UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Revised Critical Infrastructure Protection Reliability Standards	))	Docket No. RM15-14-000

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC") hereby provides comments on the Federal Energy Regulatory Commission's ("FERC" or the "Commission") Notice of Proposed Rulemaking ("NOPR") proposing to approve revisions to the Critical Infrastructure Protection ("CIP") Reliability Standards.[1] As the Commission stated in the NOPR, the proposed CIP Reliability Standards are just and reasonable, address the directives in Order No. 791,[2] and "improve the base-line cybersecurity posture of applicable entities compared to the current Commission-approved CIP Reliability Standards."[3]

As discussed below, NERC supports the Commission's proposal to approve the proposed Reliability Standards. NERC also provides responses to the issues the Commission discussed in the NOPR related to: (1) supply chain management; (2) inter-Control Center communications; (3) remote access protections; (4) protections for transient devices used at low impact BES Cyber

[1] *Revised Critical Infrastructure Protection Reliability Standards*, 152 FERC ¶ 61,054 (2015). NERC requested approval of the following seven Reliability Standards: (1) CIP-003-6 (Cyber Security – Security Management Controls); (2) CIP-004-6 (Cyber Security – Personnel and Training); (3) CIP-006-6 (Cyber Security – Physical Security of BES Cyber Systems); (4) CIP-007-6 (Cyber Security – Systems Security Management); (5) CIP-009-6 (Cyber Security – Recovery Plans for BES Cyber Systems); (6) CIP-010-2 (Cyber Security – Configuration Change Management and Vulnerability Assessments); and (7) CIP-011-2 (Cyber Security – Information Protection).

[2] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,755 (Dec 3, 2013), 145 FERC ¶ 61,160 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61, 188 (2014).

[3] NOPR at P 2.

Systems; and (5) the definition of Low Impact External Routable Connectivity ("LERC').[4] As discussed further below, NERC offers the following comments:

Supply Chain Management – NERC supports the Commission's attention to this issue and agrees that it is vital to the reliability and security of the Bulk Electric System ("BES") that electricity subsector participants continue focusing on mitigating security risks associated with the supply chain. Supply chain management is a complex global issue, however, and there are significant challenges to developing a mandatory Reliability Standard on supply chain management consistent with Section 215 of the Federal Power Act ("FPA"). If the Commission directs NERC to develop a new or modified Reliability Standard, NERC respectfully requests that the Commission provide two years for standard development to allow sufficient time for NERC to consider these issues and engage in educational and outreach efforts, such as holding technical conferences and establishing a task force, to provide a better understanding of the nature of supply chain risks and the extent to and manner in which a mandatory Reliability Standard can effectively protect against those risks. Among other matters, NERC should examine entities' existing practices for mitigating supply chain risks, how to account for those practices in a standard, and how to leverage existing supply chain management and procurement guidelines.

Inter-Control Center Communications – NERC agrees with the Commission that inter-Control Center communications play a critical role in maintaining BES reliability. NERC does not oppose further evaluation, through its standard development process, of additional cybersecurity protections for inter-Control Center communications, provided that those additional

[4] Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* ("NERC Glossary"), *available at* http://www.nerc.com/files/Glossary_of_Terms.pdf.

protections would not otherwise have an adverse effect on reliability (e.g., due to latency) and account for the various risk levels of BES Control Centers.

Remote Access Protections – The Commission-approved CIP Reliability Standards require responsible entities to implement a number of fundamental security controls for remote access. NERC respectfully submits that the Commission allow responsible entities time to implement these controls before requiring any additional protections. As with all of its standards, NERC will evaluate whether additional protections are needed as it reviews the manner in which entities implement the required controls and the effectiveness of those controls.

Transient Devices at Low Impact BES Cyber Systems – An underlying principle of the Commission-approved CIP Reliability Standards is to protect BES Cyber Systems commensurate to the risks they present to the reliability of the BES. The goal is to focus entities on protecting those BES Cyber Systems with heightened risks to the BES. Mandating that entities protect all transient devices used at low impact BES Cyber Systems may undermine that objective. Entities would have to devote a substantial amount of resources documenting the protections afforded each transient device used at low impact BES Cyber Systems, which may limit their focus on protecting higher risk BES Cyber Systems. Any potential directive to modify the CIP Reliability Standards to address this issue should be cognizant of the varying risk levels presented by low impact BES Cyber Systems and the need to focus on higher risk issues.

Definition of LERC - The definition of LERC establishes when entities are required to apply electronic access controls to their assets containing low impact BES Cyber Systems. As explained in the Technical Guideline and Basis section of proposed Reliability Standard CIP-003-6, the definition covers situations where a user or device could directly access a low impact BES Cyber Asset from outside the asset containing the low impact BES Cyber System absent a security

break (e.g., without having to go through a firewall or another Cyber Asset). Should comments to the NOPR indicate that there is confusion as to the meaning and application of LERC, NERC will take the necessary steps, such as issuing additional guidance or modifying the definition, to ensure entities can effectively and efficiently implement the proposed Reliability Standards.

I. BACKGROUND

On February 13, 2015, NERC filed the proposed CIP Reliability Standards for Commission approval in response to Order No. 791.[5] In Order No. 791, the Commission approved new and modified CIP cybersecurity Reliability Standards, referred to as the CIP version 5 Standards, and directed modifications to those standards. As discussed in the Petition, the proposed Reliability Standards include the following improvements to the CIP version 5 Standards:

- Removing the "identify, assess, and correct" language from the CIP Reliability Standards in favor of applying NERC's risk-based approach to Compliance Monitoring and Enforcement Program developed through the Reliability Assurance Initiative.[6]

- Requiring responsible entities to implement cybersecurity controls for assets containing low impact BES Cyber Systems to meet specific security objectives related to: (i) cybersecurity awareness; (ii) physical security controls; (iii) electronic access controls; and (iv) Cyber Security Incident response.[7]

- Requiring entities to implement controls to protect transient devices (e.g., thumb drives and laptop computers) connected to their high impact and medium impact BES Cyber Systems and associated PCAs.[8]

- Requiring entities to implement security controls for nonprogrammable components of communication networks at Control Centers with high or medium impact BES Cyber Systems.[9]

---

5 *Petition of the North American Electric Reliability Corporation for Approval of Proposed Critical Infrastructure Protection Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2*, Docket No. RM15-14-000 (Feb. 13, 2015) ("Petition").

6 Petition at 14-21.

7 *Id*. at 21-32.

8 *Id*. at 32-46.

9 *Id*. at 46-53.

On July 16, 2015, the Commission issued the NOPR, proposing to approve the proposed Reliability Standards and finding that they are just and reasonable, improve upon the current Commission-approved CIP Reliability Standards, and address the directives in Order No. 791.[10] The Commission also requested comment on the following issues:

1) *Supply Chain Management*: The Commission proposes to direct NERC to develop a new or modified Reliability Standard to address security risks from the supply chain for industrial control system hardware and software, and computing and networking services associated with BES operations.[11]

2) *Inter-Control Center Communications:* The Commission proposes to direct NERC to modify the CIP Reliability Standards to require protections for communication network components and data communicated between all Control Centers.[12]

3) *Remote Access Protections*: The Commission is seeking comments on the adequacy of the security controls incorporated into the CIP Reliability Standards for remote access used in relation to BES communications.

4) *Transient Devices Used at Low Impact BES Cyber Systems*: The Commission is seeking additional information on the need for including protections for transient devices used at low impact BES Cyber Systems.

5) *Definition of Low Impact External Routable Connectivity*: The Commission seeks comment on the clarity of the proposed NERC Glossary definition for LERC.

II. COMMENTS

NERC supports the Commission's proposal to approve the proposed Reliability Standards. As the Commission recognizes, the proposed Reliability Standards will bolster NERC's and the industry's ongoing efforts to provide for a reliable and secure Bulk Power System ("BPS"). NERC provides the following comments on the issues raised by the Commission in the NOPR.

---

10 NOPR at P 2.

11 *Id*. at PP 61-66.

12 *Id*. at PP 53-59.

a. Supply Chain Management

i. NOPR

The Commission proposes to expand the scope of the CIP Reliability Standards by directing NERC to "develop a new or modified Reliability Standard to provide security controls for supply chain management for industrial control system hardware and software, and computing and networking services associated with [BES] operations."[13] Citing recent malware campaigns targeting supply chain vendors, the Commission asserted that the global supply chain presents risks to the reliability and security of the BES that the Commission-approved CIP Reliability Standards do not entirely address.[14] The Commission cited to the National Institute of Standards and Technology ("NIST") Special Publication 800-161 ("SP 800-161") and the Department of Energy's ("DOE") *Cybersecurity Procurement Language for Energy Delivery Systems* (the "DOE Guidelines") as examples of guidelines that include security controls to address risks associated with the supply chain.[15]

The Commission stated that the reliability goal of any new or modified Reliability Standard addressing supply chain management "should be to create a forward-looking, objective-driven standard that encompasses activities in the system development life cycle: from research and development, design and manufacturing stages (where applicable), to acquisition, delivery, integration, operations, retirement, and eventual disposal of the Registered Entity's information and communications technology and industrial control system supply chain equipment and services."[16] The Commission also stated, because "security controls for supply chain management

[13] NOPR at P 64.

[14] *Id*. at PP 61-63.

[15] *Id*. at P 62.

[16] *Id*. at P 64.

will likely vary greatly with each responsible entity due to variations in individual business practices, the right set of supply chain management security controls should accommodate for, among other things, an entity's: (1) procurement process; (2) vendor relations; (3) system requirements; (4) information technology implementation; and (5) privileged commercial or financial information."[17]

The Commission also clarified that "due to the broadness of the topic and the individualized nature of many aspects of supply chain management," any Reliability Standard addressing supply chain management security should be consistent with the following:

- Apply only to those entities subject to the jurisdiction of Section 215 of the FPA (i.e., owners, operators and users of the BPS) and "not directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities;"
- Be a forward-looking standard and not require abrogation or renegotiation of contracts.
- Set goals about what to do while allowing flexibility for how an entity achieves those goals.
- Allow for exceptions given the diversity of products involved and acquisition processes.
- Be specific enough so that compliance obligations are clear and enforceable (i.e., identify specific controls instead of simply requiring a registered entity to have a plan).[18]

FERC is seeking comment on: (1) the general proposal to direct NERC to address supply chain management through a mandatory Reliability Standard, (2) a reasonable timeframe for standard development, (3) and anticipated features of, and requirements that should be included in the standard.[19] The following section discusses each of these issues.

---

17 NOPR at P 65.

18 *Id*. at P 66.

19 *Id*. at P 66.

ii. Comments

1. *NERC Supports Continued Focus on Supply Chain Management Security*

NERC supports the Commission's attention to supply change management and agrees that it is vital to the security of the BPS that electricity subsector participants continue their focus on mitigating supply chain security risks. Cybersecurity threats pose a serious and ongoing challenge for the electricity subsector. The security and reliability of the BPS is fundamental to national security, economic development, and public health and safety. A major disruption in electric service due to a cybersecurity incident could have far-reaching effects. As the Commission discusses in the NOPR, the supply chains for information and communications technology and industrial control systems present significant risks to BPS security, providing various opportunities for adversaries to initiate cyberattacks.[20] NERC thus recognizes that a multitude of steps should be taken throughout the life cycle of systems associated with BES operations to protect them from cybersecurity threats. NERC is committed to using its many reliability tools – e.g., guidelines, training exercises, alerts, situational awareness, and, if necessary, mandatory Reliability Standards – to support industry's efforts to mitigate supply chain risks.

As discussed below, if the Commission directs the development of a supply chain management Reliability Standard, it should: (1) provide a minimum of two years for standard development activities; and (2) clarify that any such Reliability Standard build on existing protections in the CIP Reliability Standards and the practices of registered entities, and focus primarily on those procedural controls that registered entities can reasonably be expected to implement during the procurement of products and services associated with BES operations to manage supply chain risks. Further, the Commission should also stress that the supply chain

[20] NOPR at PP 62-63.

management Reliability Standard must be flexible to account for: (i) the differences in the needs and characteristics of registered entities; (ii) the diversity of BES system environments, technologies, and risks; and (iii) issues related to the limited applicability of mandatory NERC Reliability Standards.

2. *The Commission Should Provide Two Years for Development of Any Supply Chain Management Reliability Standard to Allow NERC Sufficient Time to Engage in Educational and Outreach Efforts*

If the Commission directs NERC to develop a new or modified Reliability Standard to address supply chain issues, NERC respectfully requests that the Commission provide a minimum of two years for standard development to allow sufficient time for NERC to engage in educational and outreach efforts, as discussed below. Given the complexity of supply chain issues and the limitations of Section 215 of the FPA, NERC and its stakeholders will need significant time to analyze the nature of supply chain risks and the extent to and manner in which a mandatory Reliability Standard under Section 215 of the FPA can protect against those risks. As the Commission acknowledged, "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."[21]

The following is an overview of some of the significant challenges that NERC, working with its stakeholders, should address during the development of a supply chain management Reliability Standard:

Identifying Supply Chain Risks. As the Commission recognizes, supply chains for information and communications technology and industrial control systems are long and

[21] NOPR at P 66.

multidimensional, involving numerous parties in a multitude of countries across the globe.[22] Registered entities typically rely on a number of vendors and contractors that may use multiple third-party suppliers for components used in their products or technologies. As such, multiple entities across the globe may participate in the development, design, manufacturing, and delivery of a single product purchased by a registered entity. Supply chains risks are thus complex, multidimensional, and constantly evolving, and may include, as the Commission states, insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices. Further, as provided in NIST 800-161:

> These risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. Threats and vulnerabilities created by malicious actors (individuals, organizations, or nation states) are often especially sophisticated and difficult to detect, and thus provide a significant risk to organizations.

Supply chain management is thus a global issue that presents significant challenges across all industries. As the Commission recognizes, however, a Reliability Standard under Section 215 of the FPA has limited applicability. It cannot "directly impose obligations on suppliers, vendors or other entities that provide products or services to registered entities."[23] As such, a NERC Reliability Standard should not be expected to mitigate all risks inherent to the global supply chain.[24] Any supply chain management Reliability Standard must therefore be reasonably scoped, focusing on the measures entities can take to manage supply chain risks without holding them responsible for actions of others that are beyond their control. NERC should better understand

---

[22] As the Commission states, supply chains "are complex, globally distributed and interconnected systems that have geographically diverse routes and consist of multiple tiers of outsourcing." NOPR at P 61.

[23] NOPR at P 66.

[24] NIST SP 800-161 recognizes "it is impossible to completely eliminate all risks." NIST 800-161 at p. 2.

global supply chain risks and how to protect against those risks within the limitations of Section 215.

Identifying Effective Supply Chain Management Security Controls. Given the limited applicability of FPA Section 215, the primary mechanism in a Reliability Standard for protecting the BES from supply chain risks is through registered entity procurement practices. Further, as the Commission clarified, any proposed Reliability Standard should identify specific controls, stating that a "reliability standard that simply requires entities to 'have a plan' addressing supply chain management would not suffice."[25] NERC will thus need to analyze the types of procurement practices registered entities can implement that meaningfully reduce supply chain risks without imposing undue burden. To that end, NERC should review what entities are currently doing to mitigate supply chain risks, understand how to account for those activities in a mandatory standard, and examine how to leverage existing supply chain management and procurement guidelines.

For instance, NERC, working with its stakeholders, should review the security controls included in NIST SP 800-161 and the DOE Guidelines to determine what can be adapted to use in a mandatory Reliability Standard. Similarly, NERC understands that the Edison Electric Institute ("EEI") has developed a set of key principles and recommendations for entities to consider for managing supply chain cybersecurity risks. NERC should review the EEI principles and guidelines, as well as examine the practices entities are currently implementing, to get a better perspective on the appropriate framework for a mandatory standard and the types of controls that could be included in a supply chain management Reliability Standard.

Negotiating Leverage and Cost Issues. Any supply chain management Reliability Standard must balance the reliability need to implement supply chain management security controls with

[25] NOPR at P 66.

entities' business need to obtain products and services at a reasonable cost. Stakeholders have expressed concern that they may not have the bargaining power to persuade vendors/suppliers to implement certain cybersecurity controls to mitigate supply chain risks without significantly increasing the costs of their products and services. As stated in NIST SP 800-161, "implementing supply change management security controls will require financial and human resources, not just from the [acquirer] directly but also potentially from their systems integrators, suppliers, and external service providers that would also result in increased costs to the acquirer."[26] Further, if the Reliability Standard overly restricts the vendors/suppliers with which registered entities may contract, those vendors/suppliers may take advantage of those restrictions to increase their costs. Registered entities should not be faced with the prospect of violating a NERC Reliability Standard or entering into an unfavorable contract.

Differences in Registered Entities. One of the many challenges will be drafting a generally applicable Reliability Standard for registered entities with significant differences in purchasing power, resources needs, and types of equipment. As the Commission acknowledged, a one-size-fits-all approach to supply chain management will not work.[27] NERC, working with stakeholders, will need to develop requirements flexible enough to account for the differences in the needs and characteristics of registered entities.

Diversity of BES Facilities, Technologies, and Risks. BES system environments, technologies, and risks vary. As the Commission recognized in Order No. 791,[28] the CIP cybersecurity Reliability Standards are designed to protect BES Cyber Systems commensurate to the risks they present to the reliability of the BES. NERC will need to understand how to draft a

---

[26] *See* NIST SP 800-161 at 3.

[27] NOPR at P 65.

[28] *See* Order No. 791 at P 87.

generally applicable supply chain management Reliability Standard that accounts for different types of products and the various environment in which those products will be integrated or applied (i.e., whether the BES Cyber System would have a high, medium, or low impact rating) so that the required protections are properly tailored to the relevant cybersecurity programs and policies of that environment. Consistent with the design of the CIP version 5 Standards, NERC should consider the need to prioritize the application of supply chain management security controls to those systems that present heightened risk to the BES, such as SCADA systems, EMS, and other products integrated into environments that operationally control BES equipment.

Liability for Actions beyond a Registered Entities Control. As noted above, registered entities will not be able to mitigate all risks present in the global supply chain. It is certainly possible that despite a registered entity's best attempts to mitigate supply chain risks, they still purchase a comprised system, for instance. NERC should understand how to draft a Reliability Standard that creates affirmative obligations to implement supply chain management security controls without holding entities strictly liable for any failure of those controls to eliminate all supply chain threats and vulnerabilities.

Disincentives to Upgrade BES Systems and Technology. NERC is concerned that a mandatory supply chain management Reliability Standard could, if not reasonably scoped, create a disincentive for entities to upgrade their technology and control systems. Specifically, entities may be less inclined to purchase and install new technologies and equipment to avoid the regulatory risks and increased costs of complying with the mandatory Reliability Standard. NERC will need to examine ways to draft a supply chain management standard without inhibiting innovation and upgrades across the electricity subsector.

Considering the complexity of these issues, there is a need for significant education and outreach before meaningful standard development can begin. Addressing the entire supply chain life cycle in the manner proposed in the NOPR will require NERC to leverage the expertise of business units and individuals from registered entities, Regional Entities and other organizations (e.g., suppliers of BES systems) not typically involved in NERC matters (e.g., procurement experts). A two-year timeframe will provide NERC the opportunity to identify and take advantage of that expertise to scope the issues, understand existing practices, and frame potential solutions (both solutions within the mandatory Reliability Standards and outside of mandatory Reliability Standards).

More specifically, a two-year timeframe will provide NERC the ability, prior to initiating formal standards development, to: (1) organize technical conferences to educate NERC staff and stakeholders on these issues and obtain stakeholder input on the scope and content of any Reliability Standard; and (2) establish a task force, similar to the Geomagnetic Disturbance Task Force, to provide recommendations on the issues discussed above, amongst others. The task force would consist of both cybersecurity and procurement experts and include representatives from NERC, Regional Entities, and Commission staff, as the Commission deems appropriate. The conclusions of the task force could form the basis upon which a standard drafting team develops a standard for Commission approval. Such a two-step process (i.e., education and outreach followed by formal standard development) would create efficiencies and help ensure that NERC properly scopes any resulting standard based on the input from the appropriate subject matter experts.

3. Features of a Supply Chain Management Standard

For the reasons set forth above, NERC will need to engage in significant education efforts before it can outline the precise requirements that should be included in a supply chain management Reliability Standard. Nevertheless, a review of the issues raised above indicates that

any supply chain management Reliability Standard should build upon existing protections in the CIP Reliability Standards and entities' current practices, and focus primarily on those procedural controls that registered entities can reasonably implement during the procurement of products and services associated with BES operations to mitigate supply chain risks effectively. The supply chain management Reliability Standard must also be sufficiently flexible to account for: (i) the differences in the needs and characteristics of registered entities; (ii) the diversity of BES system environments, technologies, and risks; and (iii) issues related to the limited applicability of mandatory NERC Reliability Standards.

Importantly, while the CIP Reliability Standards do not explicitly address supply chain management procurement practices,[29] the CIP Reliability Standards currently include requirements that help mitigate supply chain risks. Among others, the CIP Reliability Standards include the following requirements, many of which include controls that correspond to controls in NIST SP 800-161:

- CIP-004-6, Requirement R1 requires responsible entities to implement cybersecurity awareness programs. The programs may include the reinforcement of cybersecurity practices to mitigate supply chain risks.

- CIP-004-6, Requirement R3 requires entities to implement a personnel risk assessment to attain and retain authorized electronic access and authorized unescorted physical access to BES Cyber Systems. The personnel risk assessment applies to any outside vendors or contractors seeking to attain and retain such access.

- CIP-004-6, Requirements R4 and R5 require entities to implement access (physical and electronic) management and access revocation programs. These programs must include outside vendors and contractors.

- CIP-005-5 and CIP-006-6 require entities to implement protections to control electronic and physical access to BES Cyber Systems, including access by outside vendors and contractors.

[29] NERC understands, however, that registered entities already embed cybersecurity protections in their procurement practices to varying degrees.

- CIP-007-6, Requirement R2 requires entities to implement a patch management process for tracking, evaluating, and installing cybersecurity patches. Applying patches on a timely basis may help mitigate risks associated with cybersecurity vulnerabilities created during the design and manufacturing stages of the supply chain.

- CIP-007-6, Requirement R3 requires entities to implement processes to deploy, detect, prevent, and mitigate the threat of malicious code. These processes may help entities detect and address malicious code inserted into a product prior to acquisition by the entity.

- CIP-007-6, Requirement R5 requires entities to implement processes for system access control. These processes would apply to any outside vendors or contractors granted access to protected devices.

- CIP-008-5 requires entities to implement a Cyber Security Incident response plans. These plans may help identify if a BES Cyber Security Incident relates to a supply chain issue and reduce the impact of any incident caused by a supply chain issue.

- CIP-009-6 requires entities to implement plans to recover the reliability functions performed by BES Cyber Systems in the event of a cybersecurity incident. These recovery plans will help reduce the impact of any incident caused by a supply chain issue.

- CIP-010-2, Requirement R3 requires entities to perform vulnerability assessments at least once every 15 calendar months. The vulnerability assessments may help identify any vulnerabilities resulting from supply chain issues.

- CIP-010-2, Requirement R3, Part 3.3 requires that entities perform, for all high impact BES Cyber Systems and their associated Electronic Access Control and Monitoring Systems and Protected Cyber Assets, an active vulnerability assessment *prior to* adding a new applicable Cyber Asset to a production environment. This assessment will help mitigate supply chain risks to the most critical assets prior to commissioning.

- CIP-010-2, Requirement R4 requires entities to implement a plan to address risks associated with transient devices. These plans must include protections for transient devices managed by vendors and contractors.

- CIP-011-2, Requirement R2 requires entities to implement processes for protecting critical information (i.e., BES Cyber System Information) prior to the reuse or disposal of Cyber Assets.

Any supply chain management reliability standard should build upon these existing requirements. As recognized by the Commission, NIST SP 800-161 and the DOE Guidelines establish instructional reference points for NERC and its stakeholders to leverage in evaluating the appropriate framework for and security controls to include in any mandatory supply chain

management Reliability Standard. Similarly, industry practices and guidelines, such as the EEI principles and recommendations referenced above, should also inform the development of any Reliability Standard. Collectively, these documents indicate that to manage supply chain cybersecurity risks, entities need to focus on the following areas, among others: (1) the cybersecurity functionality of acquired products; (2) the security practices of vendors, contractors and other parties throughout the supply chain; (3) the procurement practices of registered entities; and (4) the installation, maintenance, and retirement/disposal of Cyber Assets.

As noted above, given the limited scope of FPA Section 215, the primary mechanism by which registered entities can affect product design and the practices of suppliers, vendors, and contractors that provide products and services to registered entities is by contract. The Commission should thus clarify that the focus of any supply chain management Reliability Standard should be a set of requirements outlining those procedural controls that entities should take, as purchasers of products and services, to design more secure products and modify the security practices of suppliers, vendors, and other parties throughout the supply chain. The reliability objective of the procedural controls should be to require entities to take certain measures during procurement activities to help ensure that, to the extent possible, cybersecurity practices are embedded in the supply chain.

For example, the supply chain management Reliability Standard could include procedural controls surrounding the need to (1) transact with organizations that meet certain criteria (i.e., only transact with "trusted" suppliers), (2) include cybersecurity procurement language in contracts with suppliers, vendors and contractors for products and services, and (3) review and validate the security practices of suppliers, vendors and contractors, to the extent possible. A potential approach could be to require registered entities to obtain a certification from a supplier that an

independent third party reviewed and endorsed the supplier's supply chain management practices.[30] During its educational and outreach opportunities, NERC would evaluate this approach, amongst others, to determine whether it is reasonable, should be the primary mechanism to manage supply chain risks, or whether it is one of several alternatives that could be used under any supply chain management Reliability Standard.

Any supply chain management Reliability Standard, however, needs to provide flexibility and cannot impose strict liability on registered entities for any compromise of a BES system due to vulnerabilities in the supply chain. As discussed above, a NERC Reliability Standard cannot be expected to mitigate all of the risks presented by the global supply chain. Many of the threats lurking in the supply chain are simply beyond the reach of end users to mitigate. For instance, a registered entity may not be in privity of contract with and lack visibility into the practices of an entity used to design or manufacture a component of a product acquired from a different entity. It would be unreasonable, therefore, to hold registered entities strictly liable for any compromise of a BES system due to vulnerabilities in the supply chain. As such, consistent with FPA Section 215, a supply chain management Reliability Standard needs to focus on those actions within the control of the registered entity that could help mitigate supply chain risks throughout the system development life cycle. A failure to take certain steps, not the purchase of a compromised product, for instance, should be the basis on which an entity violates a supply chain management Reliability Standard.

Further, a reasonably scoped supply chain management Reliability Standard would also need to outline those instances when it is acceptable for an entity not to apply certain controls, whether to meet safety requirements or to acquire a product at a reasonable cost. The supply chain

[30] Similar to a third-party certification under the Sarbanes-Oxley Act.

management standard cannot completely ignore the varying business needs of registered entities and varying risks levels. As the Commission recognized, "[g]iven the specialty products involved and diversity of acquisition processes, the standard may need to allow exceptions."[31]

b. Protections for Inter-Control Center Communications

i. NOPR

The Commission proposes to direct NERC to expand the CIP Reliability Standards "to require responsible entities to implement controls to protect, at a minimum, all communication links and sensitive bulk electric system data communicated between all bulk electric system Control Centers."[32] In short, the Commission notes that while proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10 extends protections to nonprogrammable components of communication networks within a Control Center with high or medium impact BES Cyber Systems, it would not necessarily extend protections to communications between different Control Centers.[33] The Commission stated that because "inter-Control Center communications play a vital role in maintaining [BES] reliability…the communication links and data used to control and monitor the bulk electric system should receive protection under the CIP Reliability Standards."[34]

In proposing to direct NERC to include protections for inter-Control Center communications, the Commission acknowledged that many of those links consist of facilities

---

[31] NOPR at P 66. The DOE Guidelines also recognize that, for a variety of reasons, the recommended cybersecurity procurement language may not be attainable or desirable in every instance. In the context of a voluntary guidance document, it is up to the entity to determine it's "must haves" and those provisions subject to negotiation. As noted above, the challenge for NERC will be drafting a mandatory standard that allows for flexibility while also ensuring that entities implement certain essential supply chain management security controls.

[32] NOPR at PP 53-59.

[33] *Id*. at 55-56. Specifically, proposed CIP-006-6, Requirement R1, Part 1.10 requires entities to implement physical and/or logical protections to secure non-programmable communication network components at certain Control Centers within an Electronic Security Perimeter ("ESP") in those instances where the communication network components are not also within a Physical Security Perimeter. The Commission noted that because communication networks between different control centers are most often not within the same ESP, the protections required by proposed CIP-006-6 would not necessarily cover communications between different Control Controls.

[34] NOPR at P 57.

owned by telecommunications companies (i.e., third party communication infrastructure).[35] As such, the Commission clarified that, consistent with the proposed Reliability Standard CIP-006-6, Requirement R1, Part 1.10, a combination of physical and logical protections may be required.[36] The Commission seeks comment on the types of logical controls that entities could implement if there are latency concerns with the use of encryption.[37] Additionally, the Commission clarified that the proposed directive would only apply to inter-Control Center communications (i.e., communication between two (or more) Control Centers), but not between a Control Center and non-Control Center facilities such as substations.[38]

ii. Comments

NERC agrees that inter-Control Center communications play a critical role in maintaining BES reliability. Timely and accurate communication between Control Centers is important for maintaining situational awareness and the reliable operation of the BES. The ability to intercept and manipulate data communicated between Control Centers could be used to carry out successful cyberattacks against the BES. Accordingly, NERC does not oppose further evaluation, through its standard development process, of additional cybersecurity protections for inter-Control Center communications.

Should the Commission direct NERC to develop a new or modified Reliability Standard to address protections for inter-Control Center communications, NERC respectfully requests that the Commission consider the following:

- Any additional cybersecurity protections should not otherwise have an adverse effect on reliability. For instance, entities should avoid using encryption if latency would be

35 NOPR at P 58.

36 *Id*. at P 58.

37 *Id*. at P 59.

38 *Id*. at P 59.

introduced into the communication. The introduction of latency can cause undesired effects within real-time applications.

- The protections required for inter-Control Center communication should account for the various risk levels of BES Control Centers and the types of communications from those Control Centers. Consistent with the underlying principles of the CIP Reliability Standards, the required protections should be commensurate to the risks presented.

- Any Reliability Standard addressing inter-Control Center communication should be results-based, articulating an outcome-based objective that entities shall meet. A results-based standard will allow entities the flexibility to use current and future technology to achieve the stated objective.

c. Remote Access Protections

i. NOPR

The Commission seeks comment on the sufficiency of the security controls incorporated in the current CIP Reliability Standards regarding remote access used in relation to bulk electric system communications.[39] Specifically, the Commission seeks comment on whether additional steps are necessary to improve remote access protections – such as incorporation of additional network segmentation controls, connection monitoring, and session termination controls behind the responsible entity Intermediate System – and whether the adoption of any additional security controls would provide substantial reliability and security benefits.[40]

ii. Comments

NERC respectfully requests that the Commission refrain from requiring any additional protections for remote access at this time. As outlined below, the Commission-approved CIP version 5 Standards, which become effective on April 1, 2016, require responsible entities to implement a number of enhanced security controls for remote access. While panelists at the April 2014 technical conference provided suggestions for enhancing those protections, it is not yet clear

[39] NOPR at P 60. The Commission is seeking comment due to the discussion at the Commission's April 29, 2014 technical conference held pursuant to Order No. 791. *See* Order No. 791 at P 225.

[40] NOPR at P 60.

whether those additional protections are necessary. The Commission should allow responsible entities time to implement the currently-approved controls before requiring any additional protections. As with all of its standards, NERC will evaluate whether additional protections are needed as it reviews the manner in which entities implement the required controls and the effectiveness of those controls.

The CIP version 5 Standards include the following requirements imposing obligations relating to remote access protections:

- *CIP-003-6, Requirement R1*: Entities must have cybersecurity policies governing remote access to BES Cyber Systems. Senior management must approve these policies to help ensure that secure practices are implemented.

- *CIP-004-6, Requirement R1*: Responsible entities must implement a cybersecurity awareness program that, at least once a calendar quarter, reinforces cybersecurity practices, which may include practices related to remote access.

- *CIP-004-6, Requirement R2*: All personnel who have remote access capability must periodically receive training that reinforces cybersecurity practices.

- *CIP-004-6, Requirement R4, Part 4.1-4.3*: All personnel who have remote access must be explicitly authorized and periodically reviewed to ensure such access is limited and controlled.

- *CIP-004-6, Requirement R5, Parts 5.1 and 5.1*: To ensure that terminated or transferred personnel do not retain the ability to access BES Cyber Systems remotely, entities must revoke the access rights of terminated or transferred personnel.

- *CIP-005-5, Requirement R1, Part 1.1*: Entities must protect all BES Cyber Systems with routable connectivity by including them in an ESP to control access.

- *CIP-005-5, Requirement R1, Part 1.2*: All connections to BES Cyber Systems originating from outside the ESP must be through an identified access point (through a firewall) so that all connections are known and controlled.

- *CIP-005-5, Requirement R1, Part 1.3*: For all connections to BES Cyber Systems inside the ESP there must be a documented reason for such access, both inbound and outbound, and a denial to all other access.

- *CIP-005-5, Requirement R1, Part 1.4*: Remote access via dial-up connectivity must be authenticated.

- *CIP-005-5, Requirement R1, Part 1.5*: All inbound and outbound communications must be examined to detect malicious communication.

- *CIP-005-5, Requirement R2, Part 2.1*: Remote access to BES Cyber Systems must go through an Intermediate System (limiting the entry points to the ESP and controlling the types of access allowed to BES Cyber Systems).

- *CIP-005-5, Requirement R2, Part 2.2*: Remote access sessions must be encrypted to protect the confidentiality and integrity of the communications.

- *CIP-005-5, Requirement R2, Part 2.3*: Remote access sessions must have multi-factor authentication to ensure only appropriate personnel have access.

- *CIP-007-6, Requirement R1, Part 1.1*: BES Cyber Systems are further protected from potential remote access attacks by limiting their network exposed ports and services to only those required for operation of the system.

- *CIP-007-6, Requirement R4*: In the event of unauthorized or suspicious remote access, entities must keep event logs and periodically review them for intervention or after-the-fact analysis.

- *CIP-007-6, Requirement R5, Part 5.1*: Remote access users of BES Cyber Systems must also authenticate their interactive use access session to the BES Cyber System.

Collectively, these requirements provide a robust set of protections for remote access. NERC has also developed a guidance document to explain and facilitate implementation of secure interactive remote access.[41] The requirements in the CIP version 5 Standards and NERC's guidance document should help ensure that entities adequately protect against risks associated with remote access. Should NERC's review of entities' implementation of the CIP version 5 standards indicate that the protections are insufficient, further modifications to the CIP Reliability Standards may be considered at that time.

[41] The guidance document is available at http://www.nerc.com/fileUploads/File/Events%20Analysis/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

d. Protections for Transient Devices Used at Low Impact BES Cyber Systems

i. NOPR

In the NOPR, the Commission states that proposed Reliability Standard CIP-010-2, Requirement R4 "appears to provide a satisfactory level of security for transient devices used at high and medium impact BES Cyber Systems."[42] The Commission stated, however, that it is concerned that the proposed Reliability Standards do not provide adequate security controls to address the risks posed by transient devices used at low impact BES Cyber Systems.[43] The Commission requested additional information regarding the burden and necessity of expanding the CIP Reliability Standards to include specific protections for transient devices used at low impact BES Cyber Systems.[44] Depending on the information received, the Commission may direct NERC to modify the CIP Reliability Standards to address the risks posed by transient devices at low impact BES Cyber Systems.

ii. Comments

As noted above, the underlying principle of the Commission-approved CIP version 5 Standards and the categorization of BES Cyber Assets as high, medium, or low impact is to require responsible entities to protect their BES Cyber Systems commensurate with the risks they present to the reliable operation of the Bulk Electric System (i.e., commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES). The goal is to focus industry resources on those areas that provide the most reliability benefit. As the Commission recognized in Order No. 791, the requirements applicable to low impact BES Cyber Systems, given their lower risk profile, should not be overly burdensome to

42 NOPR at P 41.

43 *Id*. at P 42.

44 *Id*. at P 43.

divert resources from the protection of medium and high impact BES Cyber Systems.[45] As stated in the Petition, the standard drafting team decided against requiring specific protections for transient devices used at low impact BES Cyber Systems so as not to divert resources from protecting medium and high BES Cyber Systems.[46]

Specifically, the standard drafting team concluded that if entities were required to apply protections to each transient device used at low impact BES Cyber Systems, entities would have to devote a substantial amount of resources documenting the protections afforded each such transient device, thereby limiting the resources available for protecting higher risk BES Cyber Systems. Based on feedback provided by stakeholders, NERC understands that even the smallest responsible entities are likely to have hundreds of transient devices used at assets containing low impact BES Cyber Systems, which represent the overwhelming majority of assets across the BES. For instance, a smaller registered entity could have close to 50 technicians (employees, vendors, or contractors) in the field, each using four to five transient devices. For that entity to demonstrate compliance, it would be required to have an inventory of 200 or more transient devices and track whether the technicians applied the required protections correctly to each of those transient devices. NERC understands that the resources required to manage that effort are considerable, including the effort to change the practices of a sizable number of entity personnel and contractors across the BES. The larger registered entities would have significantly more than 200 transient devices for which to track compliance and a significantly larger workforce that uses transient devices.

---

[45] Order No. 791 at P 111 (finding that it would be unduly burdensome to require responsible entities to create and maintain an inventory of Low Impact assets for audit purposes).

[46] Petition at 35.

The standard drafting team therefore determined that requiring protections for transient devices used at low impact BES Cyber Systems would create overly burdensome compliance obligations as compared to the risks associated with low impact BES Cyber Systems. As discussed in the Petition, in the judgment of the subject matter experts on the standard drafting team, focusing on the four subject matter areas included in proposed CIP-003-6, Requirements R2 for low impact BES Cyber Systems will have the greatest cybersecurity benefit for low impact BES Cyber Systems without diverting entities' focus on the protection of high and medium impact BES Cyber Systems.[47]

Further, as discussed in the Petition, while there is no explicit controls applicable to transient devices used at low impact BES Cyber Systems, entities use many of those transient devices at high and medium BES Cyber Systems, and, in turn, would be required to apply the protections required under proposed CIP-010-2, Requirement R4 on many of the transient devices used at low impact BES Cyber Systems. As such, if a responsible entity uses the same Transient Cyber Assets and Removable Media across all impact levels, the risks posed by these devices would be mitigated at all impact levels.

Additionally, the Commission's assertion that "malware inserted via a USB flash drive at a single Low Impact substation could propagate through a network of many substations without encountering a single security control under NERC's proposal" is incorrect. Under proposed Reliability Standard CIP-003-6, routable communication between substations with low impact BES Cyber Systems must pass through a Low Impact BES Cyber System Electronic Access Point ("LEAP") that permits only necessary inbound and outbound bi-directional routable protocol

[47] As discussed in the Petition, proposed Reliability Standard CIP-003-6, Requirement R2 requires entities to (1) regularly reinforce cybersecurity awareness and practices across the organization; (2) establish protections to control physical access; (3) establish electronic access controls to limit inbound and outbound communication; and (4) implement Cyber Security Incident response plans.

access. The purpose of this security control is to prevent uncontrolled access to low impact BES Cyber Systems. LEAPs will help block the propagation of many types of malware. Specifically, malware often propagates using an IP port (or ports) to scan the network to find other devices to infect. As entities would likely not configure their LEAPs to allow that type of traffic, the LEAP would block that malware from leaving the infected substation or entering a non-infected substation.[48]

Should the Commission nevertheless determine that the risk associated with transient devices used at low impact BES Cyber Systems necessitates explicitly expanding protections to those devices, NERC respectfully requests that the Commission recognize the varying risk levels presented by low impact BES Cyber Systems and the need to focus on higher risk issues. There is a large number and significant diversity of types of assets with low impact BES Cyber Systems. The risks presented by those assets may vary greatly. Any directive to modify the CIP Reliability Standards to address this issue must therefore allow for different approaches for different types of assets to ensure that the required protections are tailored to the risks presented.

e. Definition of Low Impact External Routable Connectivity

i. NOPR

In the NOPR, the Commission seeks comment on the clarity of the proposed NERC Glossary definition for LERC.[49] As the Commission recognizes, the proposed definition "describes the scenarios where responsible entities are required to apply electronic access controls under Reliability Standard CIP-003-6, Requirement R2 to their assets containing low impact BES

[48] Moreover, communications between substations typically flow through Control Centers. If the Control Centers has high or medium impact BES Cyber Systems, the communication would receive the increased protections of Reliability Standard CIP-005-5, including requirements related to detecting and mitigating malware.

[49] NOPR at PP 69-70.

Cyber Systems."[50] The Commission seeks comment on: (1) the purpose of the meaning of the term "direct" in relation to the phrases "direct user-initiated interactive access" and "direct device-to-device connection" within the proposed definition; and (2) the implementation of the "layer 7 application layer break" contained in certain reference diagrams in the Guidelines and Technical Basis section of proposed Reliability Standard CIP-003-6.[51] Depending on the comments received, the Commission may direct NERC to modify the definition of LERC.

ii. Comments

The proposed definition for LERC delineates the circumstances under which responsible entities are required to establish electronic boundary protections for low impact BES Cyber Systems that have bi-directional routable protocol communication with devices external to the asset containing the low impact BES Cyber Systems. The intent of the standards drafting team was to require responsible entities to implement security controls (i.e., implement a LEAP) where no such controls or other barriers to electronic access would otherwise exist.

Specifically, the standard drafting team concluded that if an external user or device could connect to the low impact BES Cyber System without a security break, then the entity should have to implement a LEAP to control communication into either the asset containing low impact BES Cyber System(s) or to the low impact BES Cyber System. In contrast, if an external user or device could access the low impact BES Cyber System only following a security break, such that there were existing defenses to connecting to the low impact BES Cyber System, the standard drafting team determined that there is no need to implement a LEAP. For instance, if the external user or device could connect to a low impact BES Cyber System only after going through another Cyber

50 *Id*. at P 70.

51 NOPR at P 70.

Asset, the user or device would have to know about that intermediate Cyber Asset and then figure out how to access the low impact BES Cyber System from the intermediate Cyber Asset, which provides a similar barrier to access that a LEAP is intended to provide.

The purpose of using the term "direct" in the LERC definition was therefore to distinguish between the scenarios where an external user or device could electronically access the low impact BES Cyber System without a security break (i.e., "direct" access) from those situations where an external user or device could only access the low impact BES Cyber System following a security break (i.e., "indirect" access). As the Guidelines and Technical Basis section of proposed CIP-003-6 explains:

> When determining whether there is LERC to the low impact BES Cyber System, the definition uses the phrases "direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection." The intent of "direct" in the definition is to indicate LERC exists if a person is sitting at another device outside of the asset containing the low impact BES Cyber System, and the person can connect to logon, configure, read, or interact, etc. with the low impact BES Cyber System using a bi-directional routable protocol within a single end-to-end protocol session even if there is a serial-to-routable protocol conversion. The reverse case would also be LERC, in which the individual sits at the low impact BES Cyber System and connects to a device outside the asset containing low impact BES Cyber Systems using a single end-to-end bi-directional routable protocol session. Additionally, for "device-to-device connection," LERC exists if the Responsible Entity has devices outside of the asset containing the low impact BES Cyber System sending or receiving bidirectional routable communication to or from the low impact BES Cyber System.[52]

The Guidelines and Technical Basis section further clarifies that LERC exists where communication from an external user or device flows through an intermediate Cyber Asset (e.g., an IP/Serial converter) and the intermediate Cyber Asset only does a "pass-through" of the communication (i.e., it does nothing more than extend the communication between the low impact

[52] Reliability Standard CIP-003-6, Guidelines and Technical Basis at pp. 28-29.

BES Cyber System and the Cyber Asset external to the asset containing the low impact BES Cyber System).[53] Only where the intermediate Cyber Asset provides a complete security break (i.e., prevents extending access to the low impact BES Cyber System from the external Cyber Asset) is there no LERC. For instance, if an IP/Serial converter performs some type of authentication in the data flow at the asset containing the low impact BES Cyber System before the communication is sent to the low impact BES Cyber System, then there is no LERC.[54] In that scenario, the standard drafting team concluded, there is no need to implement a LEAP as the security break provides sufficient protection commensurate to the risks presented by low impact BES Cyber Systems.

The Guidelines and Technical Basis section also provides examples of what would or would not constitute sufficient access controls to help entities effectively implement the electronic access requirements in proposed CIP-003-6.[55] The reference models in the Guidelines and Technical Basis section are also intended to help entities by illustrating how to determine whether there is LERC and how to implement a LEAP. With respect to FERC's concern regarding implementation of the layer 7 application break in Reference Model 6, NERC notes that LERC would exist and a LEAP would be required if an entity's implementation of a layer 7 application break does not provide a sufficient security break (i.e., the layer 7 application does not prevent direct access to the low impact BES Cyber Asset). As with all of the configurations illustrated in the Reference Models, NERC and the Regional Entities will review the entity's implementation to ensure that it is consistent with the language and intent of the electronic access restrictions in proposed CIP-003-6, Requirement R2.

---

53 Reliability Standard CIP-003-6, Guidelines and Technical Basis, Reference Model 4 at p. 34.

54 Reliability Standard CIP-003-6, Guidelines and Technical Basis, Reference Model 6 at p. 36.

55 Reliability Standard CIP-003-6, Guidelines and Technical Basis at pp. 30-31.

In sum, between the language of the proposed definition and the guidance in the Guidelines and Technical Basis section of proposed CIP-003-6, there is no need to revise the definition of LERC. Nevertheless, should comments to the NOPR or questions from stakeholders during the implementation period indicate that stakeholders are confused as to the meaning and application of the LERC definition, NERC will take the necessary steps, including potentially modifying the definition through its standard development process, to ensure entities can effectively and efficiently implement the proposed Reliability Standards.

III. CONCLUSION

NERC respectfully requests that the Commission consider these comments and approve the proposed CIP Reliability Standards.

Respectfully submitted,

/s/ Shamai Elstein

Charles A. Berardesco
Senior Vice President and General Counsel
Holly A. Hawkins
Associate General Counsel
Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
charlie.berardesco@nerc.net
holly.hawkins@nerc.net
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: September 21, 2015