UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards	)	Docket No. AD19-18-000

COMMENTS OF GEORGIA SYSTEM OPERATIONS CORPORATION AND GEORGIA TRANSMISSION CORPORATION

Georgia System Operations Corporation ("GSOC") and Georgia Transmission Corporation ("GTC") appreciate the opportunity to submit these comments to the Federal Energy Regulatory Commission ("FERC" or "Commission") in response to the *Joint Staff White Paper on Notices of Penalty Pertaining to Violations of Critical Infrastructure Protection Reliability Standards* filed in this docket on August 27, 2019 ("White Paper").[1] To address concerns related to Freedom of Information Act ("FOIA") requests for Notices of Penalty ("NOPs") associated with violations of Critical Infrastructure Protection ("CIP") reliability standards, the joint staffs of the Commission and the North American Electric Reliability Corporation ("NERC") propose, in the White Paper, a new filing format for CIP NOPs. Specifically, the White Paper proposes that NERC would file a public cover letter that discloses the name of the registered entity, the Standards(s) that were violated, and the amount of the penalty imposed along with a non-public attachment for which NERC would request a designation as Critical Electric Infrastructure Information ("CEII").

The non-public attachment would provide all other information regarding the associated CIP-related violations that is typically included in a NOP. The CEII designation would exempt

[1] Comments initially were due on September 27, 2019, but the Commission provided an extension in response to a Motion for Extension of Time to File Comments filed by EEI and other trade associations. As a result, comments are now due October 28, 2019.

the information provided in the non-public attachment from disclosure under FOIA.[2] This represents a change from current practice to the extent that the names of registered entities and other details about the CIP reliability standard violations are not, currently, filed as public information.

GSOC is a not-for-profit system operations company and GTC is a not-for-profit transmission company. Both operate as cooperatives. Our members are 38 of Georgia's distribution electric membership corporations and Oglethorpe Power Corporation. GSOC and GTC are two of four companies formed to provide and deliver wholesale electric services that help light up half the households in Georgia, covering two-thirds of the state. GSOC is registered as a Transmission Operator while GTC is registered as a Distribution Provider, Planning Authority/Planning Coordinator, Transmission Owner, Transmission Planner, and Transmission Service Provider. Both GSOC and GTC are subject to the mandatory reliability standards enforced by NERC, the Regional Entities, and the Commission. Accordingly, GSOC and GTC are directly affected by proposal set forth in the White Paper.

I. NOTICE AND COMMUNICATIONS

All notices and communications with respect to this proceeding should be directed to

Christina Bigelow
Director, Legal and Compliance
GSOC
2100 East Exchange Place
Tucker, GA 30084
(770) 270-7902
christina.bigelow@gasoc.com

[2] *See* Fixing America's Surface Transportation Act ("FAST Act"), Pub. L. No. 114-94, § 61003 (specifically exempting the disclosure of CEII and establishing the applicability of FOIA exemption 3, 5 U.S.C. § 552(b)(3), which bars disclosure under FOIA of material that is protected under other federal law).

II. BACKGROUND

As described above, the White Paper proposes a revised filing format for CIP NOPs. It provides that future:

> …NERC CIP NOP submissions would ***consist of a proposed public cover letter that discloses the name of the violator, the Reliability Standard(s) violated (but not the Requirement), and the penalty amount***. NERC would submit the remainder of the CIP NOP filing containing details on the nature of the violation, mitigation activity, and potential vulnerabilities to cyber systems as a non-public attachment, along with a request for the designation of such information as CEII.[3]

The White Paper further proposes to extend this filing strategy to "…future Spreadsheet NOPs, Find, Fix, Track, and Report issues, and Compliance Exceptions."[4]

In the White Paper, the Commission and NERC staffs requested comments on:

- The potential security benefits from the new proposed format;
- Any potential security concerns that could arise from the new format;
- Any other implementation difficulties or concerns that should be considered; and
- Whether the proposed format provides sufficient transparency to the public.[5]

The White Paper also indicated that commenters may offer other, suggested approaches to the format of CIP NOPs that address the need to protect sensitive information that could be useful to a person planning an attack on critical infrastructure while balancing the goals of transparency and efficiency. In response to this request for comments, GSOC and GTC offer their comments below.

III. COMMENTS

GSOC and GTC appreciate the efforts of NERC and the Commission to "balance" transparency, security, and efficiency through the White Paper, but are concerned that: (1) the proposed changes to the NOP format do not present the optimal balance between transparency,

[3] *See* White Paper at p. 3.
[4] *Id.* at p. 11.
[5] *Id*. at p. 4.

efficiency, security, and disclosure and (2) unintended consequences and administrative burdens may result in the inadvertent deprioritizing of security in favor of transparency. There are likely disadvantages and unintended consequences with the White Paper's proposal that reduce or eliminate its benefits to the reliability and security of the Bulk Power System ("BPS"). GSOC and GTC respectfully suggest that these concerns could be alleviated by aligning the reporting practices associated with the Commission's enforcement of compliance with reliability standards with its reporting practices for other enforcement-related activities under the Commission's purview and authority. In particular, GSOC and GTC would recommend that the Commission consider applying comparable reporting practices for reliability standards compliance enforcement and the Commission's other enforcement-related activities based on risk and impact. Such alignment would allow the Commission to better protect information that could be used to undermine the security of the BPS, while providing an appropriate level of transparency about its enforcement of compliance with the CIP reliability standards.

One significant, yet unintended, consequence of the White Paper proposal is that registered entity education and information regarding CIP-related issues, best practices, and appropriate risk mitigations would be eliminated based on the timing and content of CIP NOPs set forth in the White Paper. Such information and education provides a security benefit as registered entities can and do review the available, redacted CIP NOPs to evaluate their own activities and identify areas for improvement. While it would be an unintended consequence, the removal of registered entities' ability to do so or do so in a timely manner reduce the overall security benefits to the BPS.

The achievement of a more optimal balance of transparency, security, and efficiency/administrative burden is, however, possible by aligning the Commission's general reporting practices for enforcement-related activities with its reporting practices regarding

enforcement of reliability standards compliance. GSOC and GTC respectfully suggest that, if implemented consistent with the changes suggested in these comments, revisions to CIP NOP filing and format could serve to increase security, transparency, and the protection of CEII while reducing administrative burden. Finally, GSOC and GTC respectfully request that the Commission prioritize ensuring that its new filing format does not adversely impact the availability of useful information to registered entities.

A. FOIA Considerations Provide An Important Backdrop For The Commission's Consideration Of The White Paper Proposal.

The primary purpose of the FOIA was to open administrative processes to the scrutiny of the press and general public.[6] Specifically, in *Renegotiation Bd. V. Bannercraft*, the court observed that the FOIA had, "...the ultimate purpose of enabling the public to have sufficient information to be able, through the electoral process, to make intelligent, informed choices with respect to the nature, scope, and procedure of federal governmental activities."[7] FOIA is intended to **balance** the public and privacy interests prior to disclosure.

Specifically, the Supreme Court has ruled that, when determining whether a federal agency was required to disclose information requested pursuant to the FOIA, a court had to balance the public interest in disclosure against the privacy interest Congress intended to protect.[8] Hence, FOIA's exemptions are integral to this balance and, as the White Paper recognized, several FOIA exemptions apply to CIP NOPs.

These include Exemption 3, which allows the government to withhold from disclosure information specifically exempted from disclosure by statute "if the statute affords the agency no

[6] *Renegotiation Bd. v Bannercraft Clothing Co.,* 415 U.S. 1, 39 L.Ed.2d. 123, 94 S.Ct. 1028 (1974).
[7] 149 L.Ed.2d 1113 (2nd 2012).
[8] 149 L.Ed 2d 1113 (2nd 2012); *Bibles v Oregon Natural Desert Ass'n*, 519 U.S. 355, 136 L.Ed.2d 825, 117 S.Ct. 795 (1997), infra § 45.

discretion on disclosure, or establishes particular criteria for withholding the data, or refers to particular types of information to be withheld."[9] Relative the CIP NOPs, the FAST Act is, as recognized in the White Paper, applicable because such filings "relate details about the production, generation, transportation, transmission, or distribution of energy," and "could be useful to a person in planning an attack on critical infrastructure."[10]

Exemption 7 is another FOIA exemption that the White Paper recognized as applicable and under which the CIP NOPs could meet the requirements for several subparts depending upon the violation, risk, likelihood, and impact of exploitation of such information. [11] It exempts from disclosure "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information […]" would interfere with legitimate law enforcement efforts or due process concerns.[12] Because the information included in CIP NOPs are generated as a result of violations of CIP reliability standards, the information is appropriately considered to be collected for law enforcement purposes under Exemption 7.

Finally, Exemption 4, which protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential,"[13] should be considered by the Commission as it balances the interests related to CIP NOPs. The Supreme Court explained, in *Food Marketing Institute v. Argus Leader Media*, 139 S.Ct. 2356 (2019), that information is "confidential" for the purposes of Exemption 4 "[a]t least where commercial or financial information is both customarily and actually treated as private by its owner and provided to the government under an assurance of privacy."[14] Information submitted by registered entities during

[9] *Baldrige v. Shapiro*, 455 U.S. 345, 352-53 (1982); *see also* 5 U.S.C. § 552(b)(3).
[10] *Id.*; *See* also White Paper at 3.
[11] Exemption 7(a), (e), (f).
[12] 5 U.S.C. § 552(b)(7).
[13] 5 U.S.C. § 552(b)(4).
[14] *Food Marketing Institute v. Argus Leader Media*, 139 S. Ct. 2356, 2366 (2019).

the enforcement process is generally considered confidential by such entities and, under the NERC Rules Of Procedure, is submitted under an assurance of privacy. Thus, even if the information does not rise to the level of CEII, it should be withheld from public disclosure under FOIA.

What is more, the Supreme Court has opined on what "public interest" may be weighed when an agency is balancing disclosure versus nondisclosure. It has determined that, when balancing involved interests in response to a disclosure request under the FOIA, the only relevant public interest is the extent to which disclosure would shed light on the agency's performance of its statutory duties or otherwise let citizens know what their government is up to.[15] This precedent is significant as the public interest expressed by requestors has not focused on the Commission's performance, but, rather, has focused on how "naming and shaming" violators would increase the security of the BPS. Further, given the inherently technical and complex nature of BPS operations and cybersecurity, it is unclear how the information being requested, *e.g.*, raw data such as violator names, standards, penalties, etc., would elucidate such performance without additional context.

FOIA requestors for CIP NOP filings repeatedly reference the public interest in grid security and reliability, but seek to de-sensitize significantly more sensitive information than is currently published, which would appear, *prima facie*, to undermine grid security and reliability. GSOC and GTC appreciate that the White Paper's proposal would reduce the likelihood for the publication of this information, but is concerned that such approach will not meet FOIA requestors' expectations, resulting in a more – not less – disputes over and disclosure of CIP NOPs and related information with very little (if any) attendant benefit to grid reliability and security. It is for these reasons that GSOC and GTC express concerns about whether the White Paper's proposal

[15] 149 L.Ed.2d 1113 (2nd 2012); *United States Dep't of Justice v Reporters Committee for Freedom of Press*, 489 U.S. 749, 103 L.Ed.2d. 774, 109 S.Ct. 1468 (1989), infra § 53; *United States Dep't of Defense v Federal Labor Relations Auth.*, 510 U.S. 487, 127 L.Ed.2d 325, 114 S.Ct. 1006 (1994), infra § 46.

constitutes an appropriate balance of interests, and, in response, suggests an alternate method for disclosure.

B. The White Paper Proposal Provides Additional Security Benefits, But May Not Meet FOIA Requestors' Expectations And May Increase Administrative Burden, Reducing The Overall Benefits.

GSOC and GTC agree with the Commission that the White Paper proposal for the filing of CIP NOPs presents a net increase of security benefits at the initial filing stage. However, it does not address how the Commission would respond to interveners in the associated filing dockets and/or other requesters that would request access to the non-public CEII data supporting the CIP NOPs under 18 CFR 388.113(g)(4) and (5). Hence, when considered *in toto*, the proposed benefits would be limited to circumstances where interested parties are satisfied with the publicly filed information. Otherwise, the White Paper proposal leaves the Commission in a similar position where a request for the non-public CIP NOP filings (CEII) is filed under 18 CFR 388.113(g)(4) and (5). Given the comments filed in this docket, every indication is that FOIA requestors would seek details beyond the White Paper proposal, thereby significantly reducing the security and administrative benefits that could otherwise be gleaned from that proposal.

Further, while there is a net security benefit that results from the proposed public or initial filing, this security benefit is still limited as saboteurs and malicious actors can easily access the publicly posted reliability standards and quickly discern where potential vulnerabilities could arise. For example, if an issue is identified under CIP-007, the likely vulnerabilities are ports and services, failure to patch, failure to monitor/alert, failure to maintain anti-virus protection, etc. While it would take a saboteur longer to identify a specific vulnerability, the proposed public filing would, nevertheless, provide them guidance regarding where to look and, as history has shown, saboteurs do not need to be "informed" to identify and exploit vulnerabilities. The proposed timing

of such filings mitigates this risk for the specific registered entity being penalized, but every piece of security-related information provides value to those who would seek to interrupt the transmission and distribution of electricity in North America.

Additionally, the White Paper proposal appears to equate certain pieces of data with transparency. While that may be true for this initial population of FOIA requests and associated requestors, the comments in response to the White Paper indicate that such may not be the circumstance that is applicable to every future FOIA request. Indeed, it is easy to envision future requestors utilizing ratepayer, membership, and other status to justify receiving more and different information relating to CIP NOPs, which would reduce and/or eliminate the security benefit and substantially increase the administrative burden for the Commission, NERC, regional entities, and registered entities.

For this reason, GSOC and GTC would respectfully suggest to the Commission that transparency is not synonymous with identity, penalty amounts, or even standard identifiers. Indeed, the provision of raw violation and/or penalty data without context, without knowledge of the operation of the BPS, and/or without knowledge of cybersecurity practices and principles would not only provide very little value to the public, but would also not be adequate indicia of the Commission's "performance of its statutory duties" or effective to "otherwise let citizens know what their government is up to,"[16] a key tenet of FOIA disclosure. Furthermore, GSOC and GTC submit that the lack of context and the publication of raw violation and/or penalty information may cause confusion, creating unnecessary concern and the potential for disputes over the status of grid reliability and security.

[16] 149 L.Ed.2d 1113 (2nd 2012); *United States Dep't of Justice v Reporters Committee for Freedom of Press*, 489 U.S. 749, 103 L.Ed.2d. 774, 109 S.Ct. 1468 (1989), infra § 53; *United States Dep't of Defense v Federal Labor Relations Auth.*, 510 U.S. 487, 127 L.Ed.2d 325, 114 S.Ct. 1006 (1994), infra § 46.

In light of: (1) the lack of value that raw penalty and violation data provides to the public and (2) the comments filed by requestors in this docket, GSOC and GTC would recommend that the Commission reconsider the White Paper proposal and give due consideration to alternate methods of achieving transparency such as the GSOC's and GTC's proposal, which is described in subsection D below.

C. The Proposed CIP NOP Format Reduces Its Overall Security Benefit By Limiting The Provision Of Information To Registered Entities.

The White Paper proposal eliminates the availability of information regarding CIP violations, which information is used by registered entities for educational and self-assessment purposes. Ensuring that impacted stakeholders are apprised of critical information when needed was an essential element of the FAST Act and a power and directive explicitly granted to the Commission in the FAST Act. The Commission's practices regarding information-sharing were codified at 18 CFR 388.113(f).

Currently, registered entities are able to access the redacted CIP filings, *i.e.*, NOPs, spreadsheet NOPs, Find, Fix and Track ("FFT") filings, and Compliance Exception ("CE") filings, which provide valuable information about issues that have been experienced, effective mitigation options, and best security practices. Registered entities rely on these publicly available CIP-related filings to perform internal self-assessments of compliance, to identify and internalize lessons learned, to identify areas for improvement and best practices, etc.

The timely, informative perspectives and information contained within these redacted CIP-related filings benefit the security of the entire industry by acting as a "lessons learned" and/or "security guidance/best practices." Adoption of the White Paper proposal would completely eliminate this source of information, resulting in less information sharing and maturity in CIP programs protecting the BPS. The inability to access such information could result in an overall

reduction in BPS security as registered entities would have reduced information and little or no ability to timely learn from each other about cybersecurity and mitigation measures.

While GSOC and GTC appreciate that NERC commits, in the White Paper, to ensuring that lessons learned from violations are still shared with registered entities,[17] such commitment does not assuage concerns around timing and, given the historically generic nature of lessons learned efforts, the likelihood of a reduction in the actionable nature of and value of the information being shared. As the Commission contemplates the removal of redacted CIP NOP information from the public filing library, GSOC and GTC encourage the Commission to leverage its information-sharing authority and procedures set forth at 18 CFR 388.113(f) to initiate voluntary sharing of redacted CIP NOPs. This continued sharing would ensure that the critical learning and communication of important cybersecurity information is maintained.

To facilitate this, the Commission and NERC should open a dialog with registered entities about effective, secure mechanisms through which the more detailed information included in redacted NOPs could be shared. Further, given the clear security benefits, such sharing mechanisms should be identified and in process, if possible, before the Commission issues a determination regarding the revised CIP NOP format set forth in the White Paper.

D. The Commission Should Consider Aligning Its NERC Enforcement-Related Reporting Practices With Its Other Enforcement-Related Reporting Practices.

The Commission currently administers oversight and enforcement of compliance for several technically complex industries. Its oversight and enforcement of reliability standards compliance is delegated to NERC and the regional entities. The Commission's reporting practices with respect to other areas of FERC oversight and enforcement, *e.g.*, Open Access Transmission

[17] *See* White Paper at XX.

Tariff ("OATT") compliance, market manipulation, uniform system of accounting, and accounting practices generally, are well-defined and publicly posted for public review on the Commission's website.[18] Generally, the Commission makes certain, specific information related to the results of its investigations or specific issues public.[19] For example, actions that incurred a civil penalty are publicly available on the Commission's website[20] whereas lower risk or impact issues are reported in the Commission's publication of its annual Report on Enforcement,[21] which identifies and describes its enforcement-related activities in a summary format. Specifically, the annual Report on Enforcement provides summaries of illustrative self-reports and investigations that were closed with no action as well as information on other enforcement-related activities.

GSOC and GTC respectfully suggest that the Commission's current reporting practices associated with its oversight and enforcement of OATT compliance, market manipulation, uniform system of accounting, and accounting practices generally provide an appropriate template and example for achieving transparency while ensuring security. Just as the Commission closes self-reports and investigations with no further action, NERC and the regional entities resolve lower risk reliability standards violations through FFTs and CEs, both of which result in such issues being resolved outside of the enforcement process as set forth in the NERC Rules of Procedure at Section 3A of Appendix 4C.

Given this similarity, the Commission should consider aligning how it reports on FFTs and CEs with how it reports on "no action" self-reports and investigations, *i.e.*, FFTs and CEs could be provided to the Commission in a summary report similar to its annual Report on Enforcement. Such alignment would ensure the security of sensitive information ***and*** provide the public with

[18] *See* https://www.ferc.gov/enforcement/enforcement.asp.
[19] *E.g.*, the Commission has posted summary reports regarding its audits of CIP reliability standards.
[20] *See* https://www.ferc.gov/enforcement/civil-penalties/civil-penalty-action.asp.
[21] *See* https://www.ferc.gov/legal/staff-reports/2018/11-15-18-enforcement.pdf.

important information in a comprehensive context that provides an *en globo* view of the Commission's "performance of its statutory duties" relative to reliability standards compliance.

The reporting of lower risk reliability standards' violation data in this fashion would be much more valuable to the general public as it would identify and describe trends and, further, it would be consistent with the Commission's reporting of its other enforcement-related activities and performance. Simply stated, comparable reporting of reliability standards enforcement would put reliability standards' violations, trends, penalty amounts, etc. in a format that facilitates public review and assessment of Commission performance without jeopardizing security, *e.g.*, administrative infractions versus technical infractions; risk; mitigation practices; etc. As a result, the public and other interested stakeholders would be positioned to receive important information in a digestible, contextual format that provides them with insight into the effectiveness and efficiency of the reliability standards' regulatory framework.

Importantly, 18 CFR 39.7(b)(5) already requires NERC and the regional entities to "file such periodic summary reports as the Commission shall from time to time direct on violations of reliability standards and summary analyses of such violations." The Commission's existing enforcement-related reporting practices support a bifurcation of the filing and reporting processes for issues closed without a full enforcement process versus those issues that require fulfillment of the full enforcement process. Aligning the Commission's reporting of FFTs/CEs with its reporting of "no action" issues related to the OATT, markets, accounting, etc. is appropriate given the similarity between the risk and impact profiles of such alleged violations and the Commission's current enforcement-related reporting practices for lower risk and impact issues generally.

Plainly stated, alignment of Commission reporting practices relative to lower risk issues greatly reduces security concerns while increasing transparency. With such a reporting mechanism

in place, the Commission could even publish a list of violator names on an annual basis without fear of jeopardizing the security of the BPS.

Because such reporting practices would greatly reduce the overall "attack surface" of available information while still facilitating Commission and public review of enforcement-related activities, the White Paper proposal would become more sustainable. However, it still may not be optimal. Accordingly, to ensure transparency and the appropriate classification of information as CEII, GSOC and GTC respectfully suggest that the Commission consider establishing a list of the CIP requirements that would not represent a security risk, *i.e.*, that are administrative in nature. Thereafter, it could treat CIP NOPs associated with those identified standards and requirements as public. Non-public treatment, as set forth in the White Paper, would then be reserved for or limited to the more technical violations that could pose a security risk to the BPS if publicly released. Such administration of CIP violations generally and CIP NOPs specifically would result in a net increase in transparency and a net decrease in administrative burden without adversely impacting grid security. An example of a standard and requirement that could be considered administrative in nature is CIP-004-6, R1.1.

IV. CONCLUSION

GSOC, GTC, and the utility industry at-large are committed to providing affordable, reliable electric service to their customers. Without reliability and security, such electric service is jeopardized. Hence, the industry has ample reason and motivation to ensure compliance, reliability, and security. The industry has demonstrated its commitment to these objectives through its embrace of self-reporting. Disclosure of entity names and penalty amounts will not further increase or incent compliance. Continued disclosure of sensitive information, however, sets a difficult precedent and complicates industry efforts to maintain reliability and security. Coupled

with the lack of value that the public would derive from raw penalty and violation data without context, there is concern that transparency will, ultimately, be prioritized above security and reliability. Enhanced transparency that works to the detriment of the BPS is not a net gain for the industry.

Transparency should be balanced against the continued, reliable operation of the BPS, particularly as incremental disclosures of CEII create additional risk that adversaries can better target their attacks. While there may be value in providing the public with additional information about CIP reliability standards compliance, all efforts should be made to ensure that this minimal value is not achieved at the expense of a reliable and secure BPS. Further, the potential decrease to security that could result from the elimination of information-sharing (as an unintended consequence of the White Paper proposal) presents an additional concern and a potential reduction in the overall benefits of the White Paper proposal.

GSOC and GTC appreciate the opportunity to provide these comments and respectfully encourages the Commission to: (1) consider aligning its reporting practices associated with reliability standards compliance enforcement with its other enforcement-related reporting practices; and (2) ensure that industry information-sharing mechanisms are established in advance of its final determination regarding its White Paper proposal. GSOC and GTC look forward to further engagement with the Commission and NERC on this important topic.

Respectfully submitted,

/s/ Christina V. Bigelow
Christina V. Bigelow
Director, Legal and Compliance
GSOC
2100 E. Exchange Place
Tucker, GA 30084
christina.bigelow@gasoc.com

October 28, 2019

Document Content(s)