Sector 8 Comments on NERC Draft Supply Chain Risks Report
March 1, 2019

ELCON, on behalf of Large End-Use Consumers (Sector 8), submits the following comments on NERC's draft "Cybersecurity Supply Chain Risks" report dated February 6, 2019. Large Consumers place a particularly high value on electric reliability and appreciate NERC's diligence in evaluating the risks to Bulk Electric System (BES) security posed by supply chain compromises from cyber attacks. Large Consumers also place a high value on procurement flexibility and are very sensitive to cost impacts. As such, Large Consumers seek to ensure that NERC actions on cybersecurity have demonstrated reliability benefits that justify any added costs, rely on incentives instead of standards where appropriate, and preserve procurement flexibility throughout the supply chain.

High and Medium Impact BES Cyber Systems

In the draft report, NERC Staff recommends revising the Supply Chain Standards to address Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) that provide physical access control to high and medium impact BES Cyber Systems, excluding alarming and logging. Large Consumers appreciate the recognition of differentiated treatment for EACMS based on risk level: namely that electronic access controls present a higher risk than monitoring and logging systems. Large Consumers agree with supporting NERC Staff's recommendation that only EACS be included and not monitoring and logging systems.

In addition, Large Consumers encourage NERC to work with industry to explore opportunities to streamline the verification process for EACMS, protect procurement flexibility, and promote information sharing. Industry does not support prescriptive standards, preferring flexibility in application and implementation.

Low Impact BES Cyber Systems

NERC Staff recommends:

- Entities voluntarily apply Reliability Standard CIP-013-1 Requirement R1 supply chain risk management plans to low impact systems.
- No modification of the Supply Chain Standards to include low impact BES Cyber Systems.

- Continued monitoring through the use of pre-audit surveys and questionnaires to determine whether new information supports modifying the standards to include low impact systems.

Large Consumers appreciate the recognition that low-impact BES Cyber Systems pose a low risk to the reliability of the BES and support the recommendation that low-impact BES Cyber Systems should not be included in the Supply Chain Standards. The report gives appropriate consideration to the impact framework as it currently exists in the CIP suite of standards. Large Consumers underscore the report's recognition that risk is mitigated as organizations with medium and high impact systems implement supply chain standards across their fleet that includes low-impact BES Cyber Systems. The report correctly notes that risk is further mitigated by supply chain vendors who implement supply chain standards across their systems, not knowing whether they will reside in low, medium or high impact systems.

NERC Staff's recommendation that the low-impact BES Cyber System issue continue to be monitored is appropriate but needs additional clarity. The use of pre-audit surveys is well known and generally understood. However, the use of questionnaires is too ambiguous. In NERC Staff's presentation to MRC, they indicated that the "questionnaire" used to evaluate and monitor the low-impact BES Cyber Systems will be through Section 1600 data requests. Section 1600 data requests are a formalized process that is not voluntary whereas questionnaires are ad hoc and typically voluntary. The report should contain this information as opposed to the generic term "questionnaire" if Section 1600 data requests will be used exclusively, or at least mentioned if used in addition to pre-audit surveys and questionnaires.

Perceived deficiencies that surveys, questionnaires, or data requests may reveal do not necessarily require modifications to mandatory standards. Doing so may be counterproductive – given the rapid pace that cyber threats and best practices evolve – or, at least, may impose excessive costs or restrictions on operations and procurement flexibility. Large Consumers strongly recommend the report retain the language on accounting for costs and expected benefits in considering mandatory requirements for low impact systems and add language recognizing that mandatory requirements are unnecessary where the incentives of vendors and low impact entities are aligned with BES security.

Where entities' incentives align with BES security, NERC should explore tools to motivate voluntary improvements by helping entities make better risk-informed decisions tailored to their unique circumstances. As such, additional information collection efforts should be done in mind with enhancing voluntary actions by entities with low-impact BES Cyber Systems.

NERC staff may want to tailor questions in any surveys, questionnaires, or data requests to not only evaluate current practices, but also gauge obstacles to adoption of best practices and cost considerations of changing practices. This would inform next steps on considering modifications to standards affecting low impact systems, such as better accounting of costs and expected benefits, as well as the efficacy of improved guidance and information sharing to improve voluntary practices in lieu of mandatory standards. For example, NERC could issue guidelines for on-site testing and other processes as an alternative to prescriptive management of supply and transport arrangements.

###