From:	Guy V. Zito
To:	rscmembers
Subject:	FW: Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | 8-day Final Ballot Open through January 22, 2019
Date:	Tuesday, January 15, 2019 12:38:57 PM
Attachments:	image001.png

RSC Members,

The subject standard passed the "Additional Ballot" last year with a 75.54% approval. The SDT made non-substantive changes (minimal) to allow the standard to move to a "Final Ballot" and maintain a passing vote. TFIST continues to express concerns with the standard and again has sent me similar concerns to those sent to us during the last ballot:

"TFIST recommends a NO vote on this new CIP-008 ballot.
While this is only a ballot (no comments), here are some technical reasons why TFIST makes this recommendation

- *Security concerns on Physical Security Perimeters, Electronic Security Perimeters and Protected Cyber Assets (PCAs). TFIST feels that compromised PCAs are serious and should be reported. The Standard's Applicable Systems section does not include PCAs. So, an Entity is not required to report a compromised PCA.*
- *As in other Standards, CIP-008 needs proper English since that impacts interpretation. Examples are 1) misplaced phrases, 2) punctuation, and 3) lack of clarity. TFIST cannot agree on interpreting the definitions and at least some of the Requirements. One could reasonably expect an incident handling Standards to be the easiest to read and most concise. Lack of clarity results in different interpretations and conclusions between Regional Entities, Auditors and Entities.*
- *The Implementation Guidance reads as a white paper which is inconsistent with the Standard which defines what is reportable or not.*
- *There is a gap between the two definitions, 1) Reportable Cyber Security Incident (RCSI) and 2) Cyber Security Incident (CSI). RCSI states that compromises to BES Cyber Systems (among other things) are reportable. The CSI definition does not include compromises to BES Cyber Systems."*

The Standard has passed its initial Additional Ballot period so all votes previously cast will remain in place for this ballot unless entities want to change their vote. At this time I continue to emphasize the important of the need to approve this standard**. It must be filed with the Commission by April 1, 2019.** Although TFIST concerns hold validity, reporting compromises on PCAs can be done voluntarily outside of a standard requirement and if a requirement were developed, it would require greater reporting which may be of limited value depending on the asset. I would suggest a better approach, given the timeframe, to allow this to pass and then if folks feel strongly about certain aspects of the standards, a SAR can be submitted in the future. It is highly likely that FERC will issue a NOPR to solicit comments on their concerns and a final Order may have Directives to change things. In addition, another mechanism in the Compliance area is available which might be beneficial to address some concerns (i.e. Implementation Guidance). I continue to suggest voting "**Affirmative**" on the posted materials.

If you have any questions please contact me.

Thanks,

Guy

From: NERC Standards Announcements (Do Not Reply) <NERC-StandardsAnnouncements-

DoNotReply@nerc.net>
Sent: Tuesday, January 15, 2019 12:02 PM
To: Wendy Muller <Wendy.Muller@nerc.net>
Cc: Alison Oswald <Alison.Oswald@nerc.net>
Subject: Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting | 8-day Final Ballot Open through January 22, 2019

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Announcement

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Final Ballot Open through January 22, 2019

Now Available

An **8-day** final ballot for **CIP-008-6 - Cyber Security — Incident Reporting and Response Planning** is open **Tuesday, January 15, 2019** through **8 p.m. Eastern, Tuesday, January 22, 2019.**

Balloting

In the final ballot, votes are counted by exception. Votes from the previous ballot are automatically carried over in the final ballot. Only members of the applicable ballot pools can cast a vote. Ballot pool members who previously voted have the option to change their vote in the final ballot. Ballot pool members who did not cast a vote during the previous ballot can vote in the final ballot.

Members of the ballot pools associated with this project can log in and submit their vote here. If you experience any difficulties using the Standards Balloting & Commenting System (SBS), contact Wendy Muller.

- *If you are having difficulty accessing the SBS due to a forgotten password, incorrect credential error messages, or system lock-out, contact NERC IT support directly at https://support.nerc.net/ (Monday – Friday, 8 a.m. - 5 p.m. Eastern).*
- *Passwords expire every **6 months** and must be reset.*
- *The SBS **is not** supported for use on mobile devices.*
- *Please be mindful of ballot and comment period closing dates. We ask to **allow at least 48 hours** for NERC support staff to assist with inquiries. Therefore, it is recommended that users try logging into their SBS accounts **prior to the last day** of a comment/ballot period.*

Next Steps

The voting results will be posted and announced after the ballot closes. If approved, the standard will be submitted to the Board of Trustees for adoption and then filed with the appropriate regulatory authorities.

Standards Development Process

For more information on the Standards Development Process, refer to the Standard Processes Manual.

For more information or assistance, Senior Standards Developer, Alison Oswald (via email) or at 404-446-9668.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

RELIABILITY | ACCOUNTABILITY