of standards come into question. Before pressing ahead with immediate identification of best practices in order to revise CIP, ELCON urges the Commission to review why the CIP process has deterred adoption of best practices. All speakers on Panel II indicated that CIP standards are inhibiting cloud-based and virtualization services. This is corroborated by a broad set of Registered Entities across sector categories, who have avoided use of cloud-based services because CIP standards deter deployment of some new services, even those with greater reliability benefits.

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.

To this day, entities do not know if CIP standards permit virtual services in BPS applications. CIP-003-6 to CIP011-2 presume a security architecture that is obsolete in a virtual world, namely, hardware is shared under virtualization so cyber assets do not fit neatly into a physical and electronic security perimeter. This flags a fundamental need to shift the basis for CIP standards as the pace of technological change continues to rapidly exceed the rate of response of standards development and review processes. Instead, grid cybersecurity policy should shift to encourage voluntary best practices in response to dynamic conditions.

CIP standards should not just be adapted for the technical parameters of virtualization, which will likely only "lock-in" practices that quickly become stale, but overhauled to focus on facilitating voluntary risk-informed decisions. The perverse effect of prescriptive standards is not isolated to virtualization and cloud-based

services, but also is evident in other CIP areas like supply chain management. 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.[10]

Instead of creating accidental harm, policy that motivates private sector innovation will drive development and adoption of 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.

More outcome and process-based approaches to CIP standards with clear risk-based performance benchmarks would bolster BES reliability and lower compliance burdens. While this is a bigger picture change to CIP, interim changes to CIP are necessary to swiftly enable access to virtualization services. This should be done by imposing minimal constraints and with the intent of enabling permission-less innovation, as vendors are highly motivated and better equipped to correct vulnerabilities far more quickly and effectively than a regulatory approval-based process can handle.

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

d) Discuss the potential security and operational benefits of cloud services and virtualized environments. For example, could the increased use of cloud and virtualized environments benefit operational planning and/or recovery and restoration processes?

Cloud services offer considerable security and operational benefits, but they vary based on context. Many companies find that cloud services enable more automated security operations and continuous monitoring that expedite response timeframes. Cloud services can be superior for security applications like controlling access points to specific levels. There is no single set of "best practices" in cloud services, so changes to CIP to enable cloud services must be careful not to restrict innovative growth and customized applications.

Cloud services also enable companies to leverage external expertise, as third party vendors can offer superior security services than NERC registered entities can provide themselves and at much lower cost (*e.g.*, malware protections, which are biggest attack category globally). However, regulatory constraints generally restrict decentralized cloud-based systems. CIP requirements inhibit some entities from tapping into greater expertise at far lower capital expense.

e) How should the NERC CIP Reliability Standards be modified to help assist entities in addressing compliance concerns related to cloud services, while still encouraging the adoption of cloud services for appropriate planning and operations applications?

Industry has been even more hesitant to adopt cloud-based services than virtualization, despite their reliability benefits, because of compliance uncertainty. Auditors' expectations for cloud-based products under CIP Version 5 are particularly unclear. Compliance problems with cloud services raise much larger questions about CIP compliance concerns.

ELCON stresses the need to differentiate CIP standards based on an entity's regulatory status and system impact risk. Industrial consumers and merchant generators are exposed to market forces and thus internalize operating risk. Their core incentives align with BES security and any perceived deficiencies in their cybersecurity practices result from information deficits, not a lack of motivation to address them. As such, NERC's role is better suited to promote better voluntary risk-informed decisions for these entities.

ELCON greatly appreciates the differentiated impact approach pursued under CIP to-date, but stresses that further differentiation that avoids new compliance burdens is warranted. Unexpected re-designations of entities by impact category can create major asset management problems without improving cybersecurity practices. For example, shifting a single manufacturing facility from Low to Medium BES impact status can raise compliance costs by close to $1 million.

Industrial consumers differ from other Low impact entities substantially in that their internal risk exposure exceeds their risk to BES reliability, which results in an exceptionally intrinsic risk management culture. Industrial consumers already have robust cybersecurity practices customized to their core operating businesses, which are not electricity. These practices are forward-looking and focus on adopting best emerging practices, whereas CIP standards codify best established practices.

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.

Given the unique circumstance of industrial consumers, the Commission should explore the creation of a "Low-Low" impact categorization for industrial consumers. This category could either be exempt from CIP standards or have far lower compliance stringencies. This, coupled with improvements in information flows, will result in industrial cybersecurity practices superior to what CIP standards require.

At the least, less prescriptive and more process-based approaches to CIP standards can preserve procurement flexibility but still need to address excessive reporting burdens and uneven enforcement. 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.

Flexibility should not come at the expensive of clarity. CIP compliance reviews vary by region and auditor group, creating substantial compliance uncertainty that deters adoption of innovative practices. Sharing templates or ordained cyber

configurations in advance may strike a balance to bolster compliance flexibility without sacrificing clarity.

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

Dated: August 22, 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.: August 22, 2019

/s/ W. RICHARD BIDSTRUP
W. Richard Bidstrup