From: Guy V. Zito
To: rsballot
Cc: rscmembers
Subject: NERC Ballot- Project 2016-03 Cyber Security Supply Chain Risk Management
Date: Thursday, March 2, 2017 4:53:27 PM
Importance: High

NPCC Members and Entities of the NERC Registered Ballot body.

The subject project is currently posted for formal comment and initial ballot through 8pm March 6th, 2017. TFIST has reviewed, discussed, and arrived at a consensus recommendation to the RSC to vote Negative on the subject project. The RSC however has not reached a recommended voting position regarding this initial ballot. Below is a subset list of the more significant issues that have been received both from the TFIST and other issues raised during our RSC review. NPCC is in the process of combining and developing a regional response. I also urge your respective organizations to concentrate comments on major issues. The first version of this standard doesn't have to be perfect however does have to address the FERC Directives. NPCC will endeavor to address the concerns through our comments and participation in the SDT activities. I want all to keep in mind that NERC has committed to having a stakeholder approved standard brought to the Board of Trustees for approval at their August 2017 meeting.

At this time, for the initial ballot **NPCC as the Regional Entity, will be abstaining,** in recognition of the number of issues raised by our members and entities. Some of the issues identified thus far are as follows:

- CIP-013 should move forward with only R1 and R2 since they are mostly procurement related-some concern is being expressed that the requirements for having a supply chain risk management plan seem to a cover low medium and high BES Cyber assets as well as allowing entities to assess their own risk. Further clarification and perhaps some third party verification would be beneficial.
- Contractual issues could exist. Although the FERC order doesn't require abrogation of contracts there is some concern that there could end up being multiple contracts in place, those newly negotiated and the existing ones. Confusion exists between use of terms vendor and suppliers in the draft standard and the Guidance section.
- Concerns exist regarding authentication on multiple levels and how vendors and their manufacturers may combine hardware and software into their products and how there could meaningful verification and authentication
- There are a number of areas where time seems to be an issue as it relates to implementation
- Use of "applicability tables" as they appear in other CIP standards would clarify the requirements to alleviate compliance concerns
- R3, R4 and R5 should move into existing CIP Standards to avoid P81 issues (redundancies) and ease implementation for Entities and improve auditability efficiencies.

A number of entities have expressed concern that he standard, as written, will not accomplish the objective of the four Directives appearing in Order 829 which the standard must address:

(1) Software Integrity and Authenticity
(2) Vendor Remote Access
(3) Information System Planning
(4) Vendor Risk Management and Procurement Controls

As written, the standard does attempt to accomplish addressing these, however clarifications and improvements could be made. NPCC and many of its members will be submitting detailed comments beyond the small subset appearing above. We will actively participate to try to address the issues pointed out by our entities, however it is noted that there will be many challenges for the drafting team to produce a standard that meets the Directives and is meaningful for security. It is also important that for all entities intending on submitting comments and voting negatively to please provide guidance to the drafting team on what would be acceptable and result in a positive vote as revisions are considered. NPCC's regional comment form will be posted shortly at :
https://www.npcc.org/Standards/Regional%20Standards%20Comments/Forms/Public%20List.aspx

If you have any questions please contact me.

Thanks,

Guy V. Zito
Chair of RSC, NPCC Asst. Vice President of Standards