Sector 8 Policy Input for the NERC Board of Trustees & Member Representatives Committee

August 19-20, 2020 Meetings

ELCON, on behalf of Large End-Use Consumers, submits the following policy input for the consideration of NERC's Board of Trustees (BOT) and the Member Representatives Committee (MRC). It responds to BOT Chairman Roy Thilly's July 15, 2020 letter to Jennifer Sterling, chair of the MRC.

SUMMARY

Large Consumers (Sector 8) are pleased with the development of the Electricity Information Sharing and Analysis Center (E-ISAC) and support the base elements of its Long-Term Strategic Plan.

1. **Strategic and Operational Focus Areas of the E-ISAC strategic plan.** E-ISAC's mission is right on point with a sound cybersecurity policy strategy; promote voluntary, risk-informed decisions by the private sector. E-ISAC's services and products could be better tailored to resource-constrained stakeholders whose core businesses do not include selling power. This includes better contextualization of risk mitigation strategies and data analytics, along with more expeditious transfer of classified information. Expanded coordination with other ISACs whose industries affect Large Consumers, such as ONG-ISAC and IT-ISAC, would be welcomed. E-ISAC should also employ expanded cost-benefit analysis.
2. **Recommendations for other E-ISAC Areas.** NERC should work to alleviate concerns that inhibit E-ISAC membership recruitment. NERC and E-ISAC should endeavor to codify E-ISAC's functional separation from NERC's compliance monitoring and enforcement arm as integral to the achievement of its strategic objectives.

Strategic and Operational Focus Areas

Cybersecurity policy in the electricity industry is most effective and economical when it promotes voluntary, risk-informed decisions by the private sector. E-ISAC's mission is well aligned with this. The Plan's three primary focus areas – Engagement, Information Sharing, and Analysis – are on-point with E-ISAC's mission. Large Consumers seek to make E-ISAC's fulfill its mission subject to reasonable budgetary constraints. Should E-ISAC's mission expand beyond this scope, Large Consumers' enthusiasm for the institution may change.

The Plan underscores E-ISAC's near-term objective to build and maintain membership and mentions useful areas for value-add. This is welcomed. E-ISAC's services and products could be better tailored to

resource-constrained stakeholders whose core businesses do not include selling power. For example, participation in the Cybersecurity Risk Information Sharing Program managed by E-ISAC has grown primarily for entities that pass the subscription costs onto consumers, whereas more cost-sensitive entities need to see a more robust net benefit proposition to justify participation. The effects of the new pilot project on participation should be incorporated into future cost structure considerations.

The value of E-ISAC sharing risk mitigation strategies and data and analysis depends on the suitability of its format and delivery parameters for the end user. Large Consumers already have detailed internal protocols to identify and mitigate operational cyber risk, and the nature and value of mitigating their information gaps varies. Large Consumers often factor in operational considerations for their facilities differently than utilities and thus their data needs differ. A stronger emphasis on contextualizing risk mitigation strategies and data analytics to non-utility stakeholders' needs would help enrich the value of E-ISAC services.

Contextualizing information better would help accomplish the Plan's objective to leverage threat information better to provide timely and actionable information. Routinized feedback from stakeholders will be important to strike the proper balance between information quality and expediency, as well as to inform E-ISAC on the types of information most useful to protect critical infrastructure (e.g., value-add to other subscription services that may come with vendor contracts). A particular area of value-add is to enable more expeditious transfer of classified information as the private sector often cannot procure these services in the marketplace.

E-ISAC's intent to improve collaboration with other strategic partners should emphasize other ISACs in industries that cover Large Consumers' registered entities. The Plan recognizes the need to do so with the MS-ISAC and DNG-ISAC, which is prudent given interstate commerce and natural gas-electric industries' interdependencies. It should also consider the ONG-ISAC and IT-ISAC.

Fulfillment of E-ISAC's mission could justify a rapidly ever-increasing budget, and thus cost-benefit tradeoffs should be recognized to permit proper budget scrutiny. At minimum, the development of valuations for E-ISAC's service would help inform prioritization of scarce resources. Large Consumers support the planned use of cost-benefit analysis for automated information sharing and would like to see the technique applied broadly across E-ISAC services.

Recommendations for other E-ISAC Areas

NERC should also work to alleviate concerns that inhibit E-ISAC membership recruitment, including those regarding the opacity of E-ISAC's strategic direction as it transitions to the Department of Homeland Security's multi-infrastructure framework. The current E-ISAC Code of Conduct lacks safeguards to protect against entities' information from being used in a purpose outside of the scope of E-ISAC's mission. In particular, entities that bear the costs of critical infrastructure protection (CIP) standards seek assurances that information submitted to E-ISAC will not result in cost-additive changes to CIP standards.

NERC established E-ISAC to catalyze *voluntary* information sharing within the electricity industry, but the Federal Energy Regulatory Commission (FERC) appears intent to use it as a conduit for setting *involuntary* reliability standards. As of January 2020, FERC and NERC do not appear to agree on the role of information collected under E-ISAC with respect to standards setting. FERC even went as far as to say that they "are concerned that NERC believes that the only information it can use from the E-ISAC to

inform Reliability Standards development is the information contained in the public reports" and requested a NERC filing to help FERC better understand how E-ISAC informs the development of Reliability Standards.[1] Last month, NERC submitted an answer that correctly articulated why NERC sought to establish a clear separation between E-ISAC and its mandatory compliance and enforcement functions in 2012.[2] Given FERC's posture, NERC and the E-ISAC's should endeavor to codify functional separation for E-ISAC as integral to achievement of its strategic objectives.

Relatedly, the E-ISAC would benefit from better characterization of its prospective activities relative to its mission. Some areas may be only tangentially related to its mission and be better addressed by another organization. E-ISAC should endeavor to avoid mission creep through mission alignment reviews of prospective areas and have safeguards against incessant incrementalism that can escape many standard measures of performance review.

[1] See Docket No. RR19-7-000, p. 67. https://www.ferc.gov/sites/default/files/2020-05/E-20_3.pdf
[2] See p. 14. https://elibrary.ferc.gov/idmws/file_list.asp?document_id=14787441