**UNITED STATES OF AMERICA**
**BEFORE THE**
**FEDERAL ENERGY REGULATORY COMMISSION**

| | | |
|---|---|---|
| **Reliability Standards for Critical Infrastructure Protection and Supply Chain Management** | ) | **Docket No. RM15-14-000** |

# COMMENTS OF THE EDISON ELECTRIC INSTITUTE, THE AMERICAN PUBLIC POWER ASSOCIATION, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, ELECTRIC POWER SUPPLY ASSOCIATION, ELECTRICITY CONSUMERS RESOURCE COUNCIL, TRANSMISSION ACCESS POLICY STUDY GROUP, AND THE LARGE PUBLIC POWER COUNCIL

The American Public Power Association ("APPA"), the Edison Electric Institute ("EEI"), Electric Power Supply Association ("EPSA), the National Rural Electric Cooperative Association ("NRECA"), Electricity Consumers Resource Council ("ELCON"), Transmission Access Policy Study Group ("TAPS"), and the Large Public Power Council ("LPPC"), collectively, the "The Trade Associations," respectfully submit these comments in response to the Notice of Proposed Rulemaking ("NOPR") issued by the Federal Energy Regulatory Commission ("Commission" or "FERC") on July 16, 2015, in the above-referenced docket.[1] The Commission proposes to approve seven revised critical infrastructure protection ("CIP") mandatory Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6

[1] *Revised Critical Infrastructure Protection Standards,* Notice of Proposed Rulemaking, 152 FERC ¶ 61,054 (2015).

(Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection). In addition, the Commission proposes to approve the proposed implementation plan and violation risk factor and violations security level assignments, and proposed new and revised definitions for the NERC Glossary of Terms. The Commission also proposes to direct further modification of CIP-006-6 to require protections for communication network components and data communicated between all bulk electric system control centers. Lastly, the Commission proposes to direct NERC to develop requirements relating to supply chain management for industrial control system hardware, software, and services.

**INTERESTS OF THE TRADE ASSOCIATIONS**

APPA is the national service organization representing the interests of not-for-profit, publicly owned electric utilities throughout the United States. More than 2,000 public power systems provide over 14% of all kilowatt-hour sales to ultimate customers and serve over 48 million people, doing business in every state except Hawaii. Public power systems own approximately 10.3% of the total installed generating capacity in the United States. Approximately 281 APPA members are subject to compliance with NERC standards applicable to users, owners and operators of the Bulk-Power System ("BPS").

EEI is trade association that represents all U.S. investor-owned electric companies. Our members provide electricity for 220 million Americans, operate in all 50 states and the District of Columbia, and directly employ more than 500,000 workers. With more than $85 billion in annual capital expenditures, the electric industry is responsible for millions of jobs related to the delivery of power, including the construction of modified or new infrastructure. Reliable,

affordable, and sustainable electricity powers the economy and enhances the lives of all Americans. EEI has 70 international electric companies as Affiliate Members, and 250 industry suppliers and related organizations as Associate Members. Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums. In addition, its members include Generator Owners and Operators, Transmission Owners and Operators, Load-Serving Entities, and other entities that are subject to mandatory Reliability Standards developed and enforced by NERC.

ELCON is the national association representing large industrial consumers of electricity. ELCON member companies produce a wide range of products from virtually every segment of the manufacturing community. ELCON members operate hundreds of major facilities and are consumers of electricity in the footprints of all organized markets and other regions throughout the United States. Reliable electricity supply is essential to our members' operations.

EPSA is the national trade association representing leading competitive power suppliers, including generators and marketers. Competitive suppliers, which collectively account for 40 percent of the installed generating capacity in the United States, provide reliable and competitively priced electricity from environmentally responsible facilities. EPSA seeks to bring the benefits of competition to all power customers. EPSA companies typically operate in several NERC Regions.

LPPC is an association of the 25 largest state-owned and municipal utilities in the nation and has moved separately to intervene in this proceeding. LPPC members are located throughout the nation, both within and outside RTO boundaries. LPPC represents the larger, asset owning members of the public power sector.

NRECA is the national service organization for more than 900 not-for-profit rural electric utilities that provide electric energy to over 42 million people in 47 states or 12 percent of electric customers. Kilowatt-hour sales by rural electric cooperatives account for approximately 11 percent of all electric energy sold in the United States. NRECA members generate approximately 50 percent of the electric energy they sell and purchase the remaining 50 percent from non-NRECA members. The vast majority of NRECA members are not-for profit, consumer-owned cooperatives. NRECA's members also include 65 generation and transmission ("G&T") cooperatives, which generate and transmit power to 668 of the 838 distribution cooperatives. The G&Ts are owned by the distribution cooperatives they serve. Remaining distribution cooperatives receive power directly from other generation sources within the electric utility sector. Both distribution and G&T cooperatives were formed to provide reliable electric service to their owner-members at the lowest reasonable cost. NRECA members are directly affected by the proposed Reliability Standard developed and enforced by NERC.

TAPS is an association of transmission-dependent utilities ("TDUs") in more than 35 states, promoting open and non-discriminatory transmission access.[2] TAPS members have long recognized the importance of grid reliability. As TDUs, TAPS members are users of the BPS, highly reliant on the reliability of facilities owned and operated by others for the transmission service required to meet TAPS members' loads. In addition, many TAPS members participate in the development of and are subject to compliance with NERC Reliability Standards.

[2] Duncan Kincheloe, Missouri Public Utility Alliance, chairs the TAPS Board. Jane Cirrincione, Northern California Power Agency, is TAPS Vice Chair. John Twitty is TAPS Executive Director.

## EXECUTIVE SUMMARY

The Trade Associations support the Commission's proposal to approve the seven revised CIP mandatory Reliability Standards, the implementation plan, the violation risk factor and violations security level assignments, and the new and revised definitions. We encourage the Commission to issue a final rule approving these revisions by December 31, 2015 without further modifications. Time and actual experience from the implementation process is needed to allow Responsible Entities, NERC, and the Commission to determine whether the new CIP Version 5 (" CIP V5") Reliability Standards contain reliability gaps, overlaps, or inefficiencies that merit formal review in the standards development process. We also urge the Commission to continue to support the risk-based approach taken by NERC for the CIP Reliability Standards. CIP V5 will ensure a durable, risk-informed framework that allows Responsible Entities to apply the most appropriate technologies, applications, and controls based on the risk to their assets and facilities.

The Trade Associations do not support the Commission's proposed directive for mandatory supply chain requirements because the Trade Associations do not share the Commission's views regarding a perceived gap in the mandatory Reliability Standards regarding supply chain risks for CIP and cybersecurity procurement. While the Trade Associations agree that CIP and cybersecurity risks form a high priority strategic matter for the electric industry, no events or disturbances have taken place that indicate a problem or emerging pattern or trend. Moreover, CIP V5 standards address a broad range of supply chain issues. To the extent the Commission seeks to direct NERC to develop mandatory requirements, the Trade Associations offer a set of considerations for the Commission.

## COMMENTS

### I. The Commission should approve the seven CIP Reliability Standards and associated revisions, including the implementation plan, as proposed by NERC with an order effective on or before December 31, 2015.

The Trade Associations support the Commission's proposal to approve the seven CIP Reliability Standards: CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2, and CIP-011-2 ("V5 Revisions"); the implementation plan; the violation risk factor and violations severity level assignments; and the new and revised definitions for the NERC Glossary of Terms as proposed by NERC. The Trade Associations also support the Commission's proposal to retire CIP-003-5, CIP-004-5.1, CIP-006-5, CIP-007-5, CIP-009-5, and CIP-011-1 ("V5").

The Trade Associations encourage the Commission to issue a final rule approving the V5 Revisions by December 31, 2015 so that the revisions[3] become effective under the implementation plan on April 1, 2016. This would avoid having CIP V5 become effective on April 1, 2016 and then having the V5 Revisions become effective on July 1, 2016 or later. Implementation by Responsible Entities of two different versions of the standards within a few months will unnecessarily complicate the ongoing transition to the new versions and increase the administrative transition burden with no tangible benefits to security or bulk electric system (BES) reliability. Commission action taken after December 31, 2015 will result in Responsible Entities dedicating resources toward implementing V5 to minimize compliance risk. Therefore, if a final rule approving the V5 Revisions effective by December 31 is not feasible, then we encourage the Commission to take alternative actions to avoid this burden.

[3] Specifically, the revisions set to "become effective on the later of April 1, 2016 or the first day of the first calendar that is three months after the effective date of the Commission's order approving the proposed Reliability Standard" under the implementation plan. NERC Petition at 53-54.

The Trade Associations urge the Commission not to make any changes to Requirements in the CIP V5 Revisions as proposed by NERC. CIP V5, including the V5 Revisions as proposed, provides a defense-in-depth approach that ensures that the broad range of security controls are proportionate to the potential cybersecurity risks to BES reliability. Stability of these new standards will ensure a durable and long-lived framework that allows Responsible Entities to determine the most appropriate technologies, applications, and controls based on the risk to their assets and facilities. Time is needed to allow for Responsible Entities, NERC, and the Commission itself to examine, through experience, whether CIP V5 contains reliability gaps, overlaps, or inefficiencies that merit formal review in the standards development process.

The Trade Associations also encourage the Commission to continue to support the risk-based approach taken by NERC for CIP V5.[4] The high-medium-low impact categorization is based on the National Institute of Standards and Technology (NIST) Risk Management Framework.[5] Fundamental to this risk-informed approach is the concept that the same protections required for medium and high impact BES Cyber Systems are not warranted for low impact assets due to the lower risk of these assets to BES reliability. These risk-based improvements are crucial to allowing the industry to focus on reliability and security, rather than compliance. The Trade Associations are concerned by some of the Commission's proposals in the NOPR, particularly those (e.g., CIP-006-6 and CIP-010-2) recommending expanding high and medium impact BES Cyber System controls to low impact assets (facilities), which appear to

[4] We note that NERC's risk-based approach to the CIP Version 5 Standards is consistent with NERC's overall goal to become a more risk-informed enterprise. *See N. Am. Elec. Reliability Corp.*, 150 FERC ¶ 61,108 (2015) (approving NERC's Reliability Assurance Initiative and "finding that NERC's overall goal of focusing ERO and industry compliance resources on higher-risk issues that matter more to reliability is reasonable."); *see also N. Am. Elec. Reliability Corp.*, 150 FERC ¶ 61,213 (2015) (approving in part NERC's Risk-Based Registration).

[5] *Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 78 Fed. Reg. 72,577 (Dec. 3, 2013), 145 FERC ¶ 61,160 (2013) PP 14-15.

deviate from this risk-based approach. The final rule should not adopt directives inconsistent with NERC's risk-based approach, which rightly recognizes that the same protections required for high and medium impact BES Cyber Systems are not warranted for low impact assets.

### A. Modification of the CIP-006-6 requirements to address protections for communication network components and data between all BES Control Centers should focus on High and Medium Impact BES Cyber Systems, must align with clear reliability risks, use results-based requirements, and carefully consider implementation challenges inherent to components and data exchange owned and operated by different entities.

In the NOPR, the Commission proposes to direct NERC to develop modifications to Reliability Standard CIP-006-6 to require protections for communication network components and data communicated between "all bulk electric system Control Centers." Although we agree that modifications seeking to address protections for communication network components and data communicated between Control Centers with high and medium impact BES Cyber Systems may improve the reliability of the bulk electric system, such modifications should not be extended to low impact Control Centers.

The Commission's proposal to modify CIP-006-6 to add controls for "all bulk electric system Control Centers"[6] suggests including low impact assets (i.e., Control Centers) in these modifications. The existing controls in CIP-006-6 apply only to high and medium impact BES Cyber Systems "because those locations present a heightened risk to the Bulk-Power System warranting the increased protections."[7] In developing CIP-006-6, the Standards Drafting Team considered suggestions to extend the applicability of the standard to low impact assets, but after weighing "the level of effort to meet the Requirement…against the risk posed to the BES," the

[6] NOPR at 59.

[7] NERC Petition at 48.

team concluded that the proposed revisions are "adequate and appropriate to protect the reliability of the BES."[8] Extending proposed CIP-006-6 modifications to this standard would be inconsistent with the risk-based approach supported by industry, NERC, and the Commission. Thus the final rule should not direct modifications that would require protections for data and communications with low impact Control Centers.

Regarding new protections for communication network components and data communicated between high and medium impact Control Centers, we strongly encourage the Commission consider the following in directing such modifications:[9]

1. The risk and impact is unclear and should be carefully studied to determine which additional protections are needed relative to the BES reliability risk. We recommend that the Commission direct NERC to conduct a study to: 1) identify the data communicated between control centers that is necessary for reliable BES operations; 2) determine the sensitivity of said data to a loss of availability, integrity, or confidentiality; 3) identify the controls currently in place to mitigate the risk of a loss of availability, integrity, or confidentiality; and 4) develop a plan to address remaining gaps, if any.

2. Risks to BES reliability should drive CIP modifications, if warranted. Because the Commission is proposing to modify CIP-006-6 and this standard addresses the physical security of high and medium impact BES Cyber Systems, we assume that the

[8] NERC Petition, Exhibit F, Consideration of Comments Initial Comment Period (September 3, 2014), p. 17.

[9] Should the Commission decide, despite the Trade Associations' urging, to extend CIP-006-6 to low impact control centers, we urge the Commission to consider these principles with respect to low impact control centers as well.

Commission is focusing on physical protection for these systems. Physical protection to mitigate communication loss is handled with redundant and/or path diversity. Physical protection to mitigate threats involving communication content may not be an effective protection strategy, particularly for inter-control center communications. Logical controls (e.g., encryption and connection link monitoring) may reduce risks of data being intercepted and altered more effectively. Due to the diversity among Responsible Entity operations, the capability of implementing and the effectiveness of physical and/or logical controls will vary. Modifications to the standards will require flexibility to apply to diverse operational facts and circumstances. We recommend that the Commission allow the standard drafting team to determine which reliability standards, if any, to modify to address a more clearly defined risk objective and continue to strive for results-based standards.

3. Protecting communication network components and data between Control Centers, especially those operated by different entities, may create unique challenges to implementing new requirements. For example, contracts will likely need to be renegotiated or established to address auditing to the modified standard(s). In addition to these concerns, the implementation of CIP standards will continue over the next two years. Therefore, we recommend that the Commission carefully consider the timing for further standards modifications in relation to the risk to the reliability of the BES.

4. Any further standard modifications should follow a risk-informed approach, recognizing that if a Control Center and its associated communication components

pose minimal risk to the reliability of the bulk electric system, then new requirements would not be commensurate with the risk. Therefore, we recommend that the Commission rely on the NERC-led risk assessment in determining which Control Center communications need protections and what level and type of protection is warranted.

### B. The limited applicability of CIP-010-2 is not a gap in protection to BES reliability because CIP-003-6 addresses the risks posed by transient devices used for Low Impact BES Cyber Systems.

The Commission proposes to direct NERC to provide additional information regarding the omission of low impact BES Cyber Systems from CIP-010-2 and whether this omission creates a gap in protection to BES reliability. The Commission is concerned that this omission would enable malware inserted via a transient device to propagate to multiple substations without encountering a security control.

The Trade Associations do not believe there is a gap in protection of BES reliability. The potential for propagation of malicious code or other unauthorized access was a key driver behind the creation of the Low Impact BES Cyber System External Routable Connectivity (LERC) and Low Impact BES Cyber System Electronic Access Point (LEAP) definitions and associated security requirements in CIP-003-6. One reference where this can be clearly seen is in the Guidelines & Technical Basis section in its discussion on the Reference Model 3 diagram and the following text:

"The entity also has the flexibility with respect to the location of the LEAP. LEAPs are not required to reside at the asset containing the low impact BES Cyber Systems. Furthermore, the entity is not required to establish a unique physical LEAP per asset containing low impact BES Cyber Systems. Responsible Entities can have a single Cyber Asset containing multiple LEAPs that controls the LERC for more than one asset containing low impact BES Cyber

Systems. Locating the Cyber Asset with multiple LEAPs at an external location with multiple assets containing low impact BES Cyber Systems "behind" it, however, should not allow uncontrolled access to assets containing low impact BES Cyber Systems sharing a Cyber Asset containing the LEAP(s)."

This potential propagation from a BES asset containing low impact BES Cyber Systems to another was a primary concern and the above shows that even if multiple assets containing low impact BES Cyber Systems are behind one firewall, all routable protocol communications between those assets must be controlled by a LEAP. Direct substation to substation communications with no security controls is not allowed in the current CIP-003-6 Standards with the sole focused exception included in the LERC definition intended for extremely time sensitive device to device coordination. All asset to asset level routable communications must go through the security control of the LEAP. Therefore, the application of CIP-010-2 to only medium and high Impact BES Cyber Systems is intentional and does not create a gap in protection.

In addition to the LEAP requirement, CIP-003-6 requires many protections similar to those required for high and medium BES Cyber Systems, including cyber security awareness, physical security controls, electronic access controls, and incident response. The CIP-003-6 cyber security awareness and physical access controls further minimize the risk of malware propagation and infection. These protections under CIP-003-6 are commensurate with the risk that low impact BES Cyber Systems pose to the reliability of the bulk electric system.

CIP-003-6 applies to Cyber Assets that if compromised, even by malware, would have a low impact on reliability. A risk-informed approach dictates that due to the lower risk, the same protections required by high and medium impact systems are not warranted for systems with lower reliability risk. The CIP version 5 standards framework ensures that the broad range of security controls are proportionate to the potential cybersecurity risks to reliability of the BES.

The ability of malware to traverse across low impact substations is also limited due to the diversity and complexity of these assets. Low impact assets contain Cyber Assets that are extremely diverse in nature and type of systems, and could number into tens of thousands for any particular company. These Cyber Assets are configured and connected in various ways, which reduces the ability for malware to propagate among substations. For malware to traverse across these different assets, the malware would have to be extremely complex and be able to exploit a number of different vulnerabilities to infect and traverse across the diverse Cyber Assets. The likelihood of creating and using this malware is low. The impact on reliability if such malware was created, used, and successful is also low. As a result, the risk to the BES is inherently low.

Also due to the diverse Cyber Assets, developing specific, unambiguous security controls for low impact transient cyber assets would be extremely difficult to prescribe in a standard. In addition, under CIP-003-6, Responsible Entities do not have to identify the low impact BES Cyber Assets within a system or asset. Therefore, additional transient cyber asset protections would need to be at the asset level (facility or site-level) to avoid creating substantial administrative burdens disproportionate to the risk. The flexible framework created by CIP-003-6 appropriately addresses the risk to low impact assets posed by transient devices.

For all of these reasons, the Trade Associations urge the Commission not to issue any directives that would modify CIP-010-2 to include low impact assets.

### C. An appropriate time for the Commission to evaluate whether gaps exist in remote access security controls that could impact bulk electric system reliability is after the new remote access CIP requirements have been implemented.

The NOPR asks whether enhanced security controls, such as providing additional network segmentation behind intermediate systems, are needed to improve protections for remote access. Responsible Entities are currently implementing the new Interactive Remote Access and Electronic Access Control or Monitoring Systems Controls for Intermediate Systems. It is too early to determine whether additional security controls behind the Intermediate Systems are needed to manage risks, what these controls should require, and whether they would have substantial reliability and security benefits.

### D. The Commission does not need to direct a change in the definition of Low Impact External Routable Connectivity (LERC).

The Guidelines and Technical Basis for CIP-003-6, which were subject to comment and part of the standard that Responsible Entities voted on and approved, add clarity to the LERC definition with regard to what "direct" means. Specifically, if an IP/Serial converter simply converts a routable protocol communication to a non-routable protocol communication without authentication or a layer 7 (application layer)[10] break, then a direct routable protocol connection exists (i.e., the LERC definition is met).[11] However, if the IP/Serial converter or some other Cyber Asset provides a layer 7 application layer break or requires authentication, then a new connection to the low impact BES Cyber System is established and no direct routable protocol

[10] Layer 7 is the application layer under the Open Systems Interconnect (OSI) model. It is the layer where the user interacts directly with the software application. *See* ISO/IEC 7498-1, *Information technology – Open Systems Interconnection–Basic Reference Model: The Basic Model*, available at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[11] *See* CIP-003-6 Guidelines and Technical Basis, Reference Model 4.

connection exists (i.e., the LERC definition is not met).[12] Although the Trade Associations believe the LERC definition combined with the Guidelines and Technical Basis for CIP-003-6 makes the term "direct" clear to Responsible Entities, the Trade Associations do not oppose such a modification as long as it is consistent with the Guidelines and Technical Basis and does not change its meaning.

## II. Consideration of potential mandatory NERC supply chain management requirements must align with clear reliability risks, recognize both the laws and the facts, and avoid overlaps with existing requirements.

In the NOPR, the Commission seeks comments on a proposal to direct NERC to develop a mandatory reliability standard to address supply chain management for industrial control systems. The NOPR states that even though Order No. 791 approving various mandatory NERC CIP standards did not address supply chain management issues, recent malware campaigns targeting supply chain vendors highlight a gap in the protections under the Commission-approved CIP standards.[13] The NOPR identifies a recent ICS-CERT report that describes this campaign as involving the injection of malware while a product or service remains under the control of the hardware or software vendor, and prior to the delivery to the customer.[14] Based on this report, the Commission concludes that it views as reasonable the development of a new or modified mandatory NERC reliability standard to provide security controls for supply chain management.[15]

---

[12] *See* CIP-003-6 Guidelines and Technical Basis, Reference Model 6.

[13] NOPR, p. 38.

[14] See: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A.

[15] NOPR, P. 64.

The Commission states that such a standard should encompass activities in the system development cycle, including research and development, design and manufacturing, acquisition, delivery, integration, operations, retirement, and eventual disposal. In addition, the standard should ensure security, integrity, quality, and resilience of the supply chain and the future acquisition of products and services.[16] In addition, the NOPR states that the "right set" of security controls should accommodate a company's procurement process, vendor relations, system requirements, information technology implementation, and privileged commercial and financial information.[17] The NOPR cites a document developed by the National Institute of Standards and Technology (NIST), SP600-161, a guidance document for Federal Information Processing Standard 199 for Federal Information and Information Systems.[18] The NOPR cites to a DOE cybersecurity procurement document as well.[19]

The NOPR acknowledges the broadness of the supply chain issue area and the many aspects of supply chain management, observing that a mandatory NERC reliability standard must recognize the limits of Section 215 jurisdiction by not imposing obligations directly on suppliers or vendors, not dictating the abrogation or renegotiation of existing contracts, setting goals while allowing for flexible approaches, allow for exceptions in cases where secure products may be

[16] NOPR, P. 64.

[17] NOPR, P. 65.

[18] See: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

[19] See:

http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

unavailable, and providing enough specificity so that compliance obligations are clear and enforceable.[20]

The Trade Associations strongly agree with the Commission that critical infrastructure protection, including cybersecurity, has evolved to become a significant potential risk for maintaining reliable operations. The Trade Associations and their members have strongly supported the development of the mandatory CIP standards at NERC, including CIP V5.[21] Companies across the United States are taking actions for initial CIP V5 implementation set for early 2016.

In recent years, top-level utility executives and leaders have been actively engaging with each other and with federal governmental entities to discuss these issues, through the Electricity Subsector Coordinating Council (ESCC) for example. In addition, the Trade Associations' respective members have identified security issues associated with potential supply chain disruption or compromise as being a significant threat. Trade Associations' members also participated in the development of the Cybersecurity Procurement Language for Energy Delivery Systems to which the NOPR refers. Electric system asset owners and operators actively participated in the development of this document.

As part of a Threat Scenario Project conducted by EEI with its member companies in 2011-12, specific risks were identified and a series of mitigation measures developed to assist

[20] NOPR, P. 66.

[21] *Version 5 Critical Infrastructure Protection Reliability Standards.* Order No. 791. 78 Fed. Reg. 72,577 (Dec. 3, 2013), 145 FERC ¶ 61,160.

companies in managing these risks.[22] Earlier this month, the EEI board of directors approved a set of Principles and Resources for Managing Supply Chain Cybersecurity Risk and Recommendations for Managing Supply Chain Cybersecurity Risk designed to facilitate discussions among utilities and their vendors to help manage supply chain risks.[23]

Moreover, the October 2014 report and recommendations of the NERC Reliability Issues Steering Committee (RISC) ranked cyber attack as the second most important risk to reliability in need of action.[24] In particular, the RISC report noted the "constantly evolving" nature of the issue as a rising risk trend in comparison to the 2013 report.

However, the Trade Associations do not do not support the Commission's proposed directive for mandatory supply chain requirements because the Trade Associations do not share the Commission's view of the reliability gap as described in the NOPR. In terms of supply chain management for CIP and cybersecurity products and services, transmission owners and operators

[22] In 2011, in conjunction with third party private sector experts and its member utilities, EEI initiated the Threat Scenario Project to identify cyber threats and practices to mitigate these threats. The project established common elements for each threat scenario, including a description, likely targets, potential threat actors, specific attack paths, likely impacts of a successful attack, and potential mitigation measures. The project continues to evolve as the threat landscape changes in order to keep the industry prepared to identify and defend against emerging cyber threats. http://www.eei.org/issuesandpolicy/cybersecurity/Documents/EEI%20Cybersecurity%20Backgrounder.pdf

[23] The Threat Scenario Project in 2011-12 served as the initiating event for development of the recently approved supply chain principles and recommendations. Since that time, EEI Chief Information Officers (CIOs) and their supply chain and procurement personnel worked with EEI staff to define four technical issue areas – standards, manufacturing, procurement, and assurance – and associated recommendations and mitigation measures. Following the adoption of the Principles and Resources for Managing Supply Chain Cybersecurity Risks and Recommendations for Managing Supply Chain Cybersecurity Risk by the EEI Board, EEI anticipates that member companies will continue to enhance their procurement activities and share best practices going forward. See: http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalRecommendationsforManagingSupplyChainCybersecurityRisk.pdf http://www.eei.org/issuesandpolicy/testimony-filings-briefs/Documents/150917FinalEEIPrinciplesandResourcesforManagingSupplyChainCybersecurityRisk.pdf

[24] See: http://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO%20Reliability%20Risk%20Priorities%20%20RISC%20Updates%20and%20Recommendations%20-%20October%202014.pdf

take their responsibilities extremely seriously. Especially for EMS and SCADA systems, and other critical systems needed for planning and realtime operations, the design, procurement, installation, testing, and operations and maintenance of these highly complex systems take place under rigorous management disciplines. These disciplines rest on a set of critical underlying principles that various control systems are vulnerable, critical systems and data cannot be trusted, that these systems may be compromised, and as a result Responsible Entities organize the planning and operations for these systems through elaborate defense-in-depth approaches that anticipate a broad range of combinations of contingencies. Application of these principles necessarily involves the business relationships that Responsible Entities have with third-party suppliers and vendors who provide products and services.

Since this subject within the NOPR does involve complex systems and sensitive technical issue areas relating to business proprietary and contractual arrangements, the Trade Associations consider it inappropriate to describe details of entities' business approaches to procurement, testing, and operation and maintenance of these systems, or the potential specific risks that companies anticipate in their design or procurement strategies. However, the Trade Associations understand that engagements with third-party suppliers and vendors involve comprehensive, highly detailed and candid discussions on a broad range of sensitive matters within the supply chain.

In addition, the Trade Associations disagree with the NOPR contention that a gap exists in the Commission-approved NERC standards. While NERC standards do not contain explicit provisions for supply chain management, transmission owners and operators already have significant responsibilities to perform under various Commission-approved CIP standards that

already address supply chain issues. To the extent that cyber assets fail to perform and cause instability or cascading outages, substantial compliance issues could arise, including monetary penalties of up to $1 million/day/violation. In particular, the Trade Associations view the CIP V5 framework as a comprehensive structure designed to endure various new or evolving technical threats, thus fulfilling the Section 215 mandate for cybersecurity protection for reliable operations to protect against instability, uncontrolled separation, or cascading failures.

While Order No. 791 may not contain explicit references to the term "supply chain," CIP V5 provides very strong supply chain controls. In particular, the Commission-approved CIP-010-2 for cyber asset change management establishes a bedrock principle of mistrusting any cyber assets in the high risk category, and requiring extensive testing and vulnerability assessments prior to connecting to BES assets.[25] Therefore, CIP-010-2 creates a strong incentive for Responsible Entities to work with third-party suppliers and vendors throughout the design and development of various products and services in order to avoid issues or problems at the time of connecting these cyber assets. Responsible Entities must have in place strong internal processes and controls to manage these critical business relationships, Appendix 1 of these comments, a mapping of the NIST Framework to the NIST SP800-161 supply chain overlay, and the CIP V5 mandatory standards, plainly shows that CIP V5 covers all aspects of the NIST Framework for which the Commission has explicit oversight authority.

The Trade Associations also disagree with both the Commission's characterization that the ICS-CERT reports indicate a changed threat landscape that define a reliability gap, and the actual technical challenges raised by the reports. As reported in the ICS-CERT documents, these

[25] See: http://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf

campaigns seek to inject malware, while a product is in the control of and in use by the customer and not, as the NOPR suggests, the vendor. The first ICS-CERT alert reports on the Havex malware, which infects systems through phishing emails or "watering hole" attacks, which seek to trick the customer into downloading the malware. The second alert focuses on a variant of the BlackEnergy malware, which infects Internet-connected human-machine interface devices by exploiting vulnerabilities in these devices. The ICS-CERT mitigation measures in each of the alerts are also focused on the customer and do not address security controls, while the products are under control of the vendors. While the NOPR expresses concern of a potential reliability gap, the Trade Associations strongly believe that the existing Commission-approved CIP V5 security controls address the risks associated with the issues in ICS-CERT reports referenced by the Commission in the NOPR.[26] CIP-010-2 explicitly addresses both of these issues.

Moreover, the Trade Associations can find nothing within various NERC programs and activities that lead to a reasonable conclusion that supply chain management issues have caused events or disturbances on the bulk power system. A review of the NERC RISC reports, the NERC State of Reliability reports, NERC Events Analysis reports, and minutes of meetings of the NERC Critical Infrastructure Protection Committee and Operating Committee, offer no evidence that a reliability problem exists with regard to supply chain management, and certainly not an issue rising to the level that demands mandatory requirements. Two incidents in 2015 involving EMS system issues offer no indication of a systematic risk or supply chain-related

[26] See NOPR discussion at P. 63.

problem.[27] In addition, examination of DOE OE-417 electric disturbance reports do not suggest an issue.[28]

As part of the broad policy initiative for NERC to build mandatory standards on a results-based and risk-based foundation, at this point the Trade Associations view the Commission-approved reliability standards as forming a comprehensive catalog supporting the Commission's Section 215 mandate. The Trade Associations have long supported the results-based risk-based approach for mandatory reliability standards as rightly avoiding specific requirements prescribing how companies perform to achieve reliable operations, and specifically, their supply chain management practices. The Trade Associations also strongly support the Commission-approved CIP V5 framework as providing a thorough, effective, and enduring framework to address the broad range of CIP- and cyber security-related risks. In contrast, the NOPR suggests that the pursuit of cybersecurity protection for reliable operations embodied most recently in Commission's approval of CIP V5 must include mandatory requirements for "how" companies will manage such processes. Where V5 comprises the "what" framework for cybersecurity protection, the NOPR seems to propose mandatory requirements for "how" companies conduct their performance.

The Trade Associations also believe that several other tools can provide significant support for addressing CIP and cybersecurity supply chain management in lieu of mandatory requirements. For example, Responsible Entities use the cybersecurity procurement guidance

[27] See NERC Lesson Learned # 20150604 and #20150301. Specifically, "…in the first incident the entire system went into a full system-wide auto-recovery process due to a configuration issue on control center servers while the second incident occurred during testing of switchover capabilities of EMS systems."

[28] See http://www.oe.netl.doe.gov/oe417.aspx

published by DOE, as well as procurement guidance developed by the Department of Homeland Security.[29]

The NERC reliability risk management group could provide support, including the development of supply chain guidelines. The 2014 NERC review of the polar vortex included a set of recommendations and did not rise to the level of consideration of formal mandatory requirements.[30] Since the initial 2014 report, NERC has conducted several winter season readiness activities, issued guidelines, and conducted webinars.[31] In addition, many references were made by representatives of RTOs and ISOs at the FERC open meeting on September 17 regarding coordination and planning with reliability entities for the upcoming winter season.[32] Trade Associations also understand that the various NERC regions conduct seasonal planning and coordination activities.

In addition, the North American Energy Standards Board ("NAESB") offers a certification for software products or solutions that offers another consideration for the Commission.[33] Modeled on Sarbanes-Oxley, companies offering products self-certify that those products meet certain minimum requirements set forth in the applicable NAESB standards. Currently, virtually all NAESB certifications take place under the wholesale gas

---

[29] See https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf. See footnote #19 for citation to the cysecurity procurement guidance document.

[30] See: http://www.nerc.com/pa/rrm/January%202014%20Polar%20Vortex%20Review/Polar_Vortex_Review_29_Sept_2014_Final.pdf

[31] See NERC Cold Weather Training Materials at http://www.nerc.com/pa/rrm/ea/Pages/Cold-Weather-Training-Materials.aspx.

[32] See for example: http://www.ferc.gov/industries/electric/indus-act/rto/pjm-presentation.pdf

[33] See: https://www.naesb.org//materials/certification.asp.

quadrant.[34] The Trade Associations understand that NAESB is considering expansion of its software certification program to both the retail and wholesale electric quadrants. The Commission reviews all NAESB standards and incorporates them by reference into jurisdictional tariffs.

As policy matters, the Trade Associations seek clarifications in the final order in this docket on three basic issues. First, the structure of the NOPR discussion appears to suggest a new mandate, over and above Section 215, for energy security, integrity, quality, and supply chain resilience, and the future acquisition of products and services.[35] The NOPR lays out no reasoning that connects energy security and integrity with reliable operations for bulk power system reliability. Therefore, the Trade Associations seek clarification that the Commission does not intend to define "energy security" as a new policy mandate and urges the Commission to remain faithful to its Section 215 reliability mandate as a sufficient basis for its actions.

Second, as the NOPR indicates, the Commission has no direct oversight authority over third-party suppliers or vendors and, in addition, cannot indirectly assert authority on them through jurisdictional entities.[36] The Commission's rationale, however, has no limiting principle. Without such limits, the Commission ostensibly could seek to regulate under the blanket rationale of "supply chain" any number of areas, including fuel procurement or labor relations. Such an extension would be unlawful and the Trade Associations seek clarification that the Commission will avoid seeking to extend its authority since such an extension would set

[34] See: https://www.naesb.org//pdf2/cert_products.pdf

[35] NOPR at P. 64.

[36] See Altamonte Gas Transmission Co. v. FERC, 92 F.3d 1239, 1248 (D.C. Cir. 1996) (noting FERC cannot "do indirectly what it could not do directly"); see also Richmond Power & Light v. FERC, 574 F.2d 610, 620 (D.C. Cir. 1978); Williams Gas Processing-Gulf Coast Co., L.P. v. FERC, 331 F.3d 1011, 1022 (D.C. Cir. 2003).

a troubling precedent. The potential that the Commission might seek to impose responsibilities on Responsible Entities for actions beyond their control – and beyond the Commission's jurisdiction -- could cause a broad range of unintended consequences for procurement management.

Third, while the NOPR suggests that the Commission concern goes to CIP- and cyber security-related issues, the Trade Associations have concern that the use of the term "industrial control systems" suggests that supply chain requirements could in this docket or in the future expand to include, for example, fuel procurement and delivery, or system protection devices. The Trade Associations seek clarification that the Commission does not intend for NERC to broadly address "industrial control systems" but limits its interest to CIP and cybersecurity – related supply chain matters. Should the Commission direct NERC to develop mandatory requirements, clarification of these issues in the final order will serve to inform how companies consider the issues in the standards development project.

In light of this background and context, the Trade Associations have difficulty envisioning the reliability risks unique to supply chain procurement that are not already addressed in CIP V5, and the structure and content of mandatory requirements that might address those risks. Moreover, the implementation of such requirements will be problematic to the extent that the exposure of strategic business practices by jurisdictional companies, including the specific risk management sensitivities, must remain confidential. In addition, many public power utilities would have to comply with state and local government procurement rules.

While the Trade Associations do not share the Commission's view of the reliability gap in terms of supply chain management risks, should the record lead the Commission to find that

NERC must develop mandatory requirements in the reliability standards, the Trade Associations seek Commission endorsement of the following structural and procedural principles in consideration of the directive it issues to NERC:

- develop a specific risk or threat basis
- recognize existing mandatory requirements and address only the defined gap between the threat basis and existing requirements
- set threshold boundaries for the scope of assets covered as some subset of the CIP V5 high impact asset category
- explicitly recognize that NRC procurement requirements are an inappropriate model for a FERC approach to CIP-cyber supply chain issues
- recognize the limits of Commission authority, including the inability to indirectly regulate third-party suppliers and vendors
- consider CIP-014-2 (physical security) and FAC-003-3 (vegetation management) as a potentially appropriate templates for mandatory requirements
- prior to issuing a directive and as stated in the NOPR, ensure that FERC staff conducts extensive outreach to understand the issues and sensitivities

FAC-003-3 (vegetation management) offers a potentially helpful template for consideration for several reasons. FAC-003-3 addresses a clearly defined reliability risk, purpose and scope, and performance expectations, implicitly recognizes widely varying facts and

circumstances, and system configurations, and avoids requiring prescriptive processes or methods for vegetation management.

CIP-014-2 (physical security) can also provide a useful example, where the standard allows companies to identify those critical facilities most in need of stronger protections, and requires companies to document their internal processes and controls for managing physical protection of identified critical facilities.

Neither FAC-003-3 nor CIP-014-1 explicitly informs issues involving the critical sensitivity of business proprietary or strategic contractual matters involved in contract discussions that take place between Responsible Entities and third-party vendors, or methods for ensuring that strict confidentiality must be maintained for such matters. While CIP-014-2 offers some protections for sensitive information by ensuring that such information remains on company premises, the Trade Associations urge the Commission to recognize these issues in its consideration of a potential directive.[37]

The NOPR also seeks comments on potential timeline for developing new or modified supply chain reliability requirements.[38] The Trade Associations envision that the project would require at least one year to achieve a successful ballot outcome from the date of a final Commission order in this docket. Several reasons support this general view: full consideration of the complex and unique nature of the issues, the need for comprehensive mapping of existing mandatory NERC requirements against the NIST framework, defining appropriate scope and

[37] Section 1.1.4 of the compliance monitoring process section of CIP-014-2 states the following confidentiality provision: "To protect the confidentiality and sensitive nature of the evidence for demonstrating compliance with this standard, all evidence will be retained at the Transmission Owner's and Transmission Operator's facilities."
[38] NOPR at P. 66.

purpose, appropriately structuring mandatory requirements for a new standard topic area to ensure alignment with scope, while ensuring enforceability, whether through modifications to existing standards or development of new standards, compliance measures, and implementation requirements, and the need to effectively communicate the project throughout the electric industry.

In light of the issues raised in these comments, the Trade Associations agree with the Commission on the necessity for Commission staff to conduct outreach activities.[39] After the submission of comments, the Trade Associations recommend that the Commission hold at least one staff technical workshop or conference and to do so prior to issuing a final order in this docket. Such an activity could provide an important venue to identify and discuss a broad range of policy and technical issues, and include jurisdictional companies, third-party suppliers of products and services, and federal and state agencies with relevant authorities and expertise.

## CONCLUSION

**WHEREFORE**, for the foregoing reasons, the Trade Associations respectfully request that the Commission approve the revised CIP standards as proposed by NERC in this proceeding and ensure that any future action ordered as a result of this proceeding is consistent as discussed above.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

*/s/ James P. Fama*
Edison Electric Institute
James P. Fama

[39] See NOPR P. 66

Vice President, Energy Delivery
Edison Electric Institute
Washington, D.C. 20004
202-508-5000

LARGE PUBLIC POWER COUNCIL

*/s/ Jonathan D. Schneider*
STINSON LEONARD STREET LLP
1775 Pennsylvania Avenue NW, Suite 800
Washington, D.C. 20006
(202) 728-3034
jonathan.schneider@stinsonleonard.com

AMERICAN PUBLIC POWER ASSOCIATION

*/s/ Allen Mosher*
Vice President, Policy Analysis
*/s/ Randolph Elliott*
Regulatory Counsel
2451 Crystal Drive, Suite 1000
Arlington, VA 22202
202-467-2900
amosher@publicpower.org
relliott@publicpower.org

ELECTRIC POWER SUPPLY ASSOCIATION

*/s/ Nancy Bagot, Vice President of Regulatory Affairs*
Jack Cashin, Director of Regulatory Affairs
Electric Power Supply Association
1401 New York Avenue, NW, 12th Floor
Washington, DC 20005
(202) 628-8200

ELECTRICITY CONSUMERS RESOURCE COUNCIL

*/s/ John P. Hughes*
John P. Hughes
Vice President, Technical Affairs
1101 K Street, NW, Suite 700
Washington, DC 20005

*jhughes@elcon.org*
*/s/ W. Richard Bidstrup*
Cleary Gottlieb Steen & Hamilton LLP
2000 Pennsylvania Avenue, NW, Suite 600
Washington, DC 20006
*Counsel to ELCON*
rbidstrup@cgsh.com
202-974-1500

TRANSMISSION ACCESS POLICY STUDY GROUP

*/s/ Cynthia S. Bogorad*
Latif M. Nurani
Spiegel & McDiamid LLP
1875 Eye Street, NW
Suite 700
Washington, DC 20005
202-879-4000
Attorneys for Transmission Access Policy Study Group

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

*/s/ Paul M. Breakman*
Paul M. Breakman, Assoc. Director- Regulatory Counsel
Barry R. Lawson, Assoc. Director, Power Delivery and Reliability
National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
paul.breakman@nreca.coop
barry.lawson@nreca.coop
703-907-5844

Dated: September 21, 2015

# Appendix 1

| NIST CYBER SECURITY FRAMEWORK | | | NIST Security Controls | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Function** | **Category** | **Subcategory** | **Reference to NIST 800-53 Rev 4** | **Included in NIST SP 800-161 Overlay** | **RelatedCIP V5 Requirement** | **CIP V5 Control Provides Risk Control for Supply Chain** | **CIP V5 Control Applicability Could be Extended to Supply Chain Within Organization** | **How existing CIP V5 mitigates Supply Chain Risk with no modification to applicaility.** |
| IDENTIFY (ID) | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. | **ID.AM-1**: Physical devices and systems within the organization are inventoried | CM-8 | Y | 2 | N | Y | |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | CM-8 | Y | 2,10 | N | Y | |
| | | **ID.AM-3:** Organizational communication and data flows are mapped | AC-4, CA-3, CA-9, PL-8 | Y | 2 | N | Y | |
| | | **ID.AM-4:** External information systems are catalogued | AC-20, SA-9 | Y | 5 | N | Y | |
| | | **ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | CP-2, RA-2, SA-14 | Y | 2 | N | Y | |
| | | **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and | CP-2, PS-7, PM-11 | 31<br>Y | 4 | N | Y | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | third-party stakeholders (e.g., suppliers, customers, partners) are established | | | | | | |
| | **Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. | **ID.BE-1:** The organization's role in the supply chain is identified and communicated | CP-2, SA-12 | Y | 10 part 3.3 | N | Y | |
| | | **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | PM-8 | N | 3 | N | N | |
| | | **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | PM-11, SA-14 | Y | 2,3 | N | Y | |
| | | **ID.BE-4**: Dependencies and critical functions for delivery of critical services are established | CP-8, PE-9, PE-11, PM-8, SA-14 | Y | 2,6 | N | N | |
| | | **ID.BE-5**: Resilience requirements to support delivery of critical services are established | CP-2, CP-11, SA-14 | Y | 2,6,8,9, | N | N | |
| | **Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. | **ID.GV-1:** Organizational information security policy is established | -1 controls from all families | | 3 | Y | Y | Organizational Policy establishes approach to protecting BES Cyber Systems. Process of testing for vulnerabilities and configuration management at the time of connecting a cyber asset to a critical network provides a control for supply chain risk. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **ID.GV-2:** Information security roles & responsibilities are coordinated and aligned with internal roles and external partners | PM-1, PS-7 | Y | 3,4 | Y | Y | Employees involved with modification to the critical network are designated. This prevents unauthorized connection of new types of equipment to the critical network |
| | | **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | -1 controls from all families (except PM-1) | | 3 | N | N | |
| | | **ID.GV-4**: Governance and risk management processes address cybersecurity risks | PM-9, PM-11 | Y | 3 | Y | Y | Tiering of BES Cyber Systems by NERC Standards establishes the risk tolerance. These tiers influence the security controls applied. |
| | **Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. | **ID.RA-1:** Asset vulnerabilities are identified and documented | CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 | Y | 2,5,6,7,10 | Y | Y | NERC standards address vulnerabilities, including supply chain risk. Testing for vulnerabilities and configuration management at the time of connecting a cyber asset to a critical network provides a control for supply chain risk. |
| | | **ID.RA-2:** Threat and vulnerability information is received from information sharing forums and sources | PM-15, PM-16, SI-5 | Y | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **ID.RA-3:** Threats, both internal and external, are identified and documented | RA-3, SI-5, PM-12, PM-16 | Y | | | | |
| | | **ID.RA-4:** Potential business impacts and likelihoods are identified | RA-2, RA-3, PM-9, PM-11, SA-14 | Y | 8,9 | Y | Y | Tiering of BES Cyber Systems by NERC Standards establishes the risk tolerance. These tiers influence the security controls applied. The Process of testing for vulnerabilities and configuration management at the time of connecting a cyber asset to a critical network provides a control for supply chain risk. In addition, security event monitoring, and response and Recovery mitigate the impact of a security event. |
| | | **ID.RA-5**: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | RA-2, RA-3, PM-16 | Y | 2 | Y | Y | Tiering of BES Cyber Systems by NERC Standards establishes the risk tolerance. These tiers influence the security controls applied. |
| | | **ID.RA-6:** Risk responses are identified and prioritized | PM-4, PM-9 | N | | | | |
| | **Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and | **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders | PM-9 | N | 2 | Y | Y | Tiering of BES Cyber Systems by NERC Standards establishes the risk tolerance. These tiers influence |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | assumptions are established and used to support operational risk decisions. | | | | | | | the security controls applied. |
| | | **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed | PM-9 | N | 2 | Y | Y | Tiering of BES Cyber Systems by NERC Standards establishes the risk tolerance. These tiers influence the security controls applied. |
| | | **ID.RM-3**: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | PM-8, PM-9, PM-11, SA-14 | Y | 2 | Y | Y | Tiering of BES Cyber Systems by NERC Standards establishes the risk tolerance. These tiers influence the security controls applied. |
| PROTECT (PR) | **Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. | **PR.AC-1:** Identities and credentials are managed for authorized devices and users | AC-2, IA Family | Y | 4,6,7 | N | Y | |
| | | **PR.AC-2:** Physical access to assets is managed and protected | PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 | Y | 4,6 | N | Y | |
| | | **PR.AC-3:** Remote access is managed | AC-17, AC-19, AC-20 | Y | 4,5 | N | Y | |
| | | **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties | AC-2, AC-3, AC-5, AC-6, AC-16 | Y | 4,7 | N | Y | |
| | | **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate | AC-4, SC-7 | Y | 5 | Y | Y | Critical Network is segmented from the corporate network. This prevents the introduction of malicious code to the |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | critical network from a development system. |
| | **Awareness and Training (PR.AT):** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. | **PR.AT-1:** All users are informed and trained | AT-2, PM-13 | N | 4 | Y | Y | Persons with cyber access are trained to understand the criticality of BES Cyber Systems and the need to prevent the introduction of threats to the critical environment. This prevents unauthorized connection of cyber assets to the critical network. |
| | | **PR.AT-2:** Privileged users understand roles & responsibilities | AT-3, PM-13 | N | 4 | Y | Y | Persons with cyber access are trained to understand the criticality of BES Cyber Systems and the need to prevent the introduction of threats to the critical environment. This prevents unauthorized connection of cyber assets to the critical network. |
| | | **PR.AT-3:** Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities | PS-7, SA-9 | Y | 5 | N | N | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **PR.AT-4:** Senior executives understand roles & responsibilities | AT-3, PM-13 | N | 3 | Y | Y | CIP-003 requires a Senior Manager to oversee the program. By implementing the NERC requirements and organizational policy to protect the critical network, the supply chain threat is mitigated. |
| | | **PR.AT-5:** Physical and information security personnel understand roles & responsibilities | AT-3, PM-13 | N | 4 | Y | Y | Persons with cyber access are trained to understand the criticality of BES Cyber Systems and the need to prevent the introduction of threats to the critical environment. This prevents unauthorized connection of cyber assets to the critical network. |
| | **Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | **PR.DS-1:** Data-at-rest is protected | SC-28 | Y | 5,6,11 | Y | Y | BES Cyber System Information is required to be protected by CIP-011 whether on a BES Cyber Asset or a developmental system. |
| | | **PR.DS-2:** Data-in-transit is protected | SC-8 | y | | | | |
| | | **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition | CM-8, MP-6, PE-16 | Y | 10,11 | Y | Y | The process of testing for vulnerabilities and configuration management at the time of connecting a cyber asset to a critical network provides a |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | control for supply chain risk. |
| | | **PR.DS-4:** Adequate capacity to ensure availability is maintained | AU-4, CP-2, SC-5 | Y | | | | |
| | | **PR.DS-5:** Protections against data leaks are implemented | AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 | Y | | | | |
| | | **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity | SI-7 | Y | | | | |
| | | **PR.DS-7:** The development and testing environment(s) are separate from the production environment | CM-2 | Y | 10 | Y | Y | Where technically feasible, prior to adding a cyber asset to a High Impact BES Cyber Systems an active vulnerability assessment must be performed. |
| | **Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and | **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained | CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10 | Y | 10 | Y | Y | The baseline configuration at the time of connection allows an entity to verify the software on the newly supplied cyber asset is the inventory the vendor indicated belongs on the asset. This includes open ports and active services. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | procedures are maintained and used to manage protection of information systems and assets. | **PR.IP-2:** A System Development Life Cycle to manage systems is implemented | SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8 | Y | | | | |
| | | **PR.IP-3:** Configuration change control processes are in place | CM-3, CM-4, SA-10 | Y | 10 | Y | Y | |
| | | **PR.IP-4:** Backups of information are conducted, maintained, and tested periodically | CP-4, CP-6, CP-9 | Y | 9 | Y | N | A robust recovery process serves as a means to recover from a threat introduced from the supply chain. |
| | | **PR.IP-5:** Policy and regulations regarding the physical operating environment for organizational assets are met | PE-10, PE-12, PE-13, PE-14, PE-15, PE-18 | N | | | | |
| | | **PR.IP-6:** Data is destroyed according to policy | MP-6 | Y | 11 | N | N | |
| | | **PR.IP-7:** Protection processes are continuously improved | CA-2, CA-7, CP-2, IR-8, PL-2, PM-6 | N | | | | |
| | | **PR.IP-8:** Effectiveness of protection technologies is shared with appropriate parties | AC-21, CA-7, SI-4 | y | | | | |
| | | **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | CP-2, IR-8 | Y | 8,9 | Y | Y | Response and recovery plans serves as a means to recover from a threat introduced from the supply chain. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **PR.IP-10:** Response and recovery plans are tested | CP-4, IR-3, PM-14 | N | 8,9 | Y | Y | Response and recovery plans serves as a means to recover from a threat introduced from the supply chain. |
| | | **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) | PS Family | Y | 4 | Y | Y | Personnel Risk Assessment are performed for persons with access to BES Cyber Systems. These are the persons who verify a new cyber asset security prior to connection. |
| | | **PR.IP-12:** A vulnerability management plan is developed and implemented | RA-3, RA-5, SI-2 | Y | 10 | Y | Y | The process of testing for vulnerabilities and configuration management at the time of connecting a cyber asset to a critical network provides a control for supply chain risk. Where technically feasible, prior to adding a cyber asset to a High Impact Bes Cyber Systems an active vulnerability assessment must be performed. |
| | **Maintenance (PR.MA):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures. | **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | MA-2, MA-3, MA-5 | Y | 10 | Y | Y | The process of testing for vulnerabilities and configuration management at the time of connecting a cyber asset to a critical network provides a control for supply chain risk. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | MA-4 | Y | 5,10 | N | N | |
| | **Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. | **PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | AU Family | Y | 7 | Y | N | Audit logs allow for after the fact investigation of incidents to BES Cyber Systems |
| | | **PR.PT-2:** Removable media is protected and its use restricted according to policy | MP-2, MP-4, MP-5, MP-7 | N | 10 | N | Y | |
| | | **PR.PT-3:** Access to systems and assets is controlled, incorporating the principle of least functionality | AC-3, CM-7 | Y | 4 | Y | Y | Prevents supply chain integrators from interacting with BES Cyber Systems. |
| | | **PR.PT-4:** Communications and control networks are protected | AC-4, AC-17, AC-18, CP-8, SC-7 | Y | 5,6 | Y | Y | The Network within a critical ESP is protected with electronic points preventing external cyber assets. Physical access controls prevent physical access to BES Cyber System. |
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of | **DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed | AC-4, CA-3, CM-2, SI-4 | Y | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | events is understood. | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | AU-6, CA-7, IR-4, SI-4 | Y | 7 | Y | Y | BES Cyber System Security events that indicated a security incident are reported to personnel. If a a newly connected asset causes a security event the BES Cyber System detects it. |
| | | **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors | AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 | Y | | | | |
| | | **DE.AE-4:** Impact of events is determined | CP-2, IR-4, RA-3, SI -4 | Y | 7,8 | Y | Y | Response and recovery plans serves as a means to recover from a threat introduced from the supply chain. |
| | | **DE.AE-5:** Incident alert thresholds are established | IR-4, IR-5, IR-8 | Y | 7,8 | Y | Y | Response and recovery plans serves as a means to recover from a threat introduced from the supply chain. |
| | **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. | **DE.CM-1:** The network is monitored to detect potential cybersecurity events | AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4 | Y | 7,8 | Y | Y | Response and recovery plans serves as a means to recover from a threat introduced from the supply chain. |
| | | **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events | CA-7, PE-3, PE-6, PE-20 | Y | 6 | N | Y | |
| | | **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events | AC-2, AU-12, AU-13, CA-7, CM-10, CM-11 | Y | 7 | N | Y | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **DE.CM-4:** Malicious code is detected | SI-3 | N | 7 | Y | Y | If a newly connected cyber asset introduces malicious code then malicious code detection in the BES Cyber System will detect or deter it. |
| | | **DE.CM-5:** Unauthorized mobile code is detected | SC-18, SI-4. SC-44 | Y | 5,7 | Y | Y | If a newly connected cyber asset introduces malicious code, malicious code detection in BES Cyber System will detect or deter. |
| | | **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events | CA-7, PS-7, SA-4, SA-9, SI-4 | Y | 5 | N | N | |
| | | **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed | AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 | Y | 7 | | N | |
| | | **DE.CM-8:** Vulnerability scans are performed | RA-5 | N | 10 | | | Where technically feasible, prior to adding a cyber asset to a High Impact BES Cyber Systems an active vulnerability assessment must be performed. In addition annual cyber vulnerability assessments are performed. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. | **DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability | CA-2, CA-7, PM-14 | Y | 7 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | | **DE.DP-2:** Detection activities comply with all applicable requirements | CA-2, CA-7, PM-14, SI-4 | Y | 7 | N | N | |
| | | **DE.DP-3:** Detection processes are tested | CA-2, CA-7, PE-3, PM-14, SI-3, SI-4 | Y | | | | |
| | | **DE.DP-4:** Event detection information is communicated to appropriate parties | AU-6, CA-2, CA-7, RA-5, SI-4 | Y | 7 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | | **DE.DP-5:** Detection processes are continuously improved | CA-2, CA-7, PL-2, RA-5, SI-4, PM-14 | Y | | | | |
| **RESPOND (RS)** | **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events. | **RS.RP-1:** Response plan is executed during or after an event | CP-2, CP-10, IR-4, IR-8 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | **Communications (RS.CO):** Response activities are coordinated with internal and external | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | CP-2, CP-3, IR-3, IR-8 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | stakeholders, as appropriate, to include external support from law enforcement agencies. | **RS.CO-2:** Events are reported consistent with established criteria | AU-6, IR-6, IR-8 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | | **RS.CO-3:** Information is shared consistent with response plans | CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans | CP-2, IR-4, IR-8 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | PM-15, SI-5 | N | EOP-004 | | | |
| | **Analysis (RS.AN):** Analysis is conducted to ensure adequate response and support recovery activities. | **RS.AN-1:** Notifications from detection systems are investigated | AU-6, CA-7, IR-4, IR-5, PE-6, SI-4 | Y | 8 | Y | N | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | | **RS.AN-2:** The impact of the incident is understood | CP-2, IR-4 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | | **RS.AN-3:** Forensics are performed | AU-7, IR-4 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **RS.AN-4:** Incidents are categorized consistent with response plans | CP-2, IR-4, IR-5, IR-8 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | **Mitigation (RS.MI):** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. | **RS.MI-1:** Incidents are contained | IR-4 | Y | 8 | Y | Y | Response and recovery plans serves as a means to recover from a threat introduced from the supply chain. |
| | | **RS.MI-2:** Incidents are mitigated | IR-4 | Y | 8 | Y | Y | |
| | | **RS.MI-3:** Newly identified vulnerabilities are mitigated or documented as accepted risks | CA-7, RA-3, RA-5 | Y | | | | |
| | **Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. | **RS.IM-1:** Response plans incorporate lessons learned | CP-2, IR-4, IR-8 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | | **RS.IM-2:** Response strategies are updated | CP-2, IR-4, IR-8 | Y | 8 | Y | Y | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| **RECOVER (RC)** | **Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. | **RC.RP-1:** Recovery plan is executed during or after an event | CP-10, IR-4, IR-8 | N | 9 | Y | N | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-1:** Recovery plans incorporate lessons learned | CP-2, IR-4, IR-8 | Y | 9 | Y | N | Response and recovery plans serves as a means to recover from a threat introduced from the supply chain. |
| | | **RC.IM-2:** Recovery strategies are updated | CP-2, IR-4, IR-8 | Y | 9 | Y | N | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |
| | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors. | **RC.CO-1:** Public relations are managed | | | | | | |
| | | **RC.CO-2:** Reputation after an event is repaired | | | | | | |
| | | **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams | CP-2, IR-4 | Y | 9 | N | N | Response and recovery plans serve as a means to recover from a threat introduced from the supply chain. |