20191028-5082 FERC PDF (Unofficial) 10/28/2019 12:34:03 PM

October 28, 2019

FERC/NERC Staff White Paper on CIP Standards Notice of Penalties North American Generator Forum Comments Submittal

The North American Generator Forum (NAGF) appreciates the opportunity to provide the following comments regarding certain aspects of the subject white paper:

1. **The potential security benefits from the new proposed format**

   The NAGF believes the proposed NERC CIP NOP submissions proposal process that consists of a public cover letter and a separate CEII designated, non-public, CIP NOP filing containing details on the nature of the violation, mitigation activity, and potential vulnerabilities to cyber systems will help ensure clarity regarding the public dissemination of potentially sensitive information and simplify the submission/processing of CIP NOPs. By removing the technical details that are now publicly available, bad actors would have a diminished capability to potentially exploit vulnerabilities and thus, security of the BPS would be improved.

2. **Any potential security concerns that could arise from the new format**

   The NAGF does not support the inclusion of the name of the violator in the public cover letter nor the identification of the Reliability Standard(s) violated. The NAGF supports the existing use of the term Unidentified Registered Entity (URE) in the public cover letter along with the penalty amount.

   The Bulk Power System is under constant attack from cyber intruders. The NAGF is concerned that releasing publicly the name of the violator could provide bad actors with the opportunity to "connect the dots" and develop a more robust hacking attack by using other publicly available information such those found in NERC Lessons Learned. In fact, a recent NERC Lessons Learned, "Risks Posed by Firewall Firmware Vulnerabilities," identified the mechanism used to disrupt communications between power plants and their control center. Furthermore, including the standard(s) involved in the violation in a public notice may provide sufficient intelligence to an informed hacker to better target an attack on the violating entity. For narrowly scoped standards such as CIP-005 dealing with electronic security perimeters, a bad actor may infer the issue to be with firewall or remote access controls. Providing a clear connection between the violating entity and the standards involved provides a readily accessible path for bad actors to focus attacks and threaten the security of the grid.

   In addition, the Joint Staff Report notes that public identification of the CIP violator, even without identifying the standards involved, may result in increased hacking activity, which is not a welcome result for the named entities. As a result, the NAGF firmly supports the present approach in which the use of the URE term is employed. If FERC ultimately determines to publicize the name of the entity, the NAGF strongly recommends that the Reliability Standards involved be included in the confidential attachment but not in the public cover letter.

3. **Any other implementation difficulties or concerns that should be considered**

   The NAGF identifies several concerns with the proposed implementation strategies.

20191028-5082 FERC PDF (Unofficial) 10/28/2019 12:34:03 PM

- *NERC registered entities currently have the ability to review non-attributable CIP violations on the NERC CIP NOP spreadsheets, from which lessons learned or other valuable insights can be gained for application to their host systems and environments. FERC's proposal eliminates the opportunity for Registered Entities to access the technical information concerning CIP violations, eliminating a source of potentially useful information. In this regard, as a supplemental proposal, the NAGF recommends that NERC, the Regional Entities, and industry participants collectively develop a secure mechanism by which technical, non-attributable CIP violation information is still accessible by industry participants.*
  The NAGF also recommends that FERC and NERC review other sources of CIP NOP related information to understand the complete scope of CIP NOP information that is being made available to the public.

- *Publicizing the name of the CIP-violating entity without further detail or context on the issues creates potential issues for that entity. In the absence of further detail about the nature of the violation, the entity will likely encounter unfounded, and possibly extreme, speculation on the type and severity of the issues, which places the entity in the position of: (1) divulging further details to correct the record, thereby creating additional security risk; or (2) staying silent and risk reputational harm based on the public image presented.*

- *A high majority of the violations NERC processes are identified through entity self-reports. This proposal may demotivate entities to self-report in the future for two reasons. First, entities with identified CIP violations may opt to internally mitigate the issue but will be much less inclined to self-report it when faced with the possibility that their name will be publicly identified with the standards involved, thereby increasing the risk to maintaining security of their systems and networks. This then also results in a potential downside in the audit process when Regional Entity auditors determine the violations were not self-reported, resulting in a poorer compliance culture. And secondly, merchant generators operate with slim margins generally. The potential reputational harm as outlined above and the resultant impact on facility acquisition values may also create disincentives for self-reporting.*

4. Does the proposed format provide sufficient transparency to the public?

The NAGF cannot comment on the sufficiency of the format to satisfy FERC's objectives on this matter. However, the NAGF does not believe the violator's name should be publicized; therefore, the NAGF does not support the proposal format as presented.

20191028-5082 FERC PDF (Unofficial) 10/28/2019 12:34:03 PM

Document Content(s)