BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI

In the Matter of the Establishment of a Working Case for the Writing of a New Rule on the Treatment of Customer Information by Commission Regulated Electric, Gas, Steam, Heating, Water, and Sewer Utilities and their Affiliates and Non-Affiliates.	)))))))	File No. AW-2018-0393

SUPPLEMENTAL RESPONSE TO DRAFT RULE

COME NOW Union Electric Company d/b/a Ameren Missouri ("Ameren Missouri"), Evergy Metro, Inc. d/b/a Evergy Missouri Metro and Evergy Missouri West, Inc. d/b/a Evergy Missouri West (Evergy Missouri Metro and Evergy Missouri West collectively, "Evergy"), (Ameren Missouri and Evergy collectively, "the Companies"), and submit to the Missouri Public Service Commission ("Commission") this *Supplemental Response to Draft Rule* ("*Initial Response*") addressing the proposed courses of action raised by the Commission's Staff ("Staff") in its September 16, 2019 filing, *Staff Draft Customer Information Rule* ("*Draft Rule*"). In of their position, the Companies state as follows:

As noted in its *Initial Response to Draft Rule* ("*Initial Response*"), Ameren Missouri feels that the best course of action is to continue the working case so that the proposed rule can continue to be refined. Evergy agrees with Ameren Missouri's position. Staff's rule is very sensitive to customer needs, which is understandable. The rule, however, does not necessarily go far enough in the classification of data types and may have some unintended consequences in its implementation. As noted in at page 15 of the presentation given by Janine Anthony Bowen at the October 9, 2018 workshop:

- Certain data is less sensitive than others;

- Certain uses are less sensitive and more useful than others; and
- Business realities and customer advantages are important.

The Companies have taken Staff's proposed rule and reconfigured certain aspects from an implementation standpoint to further classify data types and appropriate uses in light of business realities and customer advantages. Below, the Companies will walk through its alternate rule proposal with explanations of how they used or clarified Staff's rule as a basis.

20 CSR 4240-10.XXX Purpose Statement. The Companies softened portions of the Purpose Statement with regard to contractual requirements and a public-facing Privacy Policy for the reasons explained later in this pleading. The Companies believe this still appropriate expresses the intent of the rule.

2**0 CSR 4240-10.XXX(1) – Definitions**. The Companies did not make any revisions to Staff's proposed definitions for utility or customer information, as defined in (A) and (B). However, the Companies did propose revisions to the following definitions:

(C) Personal customer information. The Companies largely used Staff's definition, but added certain clarifications. For example, the Companies clarified that anonymized data and aggregated data would not be considered personal customer information.

(D) Anonymized customer data. While Staff discussed anonymized data conceptually, it did not include a definition. The Companies included a definition for clarity.

(E) Aggregated customer data. Based on Staff's proposed rule, it appeared to adopt language, in part, consistent with the Illinois "15/15" rule. The Companies have more fully fleshed out this definition to adopt that rule for use in Missouri.

(F) Utility-related services. The Companies began with Staff's proposed definition, and provided clarification that certain activities would clarify as utility-related service, e.g., customer service enhancement activities, enforcement of tariff provisions, service usage studies, collection activities for purchase of services, etc. If, for example, a utility needed to enter into a contract for collection activities on past-due accounts, or for the study of potential energy efficiency offerings to customer classes, those contracts should be considered tied to the provision of utility services.

(G) Utility service usage data. The Companies defined this term, which is used in the definition of "customer information," to avoid any confusion about what customer usage is.

20 CSR 4240-10.XXX(2) – Customer Information. The Companies revised Staff's proposals regarding the treatment of customer information to achieve greater clarity of when certain activities or protections would be required, and to acknowledge that certain contract provisions are subject to negotiation based on the type of data being handled. While Staff divided its proposed rule between utility-related and nonutility-related services provided, the Companies thought additional clarification of the differences, and acknowledgement of the commonalities, between the two were warranted. The remaining portions of (2) describe the terms under which non-anonymized and non-aggregated

information can be provided to others. The specific aspects of the Companies' suggestions are described below.

(A) *Anonymized and aggregated data.* The Companies added this provision to clarify that anonymized and aggregated customer data may be provided to others without customer consent since no customer can be identified through its disclosure. This will be helpful in several ways. For example, if EPRI is conducting a study of electric vehicle charging usage by state, a utility could anonymize or aggregate the data and provide it to EPRI for study. Or, if a utility is presenting a discussion of energy efficiency measures and would like to use a specific example to demonstrate the benefits, it could do so without customer consent so long as there was no way to identify the customer.

(B) *Internal treatment of data.* The Companies drafted this first section to acknowledge that their own personnel may require access to certain components of customer information during the normal course of business.

(C) *Provision of nonutility services.* The Companies propose this section to address apparent Staff concerns regarding a utility's provision of customer data when nonutility services are provided. In this section, the Companies have provided for the acknowledgement of customer consent when non-anonymized personal customer information must be provided to affiliates or third-party nonaffiliates. Further, given certain limitations on existing electronic systems, rather than require recorded or written proof of each individual customer consent, the Companies have provided for the ability to demonstrate customer consent was received. For example, many of Ameren Missouri's existing IT structures provide notice to

customers as they fill out electronic forms. However, Ameren Missouri's IT structures are typically not built to specifically log that particular customer's assent. Instead, the form is built electronically with the notice, and by filling out the form via that format, consent is given. While this is not an explicit logging of the consent, the customer, by the very nature of the electronic application, cannot participate unless they complete the application containing that notice. This level of demonstration, under existing laws in Missouri, is sufficient.

This section also provides that utility contracts with affiliates and third-party nonaffiliates for nonutility services must also comply with subsection (D), described below.

(D) *Utility services.* This section provides that, when a utility contracts with an affiliate or third-party nonaffiliate for the provision of utility-related services, it may provide non-anonymized and non-aggregated customer data without customer consent only if it complies with subsection (D).

(E) *Contractual provisions.* Staff has expressed concerns with applicable contractual provisions addressing customer data in several recent cases, including the critical infrastructure security workshop in File No. EW-2015-0206. While the Companies appreciate Staff's concerns, utilities are still constrained in negotiating contracts by what the marketplace will allow. If contractual requirements are made too stringent, a utility may not be able to find a party who is willing to enter into a contract for the required services.

For example, even NERC has declined to require specific contractual provisions when it comes to the physical and cyber protection of North America's

power grid infrastructure. CIP-013-1, which will become effective in July 2020, still allows utilities to contract in accordance with the protections required by the relevant information and not in conformance with predetermined contractual provisions.[1] For example, CIP-013-1 R1 states that each affected entity "shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber systems…" While the standard states that the processes for these level of security risk sets expectations for what should be and need not be included in the supply chain risk management plan, it does not mandate any specific provisions. For example, CIP-13-1 R1.2 requires risk mitigation plans that include "One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable…" and then lists efforts regarding notification of vendor-identified incidents, coordination of responses to incidents, notification of access terminations, etc. The ultimate determination of what how to develop these processes and when certain levels of notification of disclosures are and are not applicable is left to the governed entities.

Because there are potentially varying regulatory requirements, system configurations, and other logistical or legal obligations for a utility's vendors, it is impractical - and in some cases impossible - to mandate certain contract provisions. Accordingly, consistent with NERC's upcoming implementation of CIP-013-1 addressing supply chain management, the Companies have proposed provisions that may be considered and reasonably pursued, but are not required, in the execution of contracts and non-disclosure agreements, including:

[1] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf

1. Limiting the use of the customer information to only the contracted service ;
2. Prohibiting the transfer of ownership and other proprietary rights to customer information;
3. Confidential treatment of customer information;
4. The affirmation of the return or destruction of physical and electronic copies of customer information; and
5. The termination of affiliate or third-party access to customer information.

(F) *Grandfather clause.* Because utilities have numerous existing contracts and nondisclosure agreements in place, and renegotiating all of these agreements would be a monumental task, the Companies added a grandfather clause to clarify that existing contracts need not be renegotiated.

(G) *Energy assistance.* The Companies also notes that, like many utilities, they have agreements in place with community action agencies that allow those agencies limited and secure access customer accounts for the purposes of providing energy assistance. The community action agencies manage their relationships with the customers in determining the eligibility for and amount of incentives. A strict reading of a proposed rule could prohibit the current arrangements between utilities and community action agencies that have streamlined this process for the benefit of customers. Accordingly, the Companies have drafted a specific provision acknowledging that this type of arrangement is appropriate.

(H) *Legal obligations.* The Companies have proposed a provision allowing the current construct by which utilities may comply with orders, ordinances,

subpoenas, and other legal mandates to provide customer information when ordered to do so. The Companies have omitted, however, the Commission reporting aspect that is contained in Staff's version of this rule because it could result in a voluminous amount of research and paperwork as related to the value of the information provided. The Companies receive a substantial number of legal mandates for the provision of customer information. Aside from court orders, subpoenas, and discovery, the Companies also consistently receive ordinances from cities for safety reasons, tax assessments, etc.

(I) *Miscellaneous.* Finally, the Companies included a provision that is intended to provide for the protection of information not otherwise addressed in (2).

20 CSR 4240-10.XXX(3) – Privacy Statement. Ameren Missouri has recently undergone a redrafting of its customer-facing privacy statement at https://www.ameren.com/privacy. This re-drafting drew upon several well-recognized examples in developing the content and structure of its statement including, but not limited to, Exelon.com, MasterCard.com, and Disney.com. This statement generally identifies relevant laws, discloses how customer data may be used, and addresses numerous other data privacy concerns facing multiple industries. Ameren Missouri maintains that its privacy statement is sufficiently developed to address Staff's concerns. The language actually contained in the proposed Staff rule, however, remains problematic for Ameren Missouri and Evergy; accordingly, the Companies are proposing a revised privacy statement requirement.

The Companies note that Staff's proposed rule, which contains a more stringent requirement to "identify applicable (federal, state, county, city, etc.) laws, rules, orders, or

judicial processes (e.g., subpoenas or court orders) and utility tariffs, which support, limit, or prohibit disclosure, if known," is extremely broad, burdensome to compile, and likely provides little value to customers. For example, as previously noted, there are numerous ordinances from various cities asking for various types of customer information; compiling these ordinances alone into a single list would be an overwhelming volume of information for a customer to digest.

Finally, the Companies note that providing a paper copy of a privacy statement is superfluous in a digital age, especially when doing so simply creates additional costs that must ultimately be passed through to its customers. While is the Companies are happy to provide hard copies of this privacy statement upon request, it does not see added value in providing hard copies of this information to all of their customers. Rather, providing this information to all customers, or even to all *new* customers upon signing up for service, could prove an overwhelming amount of information.

20 CSR 4240-10.XXX(4) – Notifications Required. The Companies appreciate Staff's desire for reporting of various incidents and events when it comes to customer data. The Companies believe an appropriate reporting mechanism that will make sure Staff and the OPC receive relevant information regarding incidents is to provide copies of data that would also require reporting to the Missouri Attorney General under Section 407.1500.1 RSMo.

20 CSR 4240-10.XXX(5) – Waivers and Variances. The Companies note that Staff omitted the waivers and variance provisions from its proposed rule. While the Companies have attempted to draft a rule that considers the potential businesses uses of the information in its possession, they also acknowledge that one can never anticipate all

potential scenarios. Accordingly, the Companies have reinserted the waiver and variances provision in case it is required.

WHEREFORE, for the foregoing reasons, Ameren Missouri, and Evergy ask that the Commission take these statements and the Companies' alternate proposed rule into consideration.

Respectfully submitted,

/s/ Paula N. Johnson

Paula N. Johnson, # 68963
Senior Corporate Counsel
Ameren Services Company
P.O. Box 66149, MC 1310
St. Louis, MO 63166-6149
(314) 554-3533 (phone)
(314) 554-4014 (fax)
AmerenMOService@ameren.com
Attorney for UNION ELECTRIC COMPANY, d/b/a Ameren Missouri

/s/ Roger W. Steiner

Roger W. Steiner, MBN 39586
Robert J. Hack, MBN 36496
Evergy, Inc.
1200 Main Street, 16th Floor
Kansas City, MO 64105
Telephone: (816) 556-2791
Telephone: (810) 556-2314
Facsimile: (816) 556-2110
E-Mail: Roger.Steiner@evergy.com
E-Mail: Rob.Hack@evergy.com

Attorneys for Evergy Missouri Metro and Evergy Missouri West

CERTICATE OF SERVICE

I hereby certify that copies of the foregoing have been emailed to the parties of record on this 9th day of December, 2019:

*/s/ Paula N. Johnson*_____
Paula N. Johnson

4 CSR 240-10.XXX Customer Information Of Electrical Corporations, Gas Corporations, Heating Companies, Water Corporations and Sewer Corporations

PURPOSE: This rule is intended to prevent the mishandling and unauthorized access to or disclosure of personal customer information. The release of personal customer information to an affiliate or a third-party nonaffiliate and the treatment of customer information generally, when done in furtherance of the provision of utility-related services, is allowed without customer consent when accomplished in compliance with the conditions set out in the rule below. The release of personal customer information to an affiliate or a third-party nonaffiliate and the treatment of customer information generally, when not related to the provision of utility-related services, may only be accomplished when the customer provides consent to either the utility or the affiliate or third-party nonaffiliated, and there is a contract or nondisclosure agreement in place between the utility and the affiliate or third-party nonaffiliate protecting the privacy of the personal customer information. Each utility shall maintain a public privacy statement consistent with this rule, and make a copy of the privacy statement readily available to its customers.

(1) Definitions

(A) Utility means, for purposes of this rule, an electrical corporation, gas corporation, heating company, water corporation, or sewer corporation as defined in section 386.020, RSMo., and subject to commission regulation pursuant to Chapters 386 and 393, RSMo.

(B) Customer information means any data respecting one or more customers obtained by a utility that is not obtainable by nonaffiliated entities, or that can only be obtained at a competitively prohibitive cost in either time or resources and which may include personal customer information.

(C) Personal customer information means a subset of customer information that includes a combination of a utility customer's name, email or street address, or phone number, with that customer's social security number, driver's license number, government-issued identification number, account access credentials, payment history, financial account number, unique electronic identifier or routing code, medical information, health insurance information, customer specific utility service usage data, such as the history, quantity, quality, or timing of water, natural gas, steam heat, or electricity usage, or electricity production. Personal customer information may include information provided to a utility by an affiliated or nonaffiliated third-party person, entity, or association. Personal customer information does not include anonymized customer data, aggregated customer data, or information that is lawfully included in, or obtained from, publicly available sources, or federal, state, county, or local government records lawfully made available to the general public.

(D) Anonymized customer data is customer data that has been processed in such a manner that it can no longer be attributed to a specific customer.

(E) Aggregated customer data, for the purposes of this rule, is the aggregation of any anonymized customer data associated with at least fifteen (15) customers within a customer class, so long as no single customer's data comprises 15 percent or more of the total aggregated customer data.

(F) Utility-related services includes those services provided by a utility in furtherance of the provision of regulated utility service pursuant to Chapter 386 and 393, RSMo., and pursuant to a utility's commission-approved tariffs, as well as actions taken by the utility

to support, enhance, obtain payment for, enforce, or internally study a customer's or customers' use of those services.

(G) Utility service usage data is data gathered by a utility's metering or similar systems that measure that data in increments such as therms, decatherms, cubic feet, British thermal units, kilowatts, kilowatt hours, voltage, var, gallons, or other applicable measurement method.

(2) Customer Information.

(A) Anonymized customer data and aggregated customer data may be provided to affiliates or third-party nonaffiliates without customer consent.

(B) A utility may allow its personnel access to appropriate components of personal customer information as appropriate in the course of their duties.

(C) When a utility contracts with an affiliate or third-party nonaffiliate for nonutility services on behalf of the utility and provides non-anonymized customer information to that affiliate or third-party nonaffiliate, the utility must be able to demonstrate that it obtained the customer's consent to do so, and must also comply with the provisions of subsection (E).

(D) When a utility contracts with an affiliate or third-party nonaffiliate to perform a utility-related service on behalf of the utility and the provision of customer information is required, that information will be anonymized customer data when practical. If it is not practical to provide anonymized customer data and personal customer information is required to perform the utility-related service, the personal customer information necessary for that performance may be provided without the customer's consent when the utility has complied with its obligations under subsection (E).

(E) For contracts and nondisclosure agreements between the utility and the affiliate or third-party nonaffiliate that address an affiliate's or third-party nonaffiliate's provision of utility-related services or nonutility-related services on behalf of the utility, the utility shall consider the inclusion in the contract or nondisclosure agreement language addressing one or more of the following provisions, as appropriate or practical, and based on the information being provided:

1. A provision limiting the use of personal customer information to the contracted service;

2. A prohibition on the transfer of the ownership or other proprietary rights to personal customer information;

3. The treatment of personal customer information as confidential;

4. A provision contemplating the return or destruction of personal customer information, and verification of same, within a reasonable time following expiration or termination of the applicable contract or non-disclosure agreement; subject to regulatory or legal requirements of the affiliate or third-party nonaffiliated; and

5. A provision that contemplates the removal of electronic access to personal customer information that has been provided to the affiliate or third-party nonaffiliated within a reasonable time after termination or expiration of the contract or non-disclosure agreement, or the completion of the contracted service.

(F) The utility shall not be required to renegotiate or abrogate existing contracts or

nondisclosure agreements as a result of this rule.

(G) Utilities may consider a customer's approved receipt of energy assistance funds through a community action agency as sufficient consent to provide that community action agency with a secure means to access customer account information for the purposes of providing energy assistance funds.

(H) When required to do so by statute, commission or court order, subpoena, ordinance, or other law, a utility may provide personal customer information to the requesting body, but shall only provide the information specifically requested or necessary for the stated purpose, and shall mark the information as confidential as appropriate.

(I) Unless otherwise provided in this rule, when a third-party nonaffiliate contacts the utility regarding a customer and there is no contract or nondisclosure agreement in place between the utility and a third-party nonaffiliate, a utility may only provide personal customer information or grant customer account access to a third-party nonaffiliate when that third-party nonaffiliate provides evidence of the customer's consent to receive the information or account access.

(3) Privacy Policy

(A) Each utility shall publicly disclose its privacy practices, which shall be consistent with this rule, on its website and provide a printed copy to customers upon request. The publicly disclosed privacy practices shall describe what personal customer information obtained by the utility may be made available to affiliates and nonaffiliated third-parties without the consent of the customer. The publicly disclosed privacy practices may also generally identify applicable laws, rules, or orders that support, limit, or prohibit disclosure, if known and as appropriate.

(4) Notifications Required

(A) If there is an incident that warrants the reporting to the attorney general of a "breach of security" or "breach" as defined by Section 407.1500.1 RSMo., the utility shall provide a copy of that report to the commission staff and the office of the public counsel.

(5) Waivers and Variances

(A) Provisions of this rule may be waived by the Commission for good cause shown.

A. Introduction

1. **Title:** **Cyber Security - Supply Chain Risk Management**

2. **Number:** **CIP-013-1**

3. **Purpose:** To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

4. **Applicability:**

   4.1. Functional Entities: For the purpose of the requirements contained herein, the following list of functional entities will be collectively referred to as "Responsible Entities." For requirements in this standard where a specific functional entity or subset of functional entities are the applicable entity or entities, the functional entity or entities are specified explicitly.

   4.1.1. Balancing Authority

   4.1.2. Distribution Provider that owns one or more of the following Facilities, systems, and equipment for the protection or restoration of the BES:

   4.1.2.1. Each underfrequency Load shedding (UFLS) or undervoltage Load shedding (UVLS) system that:

   4.1.2.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

   4.1.2.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

   4.1.2.2. Each Remedial Action Scheme (RAS) where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.2.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

   4.1.3. Generator Operator

   4.1.4. Generator Owner

   4.1.5. Reliability Coordinator

   4.1.6. Transmission Operator

   4.1.7. Transmission Owner

4.2. Facilities: For the purpose of the requirements contained herein, the following Facilities, systems, and equipment owned by each Responsible Entity in 4.1 above are those to which these requirements are applicable. For requirements in this standard where a specific type of Facilities, system, or equipment or subset of Facilities, systems, and equipment are applicable, these are specified explicitly.

4.2.1. Distribution Provider: One or more of the following Facilities, systems and equipment owned by the Distribution Provider for the protection or restoration of the BES:

4.2.1.1. Each UFLS or UVLS System that:

4.2.1.1.1. Is part of a Load shedding program that is subject to one or more requirements in a NERC or Regional Reliability Standard; and

4.2.1.1.2. Performs automatic Load shedding under a common control system owned by the Responsible Entity, without human operator initiation, of 300 MW or more.

4.2.1.2. Each RAS where the RAS is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.3. Each Protection System (excluding UFLS and UVLS) that applies to Transmission where the Protection System is subject to one or more requirements in a NERC or Regional Reliability Standard.

4.2.1.4. Each Cranking Path and group of Elements meeting the initial switching requirements from a Blackstart Resource up to and including the first interconnection point of the starting station service of the next generation unit(s) to be started.

4.2.2. Responsible Entities listed in 4.1 other than Distribution Providers

4.2.2.1. All BES Facilities.

4.2.3. Exemptions: The following are exempt from Standard CIP-013-1:

4.2.3.1. Cyber Assets at Facilities regulated by the Canadian Nuclear Safety Commission.

4.2.3.2. Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters (ESPs).

4.2.3.3. The systems, structures, and components that are regulated by the Nuclear Regulatory Commission under a cyber security plan pursuant to 10 C.F.R. Section 73.54.

4.2.3.4. For Distribution Providers, the systems and equipment that are not included in section 4.2.1 above.

4.2.3.5. Responsible Entities that identify that they have no BES Cyber Systems categorized as high impact or medium impact according to the identification and categorization process required by CIP-002-5, or any subsequent version of that Reliability Standard.

5. Effective Date: See Implementation Plan for Project 2016-03.

B. Requirements and Measures

R1. Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems. The plan(s) shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

1.2. One or more process(es) used in procuring BES Cyber Systems that address the following, as applicable:

1.2.1. Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.2. Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;

1.2.3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;

1.2.4. Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;

1.2.5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and

1.2.6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

M1. Evidence shall include one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Requirement R2: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.

M2. Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, correspondence, policy documents, or working documents that demonstrate use of the supply chain cyber security risk management plan.

R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. Evidence shall include the dated supply chain cyber security risk management plan(s) approved by the CIP Senior Manager or delegate(s) and additional evidence to demonstrate review of the supply chain cyber security risk management plan(s). Evidence may include, but is not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of supply chain risk management plan(s) at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate.

C. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority:

"Compliance Enforcement Authority" means NERC or the Regional Entity, or any entity as otherwise designated by an Applicable Governmental Authority, in their respective roles of monitoring and/or enforcing compliance with mandatory and enforceable Reliability Standards in their respective jurisdictions.

1.2. Evidence Retention:

The following evidence retention period(s) identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation.

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

1.3. Compliance Monitoring and Enforcement Program

As defined in the NERC Rules of Procedure, "Compliance Monitoring and Enforcement Program" refers to the identification of the processes that will be used to evaluate data or information for the purpose of assessing performance or outcomes with the associated Reliability Standard.

Violation Severity Levels

R #	Violation Severity Levels			
	Lower VSL	Moderate VSL	High VSL	Severe VSL
R1.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include one of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s) which include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2, but the plans do not include two or more of the parts in Part 1.2.1 through Part 1.2.6.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, or the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2.	The Responsible Entity developed one or more documented supply chain cyber security risk management plan(s), but the plan(s) did not include the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Part 1.1, and the plan(s) did not include the use of process(es) for procuring BES Cyber systems as specified in Part 1.2. OR The Responsible Entity did not develop one or more documented supply chain cyber security risk management plan(s) as specified in the Requirement.

R2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement one of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s) including the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and including the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2, but did not implement two or more of the parts in Requirement R1 Part 1.2.1 through Part 1.2.6.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, or did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2.	The Responsible Entity implemented its supply chain cyber security risk management plan(s), but did not implement the use of process(es) in planning for procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the BES as specified in Requirement R1 Part 1.1, and did not implement the use of process(es) for procuring BES Cyber systems as specified in Requirement R1 Part 1.2; OR The Responsible Entity did not implement its supply chain cyber security risk management plan(s) specified in the requirement.
R3.	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity reviewed and obtained CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) but did	The Responsible Entity did not review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) within

	so more than 15 calendar months but less than or equal to 16 calendar months since the previous review as specified in the Requirement.	so more than 16 calendar months but less than or equal to 17 calendar months since the previous review as specified in the Requirement.	so more than 17 calendar months but less than or equal to 18 calendar months since the previous review as specified in the Requirement.	18 calendar months of the previous review as specified in the Requirement.

D. Regional Variances

None.

E. Associated Documents

Link to the Implementation Plan and other important associated documents.

Version History

Version	Date	Action	Change Tracking
1	07/20/17	Respond to FERC Order No. 829.	
1	08/10/17	Approved by the NERC Board of Trustees.	
1	10/18/18	FERC Order approving CIP-013-1. Docket No. RM17-13-000.	

Rationale

Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes processes for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (Order No. 829 at P. 45):

(1) Software integrity and authenticity;
(2) Vendor remote access;
(3) Information system planning; and
(4) Vendor risk management and procurement controls.

The cyber security risk management plan(s) specified in Requirement R1 apply to high and medium impact BES Cyber Systems.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders), consistent with Order No. 829 (P. 36).

Requirement R1 Part 1.1 addresses the directive in Order No. 829 for identification and documentation of cyber security risks in the planning and development processes related to the procurement of BES Cyber Systems (P. 56). The security objective is to ensure entities consider cyber security risks to the BES from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s); and options for mitigating these risks when planning for BES Cyber Systems.

Requirement R1 Part 1.2 addresses the directive in Order No. 829 for procurement controls to address the provision and verification of security concepts in future contracts for BES Cyber Systems (P. 59). The objective of Part 1.2 is for entities to include these topics in their plans so that procurement and contract negotiation processes address the applicable risks. Implementation of the entity's plan related to Part 1.2 may be accomplished through the entity's procurement and contract negotiation processes. For example, entities can implement the plan by including applicable procurement items from their plan in Requests for Proposals (RFPs), negotiations with vendors, or requests submitted to entities negotiating on behalf of the Responsible Entity such as in cooperative purchasing agreements. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Although the expectation is that Responsible Entities would enforce the security-related provisions in the contract based on the terms and conditions of that contract, such contract enforcement and vendor performance or adherence to the negotiated contract is not subject to this Reliability Standard.

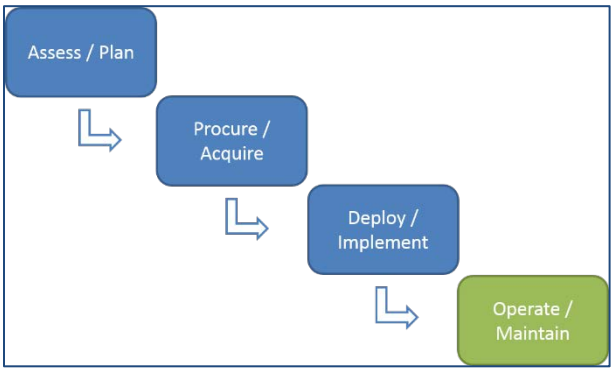
The objective of verifying software integrity and authenticity (Part 1.2.5) is to help ensure that software installed on BES Cyber Systems is not modified prior to installation without the

awareness of the software supplier and is not counterfeit. Part 1.2.5 is not an operational requirement for entities to perform such verification; instead, it requires entities to address the software integrity and authenticity issue in its contracting process to provide the entity the means by which to perform such verification under CIP-010-3.

The term *vendor(s)* as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A *vendor,* as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of CIP-013-1 address an entity's controls for managing cyber security risks to BES Cyber Systems during the planning, acquisition, and deployment phases of the system life cycle, as shown below.

Notional BES Cyber System Life Cycle



Requirement R2:

The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

Entities perform periodic assessment to keep plans up-to-date and address current and emerging supply chain-related concerns and vulnerabilities. Examples of sources of information that the entity could consider include guidance or information issued by:

- NERC or the E-ISAC
- ICS-CERT
- Canadian Cyber Incident Response Centre (CCIRC)

Supplemental Material

Responsible Entities are not required to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders) when implementing an updated plan (i.e., the note in Requirement R2 applies to implementation of new plans and updated plans).

*** FOR INFORMATIONAL PURPOSES ONLY ***

Effective Date of Standard: CIP-013-1 — Cyber Security - Supply Chain Risk Management

United States

Standard	Requirement	Effective Date of Standard	Phased In Implementation Date (if applicable)	Inactive Date
CIP-013-1	All	07/01/2020		