Sector 8 Policy Input for the NERC Board of Trustees & Member Representatives Committee August 9-10, 2017 Meetings in Ottawa, Canada

ELCON, on behalf of Large End-Use Consumers, submits the following input for consideration of the NERC Board of Trustees (BOT) and the Member Representatives Committee (MRC). It responds to BOT Chairman Roy Thilly's July 5, 2017 letter to John Twitty, Chairman of the MRC.

SUMMARY

Item 1: Supply Chain Risk Management

ELCON supports expedited outreach activity similar to the CIP v5 Transition Program, which involved a range of activities. This model included workshops, webinars, Lessons Learned, user guides, implementation studies, as well as invaluable information on implementation and compliance. This same model of outreach will help support implementation prior to the mandatory enforceable dates for CIP-013-1 and the modifications to CIP-005-6 and CIP-010-3.

Data analysis will provide a good indication of the effectiveness of the supply chain risk management standards going forward. Should any successful cyber-security incidents occur through the supply chain, these should be captured through the Incident Reporting (CIP-008) and Events Analysis (EOP-004) processes, as well as E-ISAC and other venues where data is collected.

Even though low-impact BES Cyber Systems are not specifically included in CIP-013-01, the risks associated with low impact BES Cyber Systems will be reduced by the implementation of the high-impact and medium-impact CIP requirements. The high water mark will apply on both the registered entity side and the vendor side.

Vendors and suppliers know their products best. The ERO should engage with them to share potential risks and how to keep the supply chain management process secure. NERC may consider pursuing the creation of a vendor cyber certification program.

Item 2: ERO Enterprise Consistency Concerns

ELCON would like to see NERC conduct regular reviews of both the CMEP and ORCP programs. The steady state assessments of Reliability Standards may provide an effective template for this.

SECTOR 8 INPUT

Item 1: Supply Chain Risk Management

On July 21, 2016, in Order No. 829, FERC 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 (BES) operations. The Cyber Security Supply Chain Risk Management Standard Drafting Team (SDT) drafted a new Reliability Standard CIP-013-1 and proposed modifications to CIP-005 and CIP-010 to address these directives. The standards are expected to be presented to the Board for adoption on August 10, 2017. The SDT presented a risk-based approach focused on high and medium impact BES Cyber Systems, while not including standard requirements for low impact BES Cyber Systems. To support effective implementation of these new Reliability Standard requirements by industry, NERC is committed to collaborating with industry cyber security supply chain subject matter experts to identify best practices, develop additional guidance resources, and promote a common understanding of compliance obligations. These standards will not end the need to continue to focus on the cyber security challenges presented by emerging new technologies or upgrades of older technologies. To facilitate and focus NERC's ongoing and collaborative efforts, the Board requests MRC policy input on the following questions:

1. What activities or studies NERC should engage in between now and the effective date of the new and modified standards to support effective implementation?

ELCON Response: The supply chain cyber security objectives that FERC established in Order 829 are extensive – and ELCON believes that a major transition program should be enacted quickly to support implementation. The CIP v5 Transition Program, which involved a range of activities, provides a good model. Workshops, webinars, Lessons Learned, user guides, implementation studies, and the v5 Transition Advisory Group all provided industry, and the ERO, with invaluable information on implementation and compliance. This outreach will help support implementation prior to the mandatory enforceable dates for CIP-013-1 and the modifications to CIP-005-6 and CIP-010-3.

ELCON envisions in-depth studies, Lessons Learned, and discussions surrounding:

a) Proper application of risk-based principles into the supply chain policies (i.e.; how to prioritize equipment and vendors – and collect evidence justifying findings that will satisfy Compliance Enforcement Authorities);
b) Impact of the Implementation Note in R2 (i.e.; how to ensure compliance when a contract cannot be renegotiated, and what to do with poor performing vendors);

c) Types of controls expected at each stage of the product life cycle;
d) Acceptable methods to verify digital signatures on software upgrades and patches once so they can be deployed across an entity's cyber system base safely, but with minimal disruption; and
e) Most prevalent types of Interactive Remote Access and system-to-system remote access subject to the new CIP-005-6 requirements and the associated controls required of each.

This is not an exhaustive list. We should expect that the need for other studies, workshops, webinars, and lessons learned will arise as implementation begins.

2. How should NERC evaluate the effectiveness of the standards going forward?

ELCON Response: ELCON believes that data analysis will provide a good indication of the effectiveness of the supply chain risk management standards going forward. With the implementation of the standards, the vulnerabilities and risk are reduced. If there are successful incidents of cyber-attacks through the supply chain, these should be captured through the Incident Reporting (CIP-008) and Events Analysis (EOP-004) process, as well as the E-ISAC and possibly other venues where data is collected. Reported incidents should be evaluated to determine the access method (through remote communications, compromised patches/software, or physical installation); the stage of the life cycle where the attack occurred (during manufacture, installation, post-installation); and attack vector (employee sabotage, social engineering, successful hack).

3. What risks and related issues should NERC continue to study on a collaborative basis related to the challenges of cyber security supply chain risk management, including risks related to low impact BES Cyber Systems not covered by the standards?

ELCON Response: ELCON believes that the risks and related issues of most impact to the Registered Entity base will arise naturally during the transition program and metrics gathering process. As an issue emerges, NERC can determine if further research is appropriate, and what form it should take (i.e.; a study, work-shop, focus group, etc.).

Although low-impact BES Cyber Systems are not specifically included in CIP-013-01, he risks associated with low impact BES Cyber Systems will be reduced by the implementation of the high-impact and medium-impact CIP requirements. The high water mark will apply on both the registered entity side and the vendor side. As applicable entities with high and/or medium, as well as low, impact BES cyber systems implement CIP-013, the same procurement process will be implemented across all impact levels. Registered entities will not implement their procurement process differently depending on the impact level of their identified BES cyber systems. The same is true of vendors. The same vendors who provide services to high and medium impact entities, provide services to low impact entities. Once they update their supply chain processes to facilitate compliance with CIP-013, they will be rolled out to entities of all impact levels, not just medium and high impact entities and the mitigation of risk will filter down to the owners/operators of low-impact BES Cyber Systems. Registered entities contract with many of the same vendors (e.g.; GE, CISCO), and will

benefit from the process improvements the vendors make in response to CIP-005-6, CIP-010-3, and CIP-013-1. Some small vendors may lag somewhat in response to the new requirements, but the impact to their business from high and medium-impact BES Cyber System owners will require them to step up their game sooner rather than later.

4. For assets that are not subject to the new cyber security supply chain risk management requirements, are there other actions NERC should take to address potential supply chain risks, such as developing guidelines, presenting webinars and/or collaborating with the Forums and small system representatives on strategies and best practices?

ELCON Response: Vendors and suppliers know their products best. The ERO should engage with them to share potential risks and how to keep the supply chain management process secure.

NERC may consider pursuing the creation of a vendor cyber certification program. (This may be best facilitated by the Department of Homeland Security, being that cyber security affects every major national infrastructure.) The oversight of a vendor who achieves "certified" status would not be as intense under the CIP standards – a clear financial benefit to potential customers. As a result, a certified vendor would have a leg-up on the competition; justifying their investment of time and money into the effort.

NERC (or the DHS) could charge a certification fee to offset some of the costs, but the primary benefit to them would be direct access to a community not under their regulatory umbrella. Because certification is voluntary, they could review and assess the cyber capabilities employed by vendors – and demand changes when vulnerabilities are detected. Furthermore, changes could be rapidly introduced to the program if and when new cyber threats are identified.

ERO Enterprise Consistency Concerns

In addition, I'd like to highlight the framework developed by the ERO Enterprise to address consistency concerns and identify best practices while allowing for innovation in the execution by the ERO Enterprise of both the Compliance Monitoring and Enforcement Program (CMEP) and the Organization Registration and Certification Program (ORCP). A panel discussion will be held during the August Board Compliance Committee (BOTCC) meeting to discuss this important effort. I encourage and look forward to input during this panel discussion, which may carry over to the MRC meeting.

ELCON would like to see NERC conduct regular reviews of both the CMEP and ORCP programs. The steady state assessments of Reliability Standards may provide an effective template (i.e.; assemble an expert team, assess the relevance of the materials, update them for new findings, and eliminate obsolete/redundant items). Our experience with that process has been quite positive.

While recognizing the sensitivity of any one audit team's job performance in accordance with the consistency criteria, ELCON would like the ERO Enterprise to consider the posting of summary records. Inconsistencies in the number and penalty assessments for violations

to a given standard may indicate a misunderstanding of its reliability purpose – that may be affecting multiple CEAs. Or, it is possible that one team is doing it correctly and others may need further guidance on a specific requirement.

One category of particular interest to Large Industrials is the consistent application of the risk-based compliance and registration programs, such as the Inherent Risk Assessment ("IRA") process, which is quite inconsistent among Regional Entities. By their very nature, these programs introduce uncertainty into the regulatory approach and it would be helpful to see where there are gray areas affecting regional audit/registration teams. ELCON absolutely supports the risk-based concept, and believes it to be leading to an overall improvement in BES reliability. Consistency summaries may help prove the point.

ELCON anticipates an inconsistent approach will prevail for a while and believes that summary data will drive the uniformity process.

###