UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

ADDITONAL COMMENTS OF THE EDISON ELECTRIC INSTITUTE, THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, THE ELECTRIC POWER SUPPLY ASSOCIATION, AND THE ELECTRICITY CONSUMERS RESOURCE COUNCIL

The Edison Electric Institute ("EEI"), the Electric Power Supply Association ("EPSA), the National Rural Electric Cooperative Association ("NRECA"), and the Electricity Consumers Resource Council ("ELCON" and collectively, the "Trade Associations") respectfully submit the following comments for consideration by the Commission in this docket. The Trade Associations offer these comments to supplement the record[1] in the light of the discussions that took place at the staff technical conference in Washington, D.C. on January 28, 2016 that further addressed the supply chain issues initially identified in the Notice of Proposed Rulemaking ("NOPR") issued by the Federal Energy Regulatory Commission ("FERC" or "Commission") on July 16, 2015. We respectively ask that the Commission accept these comments for the record and in determining the appropriate action on the supply chain risk issues identified in the NOPR.

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

EXECUTIVE SUMMARY

The January 28 technical conference added considerable insights into cybersecurity supply chain risk management challenges. For example, panelists representing the electric power industry at the conference affirmed that the CIP V5 mandatory requirements adequately address reliability risks introduced through the cybersecurity supply chain. Trade Associations appreciate careful consideration and continued discussion at the Commission on these complex issues, and respectively request that the Commission accept the following comments as part of the formal record of the docket.

As set forth in these comments, the Trade Associations understand the issues raised during the January 28 technical conference as focusing on methods to manage cybersecurity risk introduced by third party product and service vendors. Panelists emphasized that vendor risk management activities not already covered by the CIP V5 requirements involve contractual and third party business management matters that extend beyond the control of jurisdictional entities and Section 215 of the Federal Power Act. Panelists also raised significant concerns that additional mandatory CIP requirements could further increase business risk, procurement costs, and administrative burdens, and not reduce or mitigate reliability risks.

To meaningfully address these business risks, panelists identified several initiatives that will provide the best strategic path forward for the electric industry to enhance their vendor risk management practices and capabilities. The Trade Associations urge the Commission to look to these initiatives to provide strong and effective solutions to a broad range of vendor introduced risks, including embedded malware, defective or counterfeit devices, and comprehensive product testing. The Trade Associations believe that these initiatives are more likely to produce beneficial outcomes more effectively than new CIP requirements.

The Commission should allow time to observe existing and emerging vendor risk management initiatives and CIP V5 implementation, which will inform any decision to add or revise mandatory CIP requirements in the future.   Gathered experience will also enable the Commission to better understand and clearly identify the reliability risks it wants NERC to address that CIP V5 does not already address.

The conference also served to further underscore the recommendations the Trade Associations made in our initial filed comments, specifically that the Commission not direct NERC to develop new requirements or a new Reliability Standard to address vendor risk management. Instead, the Commission should allow CIP V5 implementation to mature and use the NERC compliance and enforcement process to evaluate whether there are potential gaps in the existing requirements. In addition, it remains very difficult to envision mandatory requirements with meaningful protections that could simultaneously avoid having the legally dubious effect of indirectly regulating third-party vendors and suppliers through jurisdictional entities.

COMMENTS

I. The Commission should allow vendor risk management initiatives to mature and inform future actions regarding CIP requirements.

We strongly encourage the Commission to recognize new collaborative initiatives as offering the most effective approach to the supply chain cyber asset procurement issues. Various vendor risk management initiatives were discussed at the January 28 technical conference; and while these programs are new and only beginning to develop, they hold strong promise for collaborative actions, where government agencies, vendors and suppliers, and utility customers of various products and services can identify and put in place practical solutions for supply chain

–types of risks. For example, the Energy Sector Critical Manufacturing Working Group ("ESCMWG") is a joint effort of the Department of Energy, the Department of Homeland Security, the Energy Sector, and the Critical Manufacturing Sector. Briefly mentioned on January 28, this group is new and has already attracted strong support and participation from responsible entities and their vendors. This group brings together electricity, oil, and natural gas asset owners and operators with the vendors who manufacture their cyber systems to evaluate the security and integrity of delivering devices, equipment, and services that support the Nation's energy infrastructure. This cybersecurity supply chain-focused effort will provide a forum for asset owners and manufacturers to discuss critical issues that may impact the energy sector, and provide recommendations and tools for areas of improvement. The Trade Associations view this approach as the most effective venue for dealing broadly with business risks in cyber asset procurement.

In addition, the Commission should monitor the development and availability of certification programs, including for example the ISASecure and the new UL Cybersecurity Assurance Program.[2] Vendor certification programs promise significant advantages for vendors and jurisdictional entities, who neither own nor operate testing facilities, or have limited testing capabilities. Moreover, the Commission should monitor the development and evolution of other industry and government procurement guidelines and seek informal discussion or informational filings that provide status reports on these initiatives. As these and other initiatives form and mature, the Commission can seek to remain informed through informal meetings with the sponsoring entities and participants.

[2] www.ul.com/cybersecurity

II. CIP V5 adequately addresses system reliability risks associated with the supply chain that are within the control of Registered Entities.

As stated in the Trade Associations comments filed in September 2015, we disagree with the Commission's characterization that the referenced ICS-CERT alerts indicate a changed threat landscape that reveals a reliability gap and disagree that these campaigns are "based on the injection of malware while a product or service remains in the control of the hardware or software vendor."[3] We note that these malware campaigns are already addressed by CIP V5. For example, protection against the introduction of malware via the supply chain such as watering hole attacks where entities obtain code (patches/updates/new releases) from a vendor that has been compromised include:

- Patch sources must be monitored monthly for new patches to vulnerabilities.
- Every change of code that affects the baseline configuration of medium and high impact systems must be authorized and tested for potential changes to cyber security controls such as new ports or services opened, new accounts added, etc. prior to the change.
- Each medium and high system must have documented malware controls in place that also require the mitigation of any malware found. Signature updates must be tested as well.
- In many instances, new code is moved to these systems via removable media. CIP V5 includes malware scans on removable media usage before connection to medium and high systems.
- For high impact systems, each cyber asset must have an active vulnerability assessment before being added to the production environment.
- High and medium impact systems must have an annual vulnerability assessment, and for high impact systems it must be an active vulnerability assessment every 3 years.
- Logging of events that could signal a cyber security incident is required to allow for detection of malware. Included are all instances of detected malware and all successful and unsuccessful login attempts.
- Detection of malware requires alerts to be generated.
- Malware that tries to communicate to a command-and-control server should be caught at

[3] 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, *filed* September 21, 2015, p.20-21.

the Electronic Security Perimeter and the required Electronic Access Points. Electronic Access Points now require deny by default with business reasons for each existing outbound rule. This was added precisely because this is a prime way to detect malware that has made it into the environment and is trying to "phone home."

- For high impact systems, there must be one or more methods for detecting known or suspected malicious communications both inbound and outbound, such as intrusion detection/prevention systems.
- Incident response plans and recovery plans (including tested backups) are required to speed recovery.

Likewise, CIP V5 protections against the introduction of malware via supply chain physical access to systems include:

- All medium and high systems must have an access controlled Physical Security Perimeter with monitoring, logging, and alerting and anyone with unescorted access must have a background check and training before physical access is allowed to the systems. Anyone without such access must have a continuous escort.
- Any transient cyber assets used to connect to a medium or high system must meet a documented cyber security plan that includes malware controls and patching.
- Any removable media used to connect to a medium or high system must be scanned for malware and mitigated if any is found before connection to such system.

In addition, CIP V5 protections against the introduction of malware by supply chain remote access include:

- In addition to the controls listed above for code and configuration changes from the supply chain, interactive remote access to medium and high systems now must meet the Interactive Remote Access controls. These controls are designed, through the use of Intermediate Systems, to prevent direct access to the applicable systems at a routable protocol level. This prevents anyone from running network sweeps or vulnerability scanners from their remote machine to discover vulnerable systems and "pivot" to them.
- All interactive remote access must be encrypted while outside the ESP. This protects the data in motion from the remote supply chain vendor to the system.
- All interactive remote access must use two factor authentication. Malware can log keystrokes and capture account names and passwords, so all interactive remote access must use other factors before access is granted. This includes anyone accessing the system from the supply chain.
- One of the ICS-CERT alerts mentioned in paragraph 63 concerned Internet connected systems which could have malware installed. For medium and high systems, CIP-005 requires an Electronic Security Perimeter. With V6, even all low impact systems require a Low Electronic Access Point with inbound and outbound rules. The guidance states one of the major factors behind this requirement is to prevent all applicable systems of any impact level from having direct Internet connectivity.
- Any dialup access to applicable systems must have authentication.

We also note that these malware campaigns were not a focus in the January 28 technical conference. Instead, during the conference, various panelists described supply chain risk as the risk introduced by third parties that provide products and services used by the bulk-power system. These risks include: embedded malware in products, defective or counterfeit devices, and vulnerabilities in products delivered. This risk is not new or unique to the bulk electric system and the Trade Associations maintain that CIP V5 adequately addresses these risks.[4]

In the NOPR, the Commission rightly acknowledged that that "security controls for supply chain management will likely vary greatly with each responsible entity due to variations in individual business practices" and points to nine NIST supply chain management security controls as "instructional to the development of any new reliability standard" to address supply chain risk management.[5] However, based on further analysis of these NIST controls and the CIP V5 requirements, we believe that under the scope of the Commission's jurisdiction,[6] the existing CIP V5 requirements already meet these NIST controls.

In understanding the NIST supply chain controls, it is important to start with the NIST SP 800-161 definition of supply chain: "the integrated set of components (hardware, software, and processes) within the organizational boundaries that composes the environment in which a system is developed or manufactured, tested, deployed, maintained and retired/decommissioned."[7] In this definition, NIST scopes activities to those within the organizational boundary. The lifecycle of industrial control systems, which includes research,

[4] *See* Initial filed comments included attachment, summary description mapping CIP V5 to NIST 161.

[5] NOPR at ¶ 65.

[6] To approve and enforce reliability standards that "provide for reliable operation of the bulk-power system." 16 US § 824o.

[7] NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (April 2015) at 5, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

development, design, manufacturing, acquisition, delivery, integration, operations, retirement, and disposal, is not entirely within the organizational boundary of electric power utilities or responsible entities that own and operate the bulk-power system. The utility's environment or boundary in the supply chain is limited to acquisition, delivery, integration, operations, retirement, and disposal, and a utility's influence is limited in the acquisition, delivery, and disposal stages because third party suppliers play a key role in these stages.[8]

Below is a more detailed explanation for how each of the nine NIST supply chain controls suggested by the Commission in the NOPR is addressed by the CIP V5 requirements.

(1) Access Control Policy and Procedures (AC-1)[9]

The NIST AC-1 control guides organizations to include their access control policies in their agreements with their suppliers, system integrators and external service providers. This supplemental NIST SP 800-161[10] security control focuses on communicating the organization or responsible entity's access control policy to third parties. The NIST SP 800-53 AC-1 base control establishes the policy framework for implementing the AC family of access controls, which include physical and remote access, least privilege, and access enforcement. CIP V5 does not require organizations to specify and include access control policies in contracts or other agreements with their system integrators, suppliers, and external service providers. Instead, CIP V5 requires responsible entities to control access to BES Cyber Systems and associated cyber assets to remain compliant with the mandatory standards and have processes to monitor and enforce the access policy. How a responsible entity ensures these third parties are aware of and

[8] *See* Speaker materials of Jonathan Appelbaum, United Illuminating Company, at the CIP Supply Chain Risk Management Technical Conference, held January 28, 2016, under RM15-14-000.

[9] *Id*. at 55.

[10] NIST SP 800-161 includes supplemental supply chain controls that are an overlay to the NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organization*.

follow these policies (e.g., through contracts) is left up to the organization.[11] To be compliant with CIP V5 (i.e., control access), responsible entities have to make third parties aware of their access control policies, whether through formal agreements, informal agreements, training, access rules, or some other method. Because CIP V5 requires responsible entities to control access to their BES Cyber Systems, a new requirement focused on specifying their access control policies in contracts or other agreements would only prescribe additional compliance burdens without an impact on the reliability of the bulk-power system.

The physical and logical access controls in CIP V5 are found in the CIP-003-6 security policy requirements; the CIP-004-6 access management and access revocation requirements; the CIP-005-5 access permission requirements; the CIP-006-6 physical access, monitoring, logging, alerting, and testing requirements; the CIP-007-6 security event monitoring, authentication, and password requirements; and the CIP-010-2 Transient Cyber Asset (TCA) authorization requirements.

(2) Security Assessment and Authorization Policies and Procedures (CA-1)[12]

The NIST SP 800-53 CA-1 base control for security assessment is a control that requires the information system owner to assess the risk to a particular system and then evaluate which of the security controls should be deployed. CIP V5 does not possess an equivalent control because the family of CIP standards has taken the security assessment requirement from the responsible entity and assigned it to the NERC Standard development process.

[11] For example, the Version 5 Transition Advisory Group developed a lessons learned guidance document that describes various approaches that responsible entities have used to manage vendor access, which includes contract considerations and other access control methods. NERC Lesson Learned CIP Version 5 Transition Program Vendor Access Management, November 23, 2015, *available at:* http://www.nerc.com/pa/CI/tpv5impmntnstdy/Vendor%20Access%20Management%20Lesson%20Learned.pdf

[12] *Id*. at 65.

The NIST SP 800-161 CA-1 control (or CA-1 overlay) guides organizations to review the risks specific to their unique environment of suppliers, system integrators, and external service providers. The cybersecurity supply chain risks are embedded malware, product vulnerabilities, and unauthorized physical and remote access to cyber assets. When CIP V5 was developed, these risks were considered from the perspective of malicious insider and outsider threats. The threat from the cybersecurity supply chain is equivalent to the malicious insider and outside actor threats. As a result, an additional requirement to perform a security assessment considering the risks specific to their unique environment of suppliers, system integrators, and external service providers would be superfluous given the existing CIP V5 requirements.

For example, CIP V5 requirements are focused on personnel with physical or electronic access to BES Cyber Systems. The use of the term “personnel” is not limited to only responsible entity personnel, but includes anyone, even third parties, with physical or electronic access to BES Cyber Systems. Personnel without access have limited, if any, ability to impact BES Cyber Systems. Other CIP V5 requirements (e.g., CIP-007-6 security patch management requirements and malicious code prevention requirements) are designed to further reduce risk introduced by suppliers that do not have direct access to BES Cyber Systems.

(3) Configuration Management Policy and Procedures (CM-1)[13]

The CM-1 supplemental control guides organizations to integrate their configuration management policy into the configuration management policy of their suppliers, system integrators, and external service providers. CIP V5 does not require organizations to specify and include their configuration management policy in contracts or other agreements with their system integrators, suppliers, and external service providers. Instead, CIP V5 requires responsible

[13] *Id*. at 68.

entities to set configuration policy and have processes to monitor and enforce this policy to be compliant. How a registered entity ensures third parties are aware of and follow these policies (e.g., through contracts) is left up to the organization.

CM-1 also contains a statement that an organization should have procedures for introducing and removing components to and from their information system boundary. Specific configuration change management policy and procedures for introducing and removing components to and from BES Cyber Systems are specified in the CIP-010-2 configuration change management and monitoring requirements; the CIP-010-2 vulnerability assessments and Transient Cyber Assets requirements; and the CIP-011-2 reuse and disposal requirements. These requirements align with NIST SP 800-161 definition of supply chain because they apply to the environment within the organizational boundary of responsible entities, i.e., where BES Cyber Systems are deployed, maintained, and retired/decommissioned. Configuration change management policy and procedures in the earlier stages of the supply chain lifecycle of BES Cyber Systems (i.e., development, manufacturing, and testing) fall within the organizational boundaries of the manufacturers of the components of BES Cyber Systems. The ability of a responsible entity to oversee or control manufacturing policy and procedures is limited to what can be agreed upon during contract negotiations during the procurement process.

(4) Identification and Authentication Policy and Procedures (IA-1)[14]

The IA-1 control guides organizations to enhance their identity and access management policies to ensure that critical roles, systems, components, and processes are identified. This control focuses on two security objectives. The first objective is focused on the personnel of the suppliers, system integrators, and external service providers accessing the cyber assets of an

[14] *Id*. at 77.

organization. The second objective is focused on the identification and inventory of the equipment and software components of the suppliers, system integrators, and external service providers.

Regarding equipment and software components, CIP-002-5.1 requires registered entities to identify their systems, components, and processes that are critical to reliability of the bulk-power system using a bright-line rule. CIP V5 requires inventory of any cyber assets connected within the same electronic security perimeter (Protected Cyber Assets) and any transient cyber assets or removable media connected to BES Cyber Systems and associated cyber assets. Although an inventory of Protected Cyber Assets and other associated cyber assets is not specifically required by the CIP Standards, the inventory is necessary to demonstrate compliance to the mandatory CIP requirements. The inventory of software components is required by the CIP-010-2 configuration requirements. The requirement delineates the specific items required for baseline monitoring.

Regarding personnel, any person, which includes third parties, accessing cyber assets in the CIP program are required to have proper authorization and business need by CIP-004-6 and traceability by CIP-007-6.

(5) System Maintenance Policy and Procedures (MA-1)[15]

The MA-1 control guides organizations to ensure that supply chain concerns are included in maintenance policies and procedures. The security objective of this control is to reduce the risk when maintenance activity is provided by a supplier, system integrator, or external service provider. Maintenance activities can include the addition or removal of physical cyber assets, deployment of security patches, or other change and configuration activities. CIP V5 applies to

[15] *Id*. at 81.

the BES Cyber Systems identified by CIP-002-5.1 and all of the applicable CIP requirements apply to each BES Cyber System. Because the CIP requirements apply to the systems themselves, the responsible entity must demonstrate compliance with all of the requirements, which would include any maintenance to the systems. Remote access controls are included in CIP-003-6 for low impact BES Cyber Systems and CIP-005-5 for medium and high Impact BES Cyber Systems. Personnel that can have access to these systems is controlled by the physical and electronic access controls found in CIP-003-6, 006-6, 004-6, 005-5, 007-6, and 010-2 as described above. These controls apply to anyone with access to the BES Cyber System, including maintenance personnel that may be outsourced.

Each responsible entity determines the process whereby internal and external parties (e.g., contractors) adhere to these requirements (e.g., through contracts).

(6) Personnel Security Policy and Procedures (PS-1)[16]

The PS-1 control guides organizations to define the roles for personnel who manage and execute supply chain infrastructure security activities. Personnel roles are addressed by the access control requirements found in CIP-003-6, CIP-004-6, CIP-005-5, CIP-006-6, CIP-007-6, and CIP-010-2. These access controls are based on need, which is determined by roles and responsibilities of personnel.

(7) System and Services Acquisition Policy and Procedures (SA-1)[17]

The SA-1 control guides organizations to address changes of ownership, control, and requirements in their system and services acquisition policy. CIP V5 does not directly address monitoring vendors for changes in ownership; however, the CIP-007-6 patch management,

[16] *Id*. at 92.

[17] *Id*. at 98.

malicious code prevention, and security event monitoring requirements and the CIP-010-2 configuration change management, monitoring, and vulnerability assessments requirements require responsible entities to assess BES Cyber Systems prior to and during operation for security vulnerabilities, unauthorized configuration changes, and malware. These requirements are within the control of responsible entities (i.e., they are security activities within their organizational boundaries) and minimize reliability (and security) risk due to vulnerabilities and malware. It is unclear how new requirements focused on monitoring vendor ownership changes would impact reliability risk. Monitoring service providers with access (physical or electronic) to BES Cyber Systems could provide some benefit; however, this risk is addressed by the CIP-004-6 personnel risk assessment program requirements, which require the assessments to be performed for contractors and service vendors. These requirements are specific to the people that have access BES Cyber Systems rather than their organizations.

(8) Supply Chain Protection (SA-12)[18]

The SA-12 control is focused on acquisition practices and includes 15 control enhancements: acquisition strategies/tools/ methods, supplier reviews, limitation of harm, assessments prior to selection/acceptance/update, use of all-source intelligence, operations security, validate as genuine and not altered, penetration testing/analysis of elements, processes, and actors; inter-organizational agreements; critical information system components; identity and traceability; and processes to address weaknesses or deficiencies. These enhancements focus on the acquisition or procurement process, which is not addressed by CIP V5. As discussed during the technical conference, many of these control enhancements are being explored and tested, in different ways by responsible entities, which vary depending on risk and available resources. In

[18] *Id*. at 101.

reading the NIST SP 800-161 it is also important to remember that this guidance is focused on federal government procurements. Differences in federal and private sector procurements must be explored. For example, the buying power of the federal government is much different in size and types of products (e.g., different missions) than responsible entities. New CIP requirements focused on procurement is further addressed in the next section.

(9) Component Authenticity (SA-19)[19]

The SA-19 control is focused on anti-counterfeit policy and includes four control enhancements: anti-counterfeit training and scanning, configuration control for component service/repair; and component disposal. Anti-counterfeit controls such as training and scanning are something to consider if an organization purchased "brokered parts" or parts that are purchased from companies that do not manufacture them. It is also a manufacturer concern. BES Cyber System components are likely to be purchased from a manufacturer who specializes in manufacturing these systems. Therefore the risk of counterfeits impacting reliability is low. Also, CIP-010-2 requires that BES Cyber Systems must be tested before they are put into production to ensure that the CIP-005-5 and CIP-007-6 controls are not adversely affected. The CIP-007-6 security patch management requirements and CIP-010-2 configuration management and monitoring requirements address the NIST configuration control and component service/repair guidance for BES Cyber Systems. The CIP-011-2 asset reuse and disposal requirements address the component disposal guidance.

Both SA-12 and SA-19 help guide organizations to control risk introduced by vendors (e.g., suppliers, system integrators, service providers, and other third parties). Within section

[19] *Id*. at 107.

215 framework there remains the question as discussed further below whether FERC can regulate vendors through utility contracts. However, another way to address this risk is through the pre-connection activity and operational monitoring. This is the security control that CIP V5 provides. The impact of an exploitation of the vendor process is equipment that will not perform correctly, attempt to communicate incorrectly, or utilize services not authorized. The pre-connection CIP requirements of baseline configuration, disabling unneeded services and ports, and in the instance of new equipment connected to a high BES Cyber System, a cyber vulnerability assessment all provide a method to manage the risk. The CIP requirements for using an electronic access point to control routable communication and security monitoring assists in detecting improper connections. The malicious code prevention requirements provide another means to detect known exploits.

Based on this analysis, the Trade Associations are not aware of any supply chain-related reliability gaps in the CIP requirements. Instead of directing NERC to develop new requirements, we recommend that the Commission allow CIP V5 implementation to mature and use the NERC compliance and enforcement program to further evaluate whether there are potential gaps in the existing requirements that could not be identified by an analysis, are related to supply chain, and create reliability risk. The Commission should expect that NERC will provide timely reporting to Commission staff of any significant discoveries of potential gaps that may require further risk analyses and discussion. The Trade Associations also envision that Commission staff will proactively examine the records of enforcement actions filed at the Commission for any emerging patterns or trends. Commission staff could also monitor industry discussions at the NERC Critical Infrastructure Protection Committee on the issues. And finally, Commission staff could monitor reporting of relevant events analyses and disturbances for any evidence of problems or potential problems tied to cybersecurity-related causes.

III. New procurement requirements will have minimal, if any, impact on addressing reliability risk; will unnecessarily and unduly increase the compliance burden; increase business risk of Registered Entities; and will trigger jurisdictional questions for CIP and other Reliability Standards.

While some panelists at the January 28 technical conference suggested that the Commission establish new requirements aimed at cyber asset procurement processes, the Trade Associations believe that such requirements will have little, if any, positive impact on the reliability of the bulk-power system because CIP V5 already impacts responsible entity procurement and integration of new systems and devices used for the bulk-power system. Below are examples of ways CIP V5 enhances these areas of the supply chain lifecycle.

(1) Acquisition or Procurement of the System or Device

Although there is no explicit requirement that a responsible entity must consider the CIP V5 requirements during procurement, it will become more costly for a responsible entity to be compliant with CIP V5 if they wait later in the cybersecurity supply chain life cycle. The CIP V5 requirements strengthen the procurement process when writing and negotiating technical specifications and other contractual issues because entities must consider the requirements that will be placed on those systems before they make purchasing decisions. During procurement, a responsible entity must develop the technical specifications required for the system or device based on the configuration and use of that system or device. Appropriate contract language must be developed to ensure that the product received meets all contracted requirements and will allow the responsible entity to be compliant with CIP V5 during operations. Specifications that must be considered include:

- Physical and electronic access – the responsible entity must negotiate the appropriate language to allow for required personnel risk assessments and training prior to gaining access to covered systems including the use of Transient Cyber Assets and removable media as well as visitor management prior to access to the systems being granted.[20]
- Networked systems – the responsible entity will need to consider up front the network architecture and how it will fit within the entity's Electronic Security Perimeters and the access rules needed for any Electronic Access Points. Appropriate technical specifications must be developed to allow for these requirements to meet the NERC CIP Standards.[21]
- Remote Access – if remote access is required, the responsible entity will need to consider how two factor authentication will be accomplished with the vendor/supplier as well as how to architect access to Intermediate Systems with encryption.[22]
- Patches – the responsible entity will need to consider the source of any supply chain patches, how the vendor will release notifications of new patches and develop required testing environments in order to test the patches prior to installation.[23]
- Ports and Services – the responsible entity will need to determine with the vendor/supplier the necessary ports and services the system will require.[24]
- Logging and alerting capability – the responsible entity must specify the logging and alerting requirements of any applicable systems.[25]
- List of accounts and default passwords – the responsible entity must require the vendor/supplier to provide a list of all accounts on the supplied systems from the supply chain along with any default passwords.[26]
- Password capabilities – the responsible entity must require the vendor/supplier to meet the password capabilities of the system, including length, complexity, change interval, unsuccessful attempt lockouts, etc.[27]
- Backup and recovery capabilities – the responsible entity must specify the backup and recovery capabilities of the system and how such capabilities can be tested.[28]

[20] CIP-004-6

[21] CIP-005-5, Requirement R1

[22] CIP-005-5, Requirement R2

[23] CIP-007-6, Requirement R2

[24] CIP-007-6, Requirement R1

[25] CIP-007-6, Requirement R4.

[26] CIP-007-6, Requirement R5.

[27] *Id.*

[28] CIP-009-6.

- Baseline configuration – the responsible entity must require the vendor/supplier to provide a baseline configuration.[29]
- Information Protection – the responsible entity must contract with the provider/supplier as to the entity's requirements regarding information protection. This should include release of information requirements, destruction requirements, access requirements and storage location requirements.[30]

(2) Integration of the System or Device

During the integration phase of the supply chain life cycle, including implementation of the vendor product or service and prior to deployment in a live environment, the responsible entity must work with the vendor/supplier to ensure that the conditions of the contract are met and to ensure the performance of system/device meets contracted specifications. CIP V5 requirements that support these integration activities include:

- Physical and electronic access – during implementation, only those contractors with compliant backgrounds and required training will be allowed physical or electronic access to the system or device.[31]
- Remote Access – if remote access is required, two factor authentication will be employed for the vendor/supplier for Interactive Remote Access sessions utilizing encryption that terminates in an Intermediate System.[32]
- Vulnerability Assessment – the entity will need to consider how to mitigate the malware risk as the product is received and implemented and mitigate any malicious code found. If signature based malware controls are used, the entity needs to consider the method of updating those signatures from the supply chain. Prior to adding a new applicable Cyber Asset to a production environment, the entity must perform an active vulnerability assessment with the established baseline configuration and develop an action plan to mitigate vulnerabilities identified.[33]
- Default Passwords – per device capability known default passwords provided by the vendor/supplier must be changed by the entity.[34]

[29] CIP-010-2.

[30] CIP-011-2.

[31] CIP-004-6.

[32] CIP-005-5, Requirement R2.

[33] CIP-010-2, Requirement R3.

[34] CIP-007-6, Requirement R5.

- Information Protection - The entity must contract with the provider/supplier as to the entity's requirements regarding information protection. This should include release of information requirements, destruction requirements, access requirements and storage location requirements.[35]

During the technical conference, panelists voiced concern that new mandatory requirements focused on procurement could require entities to use specific cybersecurity contract language or to ensure third-party vendors strictly adhere to explicit cybersecurity terms and conditions. Because the CIP V5 requirements provide significant incentive for responsible entities to consider the CIP V5 requirements in acquisition and integration, new compliance requirements would only increase compliance burdens. Mandating contract language and terms will require responsible entities to provide evidence to auditors that they are meeting these new requirements in their procurements. Mandating contract terms also raises other issues, including the result would be indirect regulation of third parties that are not under the Commission's jurisdiction.

Contract term requirements may also give third party auditors (NERC, NERC Regional Entities, and FERC) influence into sensitive business areas (e.g., contract negotiations) that may raise anti-trust issues, conflict or impact with state contract laws, and require non-disclosure agreements. Such requirements may also put responsible entities at a disadvantage when it comes to contract negotiations with product and service providers because they must use the mandated procurement requirements and cannot negotiate with providers to find the best solutions specific to their environments. Often, such negotiations require balancing security, reliability, safety, availability, and other operational and business aspects that may be unique to

[35] CIP-011-2.

each responsible entity environment, which can be very complex depending on the product or service being acquired.

New mandatory requirements focused on the procurement process may also extend beyond the Commission's jurisdiction under Section 215, which could create a slippery slope for all of the CIP Standards as well as other Reliability Standards. Moreover, such requirements could significantly increase costs and shift liabilities for failures by third parties onto jurisdictional, responsible entities.

In light of the insights and observations gathered at the January 28 technical conference, well beyond the filing deadline for comments in this docket, the Trade Associations respectfully request that the Commission accept these additional comments for the record in determining the appropriate action on the supply chain risk issues. While the Trade Associations maintain strong convictions that that supply chain issues do not create a reliability gap in the CIP requirements, if the record leads the Commission to come to a different conclusion and to the identification of such a gap, then we continue to seek a focused directive and NERC project tailored to clearly defined reliability risks. Any directive should:

1. Be clear on the reliability risks it wants the drafting team to focus on, which are not already addressed by CIP V5.
2. Keep in mind the flexibility needed, especially during the procurement process, to manage vendor-introduced risk and consider a more flexible standard structure such as with CIP-014 and avoid prescriptive requirements
3. Limit the focus to CIP V5 BES Cyber Assets or Systems that are used by and located at facilities that qualify as HIGH impact per the methodology included in CIP-002-5.1 to balance compliance burden with reliability risk
4. Explicitly recognize jurisdictional limits and relieve jurisdictional entities of risks associated with liability for failures by third-party vendors

5. Allow at least one year for discussion, development, and approval by the NERC Board of Trustees

6. State explicitly that cybersecurity procurement requirements will not serve as precedent for development of mandatory requirements for other types of products or services, including for example fuel supply or critical power plant components.

7. Ensure that mandatory NERC standards, including CIP, define an enduring structure for risk-based performance against defined reliability risks. FERC should avoid seeking to address symptomatic issues in mandatory requirements, whether the latest malware or cyber "worm," as both inefficient and inappropriate. Within NERC, other venues and tools can and should provide more timely information and recommended actions, including E-ISAC and various NERC advisories.

CONCLUSION

WHEREFORE, for the foregoing reasons, the Trade Associations respectfully request that the Commission accept these comments for the record in its consideration of the issues and ensure that any future action ordered as a result of this proceeding is consistent as discussed above.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

/s/ David K. Owens, Executive Vice President, Business Operations
Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, D.C. 20004
202-508-5000

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

NATIONAL RURAL ELECTRIC
COOPERATIVE ASSOCIATION

/s/ 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

ELECTRICITY CONSUMERS RESOURCE
COUNCIL

/s/ John P. Hughes, Chief Executive Officer
Electricity Consumers Resource Council
1101 K Street, NW, Ste. 700
Washington, DC 20005
jhughes@elcon.org

Dated: April 21, 2016