July 21, 2016

Commissioner Cheryl A. LaFleur

STATEMENT

FEDERAL ENERGY REGULATORY COMMISSION

Docket No. RM15-14-002
Item No. E-8

Statement of Commissioner Cheryl A. LaFleur on Standards for Supply Chain Cyber Controls

"In today's order, the Commission elects to proceed directly to a Final Rule and require the development of a new reliability standard on supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. I fully support the Commission's continued attention to the threat of inadequate supply chain risk management procedures, which pose a very real threat to grid reliability.

"However, in my view, the importance and complexity of this issue should guide the Commission to proceed cautiously and thoughtfully in directing the development of a reliability standard to address these threats. I am concerned that the Commission has not adequately considered or vetted the Final Rule, which could hamper the development and implementation of an effective, auditable, and enforceable standard. I believe that the more prudent course of action would be to issue today's Final Rule as a Supplemental Notice of Proposed Rulemaking (Supplemental NOPR), which would provide NERC, industry, and stakeholders the opportunity to comment on the Commission's proposed directives. Accordingly, and as discussed below, I dissent from today's order.[1]

I. The Commission's Decision to Proceed Directly to Final Rule is Flawed and Could Delay Protection of the Grid Against Supply Chain Risks

"Last July, as part of its NOPR addressing revisions to its cybersecurity critical infrastructure protection (CIP) standards, the Commission raised for the first time the prospect of directing the development of a standard to address risks posed by lack of controls for supply chain management.[2] The Commission indicated that new threats might warrant directing NERC to develop a standard to address those risks. While the Commission noted a variety of considerations that might shape the standard, including, among others, jurisdictional limits and the individualized nature of companies' supply chain management procedures, the Commission notably did not propose a specific standard for comment. Instead, the Commission sought comment on (1) the general proposal to require a standard, (2) the anticipated features of, and requirements that should be included in, such a standard, and (3) a reasonable timeframe for development of a standard.[3]

"The record developed in comments responding to the Supply Chain NOPR and through the January 28, 2016 technical conference reflects a wide diversity of views regarding the need for, and possible content of, a reliability standard

[1] I do agree with one holding in the order: that the Commission has authority under section 215 of the Federal Power Act to promulgate a standard on this issue.

[2] *Revised Critical Infrastructure Protection Reliability Standards*, Notice of Proposed Rulemaking, 80 Fed. Reg. 43,354 (July 22, 2015), 152 FERC ¶ 61,054 (2015). I will refer to the section of that order addressing supply chain issues as the "Supply Chain NOPR," and the remainder of the order as the "CIP NOPR."

[3] *Id.* P 66.

addressing supply chain management. Notwithstanding these diverse views, there was broad consensus on one point: that effectively addressing cybersecurity threats in supply chain management is tremendously complicated, due to a host of jurisdictional, technical, economic, and business relationship issues. Indeed, in the Supply Chain NOPR, the Commission recognized "that developing a supply chain management standard would likely be a significant undertaking and require extensive engagement with stakeholders to define the scope, content, and timing of the standard."[4]

"Yet, the Commission is proceeding straight to a Final Rule without in my view engaging in sufficient outreach regarding, or adequately vetting, the contents of the Final Rule. As to those contents, it is worth noting that the four objectives that will define the scope and content of the standard were not identified in the Supply Chain NOPR. Therefore, even though the Final Rule reflects feedback received on the Supply Chain NOPR, and is not obviously inconsistent with the Supply Chain NOPR, no party has yet had an opportunity to comment on those objectives or consider how they could be translated into an effective and enforceable standard.[5] This is a consequence of: (1) the lack of outreach on supply chain threats prior to issuing the Supply Chain NOPR; (2) the lack of detail in the Supply Chain NOPR regarding what a standard might look like; and (3) the decision today to proceed straight to a Final Rule rather than provide additional opportunities for public feedback.

A. The Commission and the Public's Consideration of Supply Chain Risks Would Benefit from Additional Stakeholder Engagement

"First, I believe that meaningful stakeholder input on the content of any proposed rule is essential to the Commission's deliberative process. This is especially important in our reliability work, as any standard developed by NERC must be approved by stakeholder consensus before it may be filed at the Commission. I do not believe that the record developed to date establishes that the Final Rule will lead to an appropriate solution to address supply chain risks. I note that much of the feedback we received in response to the Supply Chain NOPR was not focused on the merits of particular approaches to address supply chain threats. Yet, in this order, the Commission directs the development of a standard based on objectives not reflected in the Supply Chain NOPR, depriving the public of the ability to comment, and the Commission of the benefit of that public comment.

"In retrospect, given both the preliminary nature of the consideration of the issue and the lack of a concrete idea regarding what a proposed standard would look like, I believe that the Supply Chain NOPR was, in substance, a *de facto* Notice of Inquiry and should have been issued as such, rather than as a subsection of the broader CIP NOPR on changes to the CIP standards. For example, it is instructive to compare the Supply Chain NOPR with two other documents: (1) the Notice of Inquiry being issued today on cybersecurity issues arising from the recent incident in Ukraine,[6] and (2) the NOPR concerning the proposed development of a reliability standard to address geomagnetic disturbances.[7] The level of detail and consideration of the issues presented in the Supply Chain NOPR are much more consistent with that in a Notice of Inquiry than a traditional NOPR. As a result, I am concerned that the Commission, by styling its prior action as a NOPR, has skipped a critical step in the rulemaking process: the opportunity for public comment on its directive to develop a standard and the objectives that will frame the design and development of that standard. As explained below, I believe this procedural decision actually makes it less likely that an effective, auditable, and

[4] *Id.*

[5] To be clear, I am less concerned about whether the Final Rule satisfies minimal notice requirements than whether the Final Rule represents reasoned decision making by the Commission.

[6] *Cyber Systems in Control Centers*, Notice of Inquiry, Docket No. RM16-18-000.

[7] *Reliability Standards for Geomagnetic Disturbances*, Notice of Proposed Rulemaking, 77 FR 64,935 (Oct. 24, 2012), 141 FERC 61,045 (2012).

enforceable standard will be implemented on a reasonable schedule, particularly given the acknowledged complexity of this issue.[8]

B. The Lack of Adequate Stakeholder Engagement Will Have Negative Consequences for the Standards Development Process

"I am also concerned about the consequences for the standards development process of the Commission's decision to proceed straight to a Final Rule. In particular, I am concerned that the combination of insufficient process and discussion to develop the record and inadequate time for standards development (since the Commission substantially truncated NERC's suggested timeline)[9] will handicap NERC's ability to develop an effective and enforceable proposed standard for the Commission to consider. As noted above, NERC, industry, and other stakeholders will have no meaningful opportunity before initiating their work to provide feedback on the contents of the rule, to seek clarification from the Commission, or to propose revisions to the rule. Yet, this type of feedback is a critical component of the rulemaking process, to ensure that the entities tasked with implementing the Commission's directive have been heard and understand what they are supposed to do. I believe that the Commission is essentially giving the standards development team a homework assignment without adequately explaining what it expects them to hand in.

"I do not believe that the Final Rule's flexibility is a justification for proceeding straight to a Final Rule. Indeed, given the inadequate process to date, I fear that the flexibility is in fact a lack of guidance and will therefore be a double-edged sword. The Commission is issuing a general directive in the Final Rule, in the hope that the standards team will do what the Commission clearly could not do: translate general supply chain concerns into a clear, auditable, and enforceable standard within the framework of section 215 of the Federal Power Act. While the Commission need not be prescriptive in its standards directives, the Commission's order assumes that the standards development team will be able to take the "objectives" of the Final Rule and translate them into a standard that the Commission will ultimately find acceptable. I believe that issuing a Supplemental NOPR would benefit the standards development process by enabling additional discussion and feedback regarding the design of a workable standard.

---

[8] I believe that *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166 (2014) (Physical Security Directive Order), which is cited in the Final Rule as support for today's action, is primarily relevant to demonstrate a different point than the order indicates. The Physical Security Directive Order followed focused outreach with NERC and other stakeholders to discuss how a physical security standard could be designed and implemented within the parameters of section 215 of the Federal Power Act. As a result of that outreach, the directives in the Physical Security Directive Order were clear, targeted, and reflected shared priorities between the Commission and NERC. Physical Security Directive Order, 146 FERC ¶ 61,166 at PP 6-9. Consequently, NERC was able to develop and file a physical security standard with the Commission in less than three months, and the Commission ultimately approved that standard in November 2014, only roughly eight months after directing its development. *Physical Security Reliability Standard*, 149 FERC ¶ 61,140 (2014). In my view, this example demonstrates how essential outreach is to the timely and effective development of NERC standards.

[9] In its comments responding to the Supply Chain NOPR, NERC requested that, if the Commission decides to direct the development of a standard, the Commission provide *a minimum* of two years for the standards development process. However, the Commission disregards that request and directs NERC to develop a standard in just one year, apparently based solely on the Trade Associations' request that the Commission allow *at least* one year for the standards development process. I believe this timeline is inconsistent with the Commission's own recognition of the complexity of this issue, and, as discussed herein, likely to delay rather than expedite the implementation of an effective, auditable, and enforceable standard.

C. By Failing to Engage in Adequate Stakeholder Outreach Before Directing Development of a Standard, the Commission Increases the Likelihood that Implementation of a Standard Will be Delayed

A compressed and possibly compromised standards development process also has real consequences for the Commission's consideration of that proposed standard, whenever it is filed for our review. Unlike our authority under section 206 of the FPA, the Commission lacks authority under section 215 to directly modify a flawed reliability standard. Instead, to correct any flaws, the statute requires that we remand the standard to NERC and the standards development process.[10] Thus, notwithstanding the majority's desire to quickly proceed to Final Rule, the statutory construct constrains our ability to timely address a flawed standard, which could actually delay implementation of the protections the Commission seeks to put in place.

"Given the realities of the standards development and approval process, we are likely years away from a supply chain standard being implemented, even under the aggressive schedule contemplated in the order. I believe that the Commission should endeavor to provide as much advance guidance as possible before mandating the development of a standard, to increase the likelihood that NERC develops a standard that will be satisfactory to the Commission and reduce the need for a remand. I worry that the limited process that preceded the Final Rule and the expedited timetable will make it extremely difficult for NERC to file a standard that the Commission can cleanly approve. Had the Commission committed itself to conducting adequate outreach, I believe we could have mitigated the likelihood of that outcome, and more effectively and promptly addressed the supply chain threat in the long term. "Delaying" action for a few months thus would, in the long run, lead to prompter and stronger protection for the grid.

II. Conclusion

"The choice the Commission faces today on supply chain risk management is not between action and inaction. Rather, given the importance of this issue, I believe that more considered action and a more developed Commission order, even if delayed by a few months, is better than a quick decision to "do something." Ultimately, an effective, auditable, and enforceable standard on supply chain management will require thoughtful consideration of the complex challenges of addressing cybersecurity threats posed through the supply chain within the structure of the FERC/NERC reliability process. In my view, the Commission gains very little and does not meaningfully advance the security of the grid by proceeding straight to a Final Rule, rather than taking the time to build a record to support a workable standard.

"Accordingly, I respectfully dissent."

[10] 18 U.S.C. § 824o(d)(4).