NPCC Members and Entities of the NERC Registered Ballot Body,

The NPCC Regional Standards Committee (RSC) has reviewed the subject ballot and received input from the NPCC Task Force on Infrastructure Security and Technology (TFIST) for the subject posted material under an initial ballot and formal comment period which will close on February 3, 2020 at 8pm. The issues with the draft standards which have been identified are related to revoking access, nebulous meaning of what constitutes “key management” and demonstration of compliance when redeploying assets after they were previously destroyed or sanitized. The NPCC RSC Members have not indicated support for the standards as they currently are drafted. There is an opportunity for improving the standards and NPCC and its members will be working with the NERC drafting team on future drafts to address NPCC member’s concerns should these standards fail ballot.

NPCC is collecting up the comments submitted for the posted materials and will be submitting them and posting them on the NPCC website shortly. NPCC as the Regional Entity, at this time, will abstain from this ballot in recognition that the SDT is aware of the issues and it is our understanding that they will be developing another draft.

If you have any questions please contact me.

Thanks,

Guy V. Zito
NPCC Asst. Vice President - Standards
Chair of the RSC
The attached Word has TFIST’s consensus comments on the proposed BCSI updates.

TFIST recommends voting NO on all five of the BCSI ballots because of CIP-011. If CIP-011 was acceptable, TFIST would recommend voting YES. The BCSI ballots are

- CIP-004
- CIP-011
- Non-binding vote on CIP-004
- Non-binding vote on CIP-011
- Implementation Plan

Expect some NPCC Members to submit their own additional comments. While no showstoppers, here are CIP-011 near showstoppers and these vary by Member

- Part 1.1
- Part 1.4 - how does an Entity mitigate third parties?
- Part 1.5
  - calls for individual access termination which is problematic when a third party is working on your information at their location
  - earlier Parts call for dealing with vendors not their staff – SDT needs to be consistent
- Part 2.2
  - could not reach consensus
  - This part requires separation of custodial duty from key management program. How to separate when one staff does both?
- Part 3.1 - how to demonstrate that a virtualized asset was sanitized/destroyed before reuse/disposal?

-brian