NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Meeting Notes
Project 2016-03 Cyber Security Supply Chain Risk Management Standards Drafting Team

March 14-15, 2017 | 8:30 a.m. - 5:00 p.m. Central
March 16, 2017 | 8:30 a.m. - 1:00 p.m. Central

Hotel Contessa
San Antonio, TX

Administrative

1. Introductions

The meeting was brought to order by the Chair at 8:30 a.m. central on March 14, 2017. Participants were:

First Name	Last Name	Company	Member/ Observer
Paul	Ackerman	Exelon Corporation	O
Tom	Alrich	Deloitte	O
Christina	Alston	Georgia Transmission	M
Steve	Baleno	SCANA	O
Joseph	Baugh	WECC	O
Matt	Brady	Entergy	O
Curt	Brockmann	CPS Energy	O
Tony	Bruton	Oncor	O
James	Chuber	Duke Energy	M
Rebecca	Crawford	Arizona Public Service Co	O
Trey	Cross	ACES	O
Scott	Crow	FoxGuard Solutions, Inc.	O

First Name	Last Name	Company	Member/ Observer
Norm	Dang	IESO	M
Chris	Evans	Southwest Power Pool	M
Mikhail	Falkovich	Con Edison	O
Brian	Gatus	SCE	M
David	Gayle	Dominion Resources	M
Garit	Gemeinhardt	Fortress Information Security	O
Michael	Graham	Consolidated Edison	O
Venona	Greaff	Oxy	O
Ciro	Guzzetta	Con Edison	O
Rusty	Griffin	CPS Energy	M
Rod	Kinard	Oncor	O
Robert	Koziy	Open Systems International Inc.	O
James	McQuiggan	Siemens Wind Power	O
Scott	Mix	NERC	O
JoAnn	Murphy	PJM Interconnection	M
Juliet	Okafor	Fortress Information Security	O
Mark	Olson	nerc	O
Skip	Peeples	Salt River Project	M
James	Schue	ERCOT	O
Corey	Sellers	Southern Company	M
Jeffrey	Sweet	AEP	O

First Name	Last Name	Company	Member/ Observer
Simon	Slobodnik	FERC	O
Jason	Snodgrass	Georgia Transmission Corp	O
Katrina	Thomas	Georgia System Operations Corporation	O
Nathan	Tremmel	Utility Services, Inc.	O
Margaret	Wilson	FirstEnergy Corp	O
Christopher	Wilson	Southern Company	O
Jason	Witt	East Kentucky Power Cooperative	M
Web participants attached			

2. **Determination of Quorum**
   The rule for NERC Standard Drafting Team (SDT or team) states that a quorum requires two-thirds of the voting members of the SDT. Quorum was achieved as 11 of 11 members were present.

3. **NERC Antitrust Compliance Guidelines and Public Announcement**

   NERC Antitrust Compliance Guidelines and public announcement were reviewed by Mark Olson. There were no questions raised.

4. **Review summary of stakeholder issues (issues summary) from initial comments.** Participants reviewed the issues summary from preceding conference call. SDT agreed that these issues reflected stakeholder concerns from the initial comment period for CIP-013. The SDT agreed that the meeting would be approached by considering each issue, developing an SDT position, developing revisions to CIP-013-1 where appropriate, and determining other actions needed to address the stakeholder concern, where appropriate.

5. **Consideration of stakeholder comments to limit the scope of the standard to only planning and procurement life cycle actions.** Participants considered Order No. 829 directives. The SDT agreed that some directives could only be met by developing requirements that would apply to cyber systems in operation/maintenance phase of the life cycle. Examples discussed included some Order No. 829 directives related to vendor-initiated remote access and machine-to-machine remote access with vendors.

6. **Consideration of stakeholder comments on R1 (Supply Chain Cyber Security Risk Management Plans).**

a. **Scope of cyber assets.** Participants discussed applicability in R1 as described in the initial draft. The SDT supports using the defined term BES Cyber System for clarity. The SDT recognized stakeholder concerns that associated cyber systems are not clearly identified in the order. Associated cyber systems was removed from R1 in the working draft of CIP-013.

b. **Applicability to Low Impact BES Cyber Systems.** Participants discussed stakeholder concerns. FERC staff observer commented that the order does not exclude these. The SDT agreed to draft a separate requirements for (1) entities with high and medium impact BES Cyber Assets, and (2) entities with low impact BES Cyber Assets. The SDT reviewed draft wording that could be used in a CIP-003 requirement.

c. **Clarifications on applicability to existing contracts.** Participants discussed stakeholder concerns. SDT developed a note to include in CIP-013 requirements to address.

d. **Stakeholder concerns with vendor cooperation.** Participants discussed stakeholder concerns. The SDT affirmed that the reliability objective of the proposed requirement is to include cyber security issues in the procurement process; consistent with industry supply chain cyber security risk management practices. End-state contracts are not necessarily the measure of performance due to the myriad issues involved in negotiating products and services with vendors. The SDT developed a note to include in CIP-013 requirements to clearly indicate that an entity's performance with R1 is not based on final contract.

e. **Development of the plan.** Participants discussed stakeholder comments to separate development from implementation. The SDT created a separate requirements.

f. **Defining term *vendor*.** Participants discussed stakeholder comments. The SDT believes the description in the Rationale section provides clarity for meeting the objectives of the standard.

g. **Clarification wording.** Participants considered stakeholder recommendations for clarifications to the requirement. The SDT made revisions where appropriate.

7. **Consideration of stakeholder comments on R2 (Review of plans).**

a. **Streamlining the requirement.** Participants discussed comments recommending the removal of parts that were viewed as redundant. The SDT developed a revised requirement without subparts.

b. **Obligation to review.** Participants discussed stakeholder concerns that obligations to review in response to threat changes is unclear. The SDT agreed that the requirement as revised addresses stakeholder concerns. Plans must be reviewed at least every 15 months. Specific practices for additional review are not stipulate, consistent with other reliability standards. The SDT agreed that the appropriate place to list examples of threat-related guidance is in the guidance section and not the requirement.

c. **Initial approval of plans.** Revised wording of the requirement to develop the plan now includes obtaining approval. This change addresses stakeholder comments to clarify initial approval.

d. **Approval by CIP Senior Manager delegates.** SDT confirmed that their intent was for the standard to allow this.

8. **Consideration of stakeholder comments on R3 (Software Integrity and Authenticity).**

   a. **Revisions and alignment with approved standards.** Participants considered stakeholder concerns with including this objective in CIP-013 and with the drafted wording. The SDT agreed to additional coordination with the Project 2016-02 CIP Revisions drafting team to address stakeholder concerns. SDT chair and vice-chair advised that they would coordinate with counterparts.

   b. **Technical Feasibility Exceptions or rewording needed to provide flexibility for asset or vendor capability.** Participants discussed stakeholder concerns. More flexible wording for the requirement was developed.

   c. **Potential negative impact on reliability - may negatively impact ability to patch systems in the required timeframe for CIP-007 R2.3.** Participants discussed stakeholder concerns. SDT will consider ways to address the concern and meet Order No. 829 directives as they align with approved standards.

   d. **Cyber asset scope.** Participants discussed comments about limiting scope to assets "with externally routed connectivity and dial-up", or to include EACMS, PACS, PCA, etc. SDT will consider this further as they align with approved standards.

   e. **Relationship to R1.** Participants discussed comments reflecting stakeholder understanding of the relationship between R3 and R1 Part 1.2.5. SDT agreed that some commenters did not understand their intent for requiring both procurement controls and operating controls.

   f. **Clarification wording.** Participants considered stakeholder recommendations for clarifications to the requirement. The SDT made revisions where appropriate.

9. **Consideration of stakeholder comments on R4 (Vendor Remote Access).**

   a. **Revisions and alignment with approved standards.** Participants considered stakeholder concerns with including this objective in CIP-013 and with the drafted wording. The SDT agreed to additional coordination with the Project 2016-02 CIP Revisions drafting team to address stakeholder concerns. SDT chair and vice-chair advised that they would coordinate with counterparts.

   b. **Technical Feasibility Exceptions or rewording needed to provide flexibility for asset or vendor capability.** Participants discussed stakeholder concerns. More flexible wording for the requirement was developed.

   c. **System-to-system and machine-to-machine terms for remote access are both used.** SDT agreed that this caused confusion between requirements and guidance. System to system is the term that will be used consistently.

   d. **Clarity in term *unauthorized activity*.** Participants discussed stakeholder concerns. The SDT agreed to revise Part 4.3 to require response to **detected** unauthorized activity.

   e. **Clarification wording.** Participants considered stakeholder recommendations for clarifications to the requirement. The SDT made revisions where appropriate.

10. **Consideration of stakeholder comments on R5 (Software verification and vendor remote access for lows).** Participants discussed stakeholder recommendations to remove R5. Several participants viewed requirements for verifying software at low-impact BES Cyber System level to be onerous and challenging for compliance demonstration. FERC staff observer suggested that performance of potential requirements at the asset or group of asset level could be achieved in a manner similar to CIP-003 requirements. SDT agreed that operational controls for low-impact BES Cyber Systems may not be warranted in a risk-based standard. SDT agreed to remove R5. SDT confirmed that supply chain risk to lows is still being included in supply chain risk management plan requirement.

11. **Next steps.** Summary of issues was reviewed by Mark Olson. The SDT is targeting mid-April for second posting of revised CIP-013, related material, and any draft revisions to approved CIP standards that may be needed to address directives.

12. **Future meeting(s)**

    a. March 30, 2017 | Web Meeting

    b. April 6, 2017 | Web Meeting

    c. April 11-12, 2017 | in-person meeting at NERC Headquarters Atlanta

    d. June 7-9, 2017 | in-person meeting, location TBD

13. The meeting adjourned at 11:45 a.m. central on March 16, 2017

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Description of Current Draft

This is the first draft of the proposed standard.

Completed Actions	Date
Standards Committee approved Standard Authorization Request (SAR) for posting	October 19, 2016
SAR posted for comment	October 20 - November 21, 2016
45-day formal comment period with ballot	January 19 - March 6, 2017

Anticipated Actions	Date
45-day formal comment period with ballot	~~January~~ April 2017
NERC Board (Board) adoption	August 2017

New or Modified Term(s) Used in NERC Reliability Standards

This section includes all new or modified terms used in the proposed standard that will be included in the *Glossary of Terms Used in NERC Reliability Standards* upon applicable regulatory approval. Terms used in the proposed standard that are already defined and are not being modified can be found in the *Glossary of Terms Used in NERC Reliability Standards*. The new or revised terms listed below will be presented for approval with the proposed standard. Upon Board adoption, this section will be removed.

Term(s): None

Upon Board adoption, the rationale boxes will be moved to the Supplemental Material Section.

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 CIP-002-5 identification and categorization processes

~~4.2.3.4.~~

5. **Effective Date:** See Implementation Plan.

B. Requirements and Measures

Rationale for Requirement R1:

The proposed Requirement addresses Order No. 829 directives for entities to implement a plan(s) that includes controls for mitigating cyber security risks in the supply chain. The plan(s) is required to address the following four objectives (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 BES Cyber Systems ~~and, to the extent applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets~~. Cyber security risks threaten the confidentiality, integrity, and availability of cyber assets.

Implementation of the cyber security risk management plan(s) does not require the Responsible Entity to renegotiate or abrogate existing contracts, consistent with Order No. 829 (P. 36) as specified in the Implementation Plan. Master agreements, which are amended or changed to procure vendor products or services, are also not required to be renegotiated or abrogated solely due to the entity's implementation of its cyber security risk management plan.

Requirement R1 Part 1.1 addresses Order No. 829 directives for identification and documentation of risks in the planning and development processes related to proposed BES Cyber Systems (P. 56). The objective is to ensure entities consider risks and options for mitigating these risks when planning, acquiring, and deploying BES Cyber Systems.

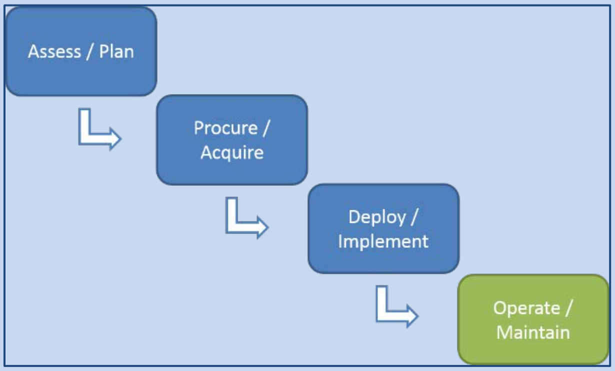
Requirement R1 Part 1.2 addresses Order No. 829 directives for procurement controls to address vendor-related security concepts in future contracts for BES Cyber Systems ~~and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets~~. (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 elements contained in the entity's plan related to Part 1.2 is 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) and in negotiations with vendors. Obtaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan. Responsible entities use various means to assure vendor adherance to agreements with the responsible entity, however a responsible entity's implementation of its plan is not based on vendor performance of those agreements.

The objective of verifying software integrity and authenticity (Part 1.2.5) is to ensure that the software being installed in the applicable cyber system was not modified without the awareness of the software supplier and is not counterfeit.

The term *vendors* as used in the standard includes (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.

Collectively, the provisions of Requirement R1 and R2 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



Requirements R3 through R5 address controls for software integrity and authenticity and vendor remote access that apply to the operate/maintain phase of the system life cycle.

R1. Each Responsible Entity shall ~~implement~~ develop and obtain CIP Senior Manager or delegate approval of one or more documented supply chain cyber security risk management plan(s) that address controls for mitigating cyber security risks during planning and procurement of ~~to~~ high and medium impact BES Cyber Systems ~~and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access~~

~~Control Systems, and Protected Cyber Assets~~. The plan(s) shall address: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. The use of process(es) ~~controls~~ in BES Cyber System planning to address cyber security risk(s) to the BES during the procurement and deployment of vendor products and services ~~and development~~ to:

~~**1.1.1.** Identify and assess risk(s) during the procurement and deployment of vendor products and services; and~~

~~**1.1.2.** Evaluate methods to address identified risk(s).~~

1.2. The use of procurement process(es) for ~~controls in procuring~~obtaining vendor product(s) or service(s) that address the following items, to the extent each item ~~applies~~ impacts ~~to~~ the Responsible Entity's BES Cyber Systems ~~and, if applicable, associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets~~:

1.2.1. Process(es) for notification and coordination of response of vendor-identified cyber security risks; ~~events~~;

1.2.2. Process(es) for notification when vendor employee remote or onsite access should no longer be granted;

1.2.3. Process(es) for disclosure of known vulnerabilities;

~~**1.2.4.** Coordination of response to vendor-related cyber security incidents;~~

~~1.2.5.~~1.2.4. Process(es) for verifying software integrity and authenticity of all software and patches that are intended for use; and

~~1.2.6.~~1.2.5. Coordination of remote access controls for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s); and

~~1.2.7.~~1.2.6. ~~Other process(es) to address risk(s) as determined in Part 1.1.2, if applicable.~~

M1. Evidence shall include ~~(i)~~ one or more documented and approved supply chain cyber security risk management plan(s) that address controls for mitigating cyber security risks during planning and procurementas specified in the Requirement.; ~~and (ii) documentation to demonstrate implementation of the supply chain cyber security risk management plan(s), which could include, but is not limited to, written agreements in electronic or hard copy format, correspondence, policy documents, or working documents that demonstrate implementation of the cyber security risk~~ management plan(s) in planning and procuring BES Cyber Systems.

R2. Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.

Note: Implementation of the plan does not require the Responsible Entity to renegotiate or abrogate existing contracts. Additionally, the following issues are beyond the scope of Requirement R1: (1) the actual terms and conditions of a procurement contract; (2) contract performance and enforcement.

~~M1.~~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.

Rationale for Requirement ~~R2~~R3:
The proposed requirement addresses Order No. 829 directives for entities to periodically reassess selected supply chain cyber security risk management controls (P. 46).

~~Order No. 829 also directs that the p~~Entity's perform periodic assessment ~~"ensure that the required~~to keep plans ~~remains~~ up-to-date and~~,~~ address~~ing~~ current and emerging supply chain-related concerns and vulnerabilities.~~" (P. 47).~~ Examples of sources of information that the entity could consider~~s~~ includes guidance or information issued by:

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

~~R2.~~R3. Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval ~~update, as necessary,~~of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months~~, which shall include:~~. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

~~**2.1.** Evaluation of revisions, if any, to address applicable new supply chain security risks and mitigation measures; and~~

~~**2.2.** Obtaining CIP Senior Manager or delegate approval.~~

~~M2.~~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~~) and evaluation of revisions~~)~~, if any, to address applicable new supply chain security risks and mitigation measures as specified in the Requirement.~~ 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.

Rationale for Requirement ~~R3~~R4:
The proposed requirement addresses Order No. 829 directives for verifying software integrity and authenticity prior to installation in BES Cyber Systems (P. 48).

The objective of ~~verifying~~ software integrity and authenticity process(es) is to mitigate risks to the BES Cyber System from ~~ensure that the~~ software ~~being installed in the BES Cyber System~~that has potentially been ~~was not~~ modified without the awareness of the software supplier ~~and~~ or is ~~not~~ counterfeit. System capabilities vary.

~~R3.~~R4. Each Responsible Entity shall implement one or more documented process(es) to achieve the objective of ~~for~~ verifying the integrity and authenticity of the following vendor-provided software and firmware, where a verification method is available, before being ~~placed~~ used in operation on high and medium impact BES Cyber Systems: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

~~3.1.~~4.1. Operating System(s);

~~3.2.~~4.2. Firmware;

~~3.3.~~4.3. Commercially available or open-source application software; and

4.4. Patches, updates, and upgrades to 3.1 through 3.3.

~~3.4.~~

~~M3.~~M4. Evidence shall include (i) a documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation that the entity performed the actions contained in the process to verify the integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware prior to installation on high and medium impact BES Cyber Systems.

Rationale for Requirement ~~R4~~R5:
The proposed requirement addresses Order No. 829 directives for controls on vendor-initiated remote access to BES Cyber Systems covering both user-initiated and machine-to-machine vendor remote access (P. 51). The objective of the

Requirement is to mitigate potential risks of a compromise at a vendor from traversing over an unmonitored remote access connection.

The objective of Requirement R4 Part 4.3 is for entities to have the ability to rapidly disable remote access sessions in the event of a system breach as specified in Order No. 829 (P. 52).

~~R4.~~R5. Each Responsible Entity shall implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems. The process(es) shall provide the following for (i) vendor-initiated Interactive Remote Access and (ii) system-to-system remote access with a vendor(s): *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

~~4.1.~~ Authorization Authorizing sessions of ~~of~~ remote access by the Responsible Entity;[MO1]

5.1. Logging and controlling remote access sessions

~~4.2.~~5.2. ~~Logging and monitoring of remote access sessions to d~~Detecting unauthorized activity during remote access sessions; and

~~4.3.~~5.3. Disabling or otherwise responding to detected unauthorized activity during remote access sessions.

~~M4.~~M5. Evidence shall include (i) a documented process(es) for controlling vendor remote access as specified in the Requirement; and (ii) evidence to show that the process was implemented. This evidence may include, but is not limited to, documentation of authorization of vendor remote access; hard copy or electronic logs of vendor-initiated Interactive Remote Access and system-to-system remote access sessions; hard copy or electronic listing of alert capabilities applicable to vendor remote access of the BES Cyber System; or records of response to unauthorized vendor remote access.

~~**Rationale for Requirement R5:**~~

~~The proposed requirement addresses Order No. 829 directives for (i) verifying software integrity and authenticity; and (ii) controlling vendor remote access, as they apply to low impact BES Cyber Systems. (P. 48 and P. 51).~~

~~An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.~~

~~An entity could apply process(es) used for Requirements R3 and R4 to satisfy its obligations in Requirement R5 or could develop a separate policy or process(es) to address low impact BES Cyber Systems.~~

~~**R5.** Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall have one or more documented cyber security policies, which shall be reviewed and approved by the CIP Senior Manager or delegate at least once every 15 calendar months, that address the following topics for its low impact BES Cyber Systems: *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*~~

~~**5.1.** Integrity and authenticity of software and firmware and any patches, updates, and upgrades to software and firmware; and~~

~~**5.2.** Controlling vendor-initiated remote access, including system-to-system remote access with vendor(s).~~

~~**M5.**~~**M6.** ~~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 each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager or delegate for each cyber security policy.~~

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.	N/A	N/A	The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include one of the elements specified in Parts 1.1 or 1.2.	The Responsible Entity implemented one or more documented supply chain risk management plan(s), but the plan(s) did not include either of the elements specified in Parts 1.1 or 1.2.; OR The Responsible Entity did not implement one or more documented supply chain risk management plan(s) as specified in the Requirement.
R2.	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 15 calendar months but less than or equal to 16 calendar months	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 16 calendar months but less than or equal to 17 calendar months	The Responsible Entity reviewed and updated, as necessary, its supply chain cyber security risk management plan(s) and obtained CIP Senior Manager or delegate approval but did so more than 17 calendar months but less than or equal to 18	The Responsible Entity did not review and update, as necessary, its supply chain cyber security risk management plan(s) and obtain CIP Senior Manager or delegate approval within 18 calendar months of the previous review as specified in the Requirement.

	since the previous review as specified in the Requirement.	since the previous review as specified in the Requirement.	calendar months since the previous review as specified in the Requirement.	
R3.	N/A	N/A	N/A	The Responsible Entity did not implement one or more documented process(es) for verifying the integrity and authenticity of software and firmware before being placed in operation on high and medium impact BES Cyber Systems as specified in the Requirement.
R4.	N/A	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include one of the elements specified in Part 4.1 through Part 4.3.	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include two of the elements specified in Part 4.1 through Part 4.3.	The Responsible Entity implemented one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems, but did not include any of the elements specified in Part 4.1 through Part 4.3; OR, The Responsible Entity did not implement one or more documented process(es) for controlling vendor remote access to high and medium impact BES Cyber Systems as

				specified in the Requirement.
R5.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 15 calendar months but less than or equal to 16 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 16 calendar months but less than or equal to 17 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include one of the elements in Parts 5.1 or 5.2; OR The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the approval was more than 17 calendar months but less than or equal to 18 calendar months from the previous review.	The Responsible Entity had cyber security policies specified in the requirement that were reviewed and approved by the CIP Senior Manager or delegate, however the cyber security policies but did not include either of the elements in Parts 5.1 or 5.2; OR The Responsible Entity did not have cyber security policies that were reviewed and approved by the CIP Senior Manager or delegate 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	TBD	Respond to FERC Order No. 829	NA

Standard Attachments

None

Guidelines and Technical Basis

Rationale

During development of this standard, text boxes were embedded within the standard to explain the rationale for various parts of the standard. Upon BOT adoption, the text from the rationale text boxes was moved to this section.

All sessions in Eastern Daylight Time (New York, GMT-04:00)
Session detail for 'NERC Meeting Room':

Participant	Name	Email	Date
	Aaron	aaron.curtis@kcpl.com	3/16/2017
	Alwyn Wood	alwyn.wood@ge.com	3/14/2017
	Alwyn Wood	alwyn.wood@ge.com	3/16/2017
	Amelia Sawyer	amelia.sawyer@centerpointenergy.com	3/14/2017
	Amelia Sawyer	amelia.sawyer@centerpointenergy.com	3/15/2017
	Amelia Sawyer	amelia.sawyer@centerpointenergy.com	3/16/2017
	Bryan Owen	bryan@osisoft.com	3/15/2017
	Bryan Owen (OSIsoft)	bryan@osisoft.com	3/16/2017
	C	chjesen@bpa.gov	3/14/2017
	Chantal Mazza	mazza.chantal@hydro.qc.ca	3/14/2017
	Chantal Mazza	mazza.chantal@hydro.qc.ca	3/14/2017
	Chantal Mazza	mazza.chantal@hydro.qc.ca	3/14/2017
	Dan Reddy	scrmsme@outlook.com	3/14/2017
	Dan Reddy	scrmsme@outlook.com	3/15/2017
	Dan Reddy	scrmsme@outlook.com	3/16/2017
	Daniel Moore	d_moore@wfec.com	3/15/2017
	Daniel Moore	d_moore@wfec.com	3/16/2017
	Daniel Phillips	daniel.phillips@ferc.gov	3/14/2017
	Daniel Phillips	daniel.phillips@ferc.gov	3/15/2017
	Daniel Phillips	daniel.phillips@ferc.gov	3/15/2017
	David Foose	david.foose@emerson.com	3/14/2017
	David Foose	david.foose@emerson.com	3/14/2017
	David Foose	david.foose@emerson.com	3/15/2017
	Douglas	doug.webb@kcpl.com	3/14/2017
	Douglas	doug.webb@kcpl.com	3/14/2017
	Douglas Webb	doug.webb@kcpl.com	3/14/2017
	Douglas Webb	doug.webb@kcpl.com	3/15/2017
	Douglas Webb	doug.webb@kcpl.com	3/16/2017
	Edd	edward.dobrowolski@navigant.com	3/14/2017
	Edd	edward.dobrowolski@navigant.com	3/14/2017
	Edd	edward.dobrowolski@navigant.com	3/14/2017
	Edd	edward.dobrowolski@navigant.com	3/14/2017
	Edd	edward.dobrowolski@navigant.com	3/15/2017
	Edd	edward.dobrowolski@navigant.com	3/15/2017
	Edd	edward.dobrowolski@navigant.com	3/16/2017
	Elise Baker	bakerea@bv.com	3/15/2017
	Geo Masters	george_masters@selinc.com	3/14/2017
	Geo Masters	george_masters@selinc.com	3/14/2017
	Geo Masters	george_masters@selinc.com	3/14/2017
	George Oliveira	oliveira.george@hydro.qc.ca	3/14/2017
	George Oliveira	oliveira.george@hydro.qc.ca	3/15/2017
	Harvey Lloyd	harvey.lloyd@ferc.gov	3/14/2017
	Harvey Lloyd	harvey.lloyd@ferc.gov	3/14/2017
	Harvey Lloyd	harvey.lloyd@ferc.gov	3/14/2017

Harvey Lloyd	harvey.lloyd@ferc.gov	3/15/2017
Harvey Lloyd	harvey.lloyd@ferc.gov	3/15/2017
Harvey Lloyd	harvey.lloyd@ferc.gov	3/16/2017
Hong Ablack	hong.ablack@centerpointenergy.com	3/15/2017
J Smith	jess_smith@selinc.com	3/14/2017
J Smith	jess_smith@selinc.com	3/14/2017
Jamie Schue	james.schue@ercot.com	3/14/2017
Jamie Schue	james.schue@ercot.com	3/14/2017
Jamie Schue	james.schue@ercot.com	3/15/2017
Jason Snodgrass	jason.snodgrass@gatrans.com	3/16/2017
Jay Cribb	jscribb@southernco.com	3/14/2017
Jay Cribb	jscribb@southernco.com	3/14/2017
Jay Cribb	jscribb@southernco.com	3/14/2017
Jay Cribb	jscribb@southernco.com	3/14/2017
Jay Cribb	jscribb@southernco.com	3/16/2017
Jeff Craigo	jeff.craigo@rfirst.org	3/14/2017
Jeff Craigo	jeff.craigo@rfirst.org	3/14/2017
Jeff Craigo	jeff.craigo@rfirst.org	3/14/2017
Jeff Craigo	jeff.craigo@rfirst.org	3/15/2017
Jeff Craigo	jeff.craigo@rfirst.org	3/15/2017
Jennifer	jennifer.blair@lge-ku.com	3/14/2017
Jennifer	jennifer.blair@lge-ku.com	3/15/2017
Jennifer	jennifer.blair@lge-ku.com	3/15/2017
Jennifer	jennifer.blair@lge-ku.com	3/16/2017
Jennifer	jennifer.blair@lge-ku.com	3/16/2017
Jennifer Blair	jennifer.blair@lge-ku.com	3/14/2017
Jennifer Blair	jennifer.blair@lge-ku.com	3/14/2017
Jennifer Blair	jennifer.blair@lge-ku.com	3/14/2017
Jennifer Blair	jennifer.blair@lge-ku.com	3/14/2017
Jennifer Blair	jennifer.blair@lge-ku.com	3/14/2017
Jerrod Montoya	jerrod.montoya@oati.net	3/14/2017
Jerrod Montoya	jerrod.montoya@oati.net	3/14/2017
Jerrod Montoya	jerrod.montoya@oati.net	3/15/2017
Jim Fletcher	jrfletcher@aep.com	3/14/2017
Jim Fletcher	jrfletcher@aep.com	3/15/2017
Jim Fletcher	jrfletcher@aep.com	3/16/2017
Jim Fletcher	jrfletcher@aep.com	3/16/2017
Joel	joelc@centralpwr.com	3/15/2017
John Calder	john.calder@dom.com	3/14/2017
John Calder	john.calder@dom.com	3/15/2017
John Calder	john.calder@dom.com	3/16/2017
John Dirks	john.dirks@srpnet.com	3/14/2017
John Dirks	john.dirks@srpnet.com	3/14/2017
John Dirks	john.dirks@srpnet.com	3/14/2017
John Dirks	john.dirks@srpnet.com	3/15/2017
John Dirks	john.dirks@srpnet.com	3/16/2017
Kaathie Heale	kathie.heale@gasoc.com	3/14/2017

Kathie Heale	kathie.heale@gasoc.com	3/14/2017
Kathie Heale	kathie.heale@gasoc.com	3/14/2017
Kathie Heale	kathie.heale@gasoc.com	3/15/2017
Kathie Heale	kathie.heale@gasoc.com	3/15/2017
Kathie Heale	kathie.heale@gasoc.com	3/16/2017
Kathie Heale	kathie.heale@gasoc.com	3/16/2017
Ken Stell	ken.stell@dynegy.com	3/14/2017
Ken Stell	ken.stell@dynegy.com	3/14/2017
ken stell	ken.stell@dynegy.com	3/15/2017
Ken Stell	ken.stell@dynegy.com	3/15/2017
Ken Stell	ken.stell@dynegy.com	3/16/2017
ken stell	ken.stell@dynegy.com	3/16/2017
Kevin Bunch	kevin.bunch@edfenergyservices.com	3/14/2017
Kevin Bunch	kevin.bunch@edfenergyservices.com	3/14/2017
Kevin Bunch	kevin.bunch@edfenergyservices.com	3/14/2017
Kevin Bunch	kevin.bunch@edfenergyservices.com	3/14/2017
Kevin Bunch	kevin.bunch@edfenergyservices.com	3/15/2017
Kevin Bunch	kevin.bunch@edfenergyservices.com	3/16/2017
Kimberly	kim.zimmerman@energysec.org	3/14/2017
Kimberly	kim.zimmerman@energysec.org	3/14/2017
Kimberly Zimmerman	kim.zimmerman@energysec.org	3/14/2017
Kimberly Zimmerman	kim.zimmerman@energysec.org	3/14/2017
Kimberly Zimmerman	kim.zimmerman@energysec.org	3/15/2017
Kimberly Zimmerman	kim.zimmerman@energysec.org	3/15/2017
Kimberly Zimmerman	kim.zimmerman@energysec.org	3/16/2017
Laura Anderson	laura.anderson@nerc.net	3/14/2017
Laura Anderson	laura.anderson@nerc.net	3/14/2017
Laura Anderson	laura.anderson@nerc.net	3/14/2017
Laura Anderson	laura.anderson@nerc.net	3/15/2017
Laura Anderson	laura.anderson@nerc.net	3/15/2017
Laura Anderson	laura.anderson@nerc.net	3/16/2017
Louis Guidry (Cleco)	louis.guidry@cleco.com	3/14/2017
Louis Guidry (Cleco)	louis.guidry@cleco.com	3/14/2017
Louis Guidry (Cleco)	louis.guidry@cleco.com	3/14/2017
Louis Guidry (Cleco)	louis.guidry@cleco.com	3/15/2017
Lynn Schloesser	lschloesser@acec.org	3/15/2017
Lynn Schloesser	lschloesser@acec.org	3/16/2017
Margaret	mtwilson@firstenergycorp.com	3/14/2017
Margaret	mtwilson@firstenergycorp.com	3/14/2017
Margaret	mtwilson@firstenergycorp.com	3/15/2017
Margaret	mtwilson@firstenergycorp.com	3/16/2017
Mark McCarl	mark.mccarl@duke-energy.com	3/14/2017
Mark McCarl	mark.mccarl@duke-energy.com	3/14/2017
Mark McCarl	mark.mccarl@duke-energy.com	3/15/2017
Mark Olson	mark.olson@nerc.net	3/14/2017
Mark Olson	mark.olson@nerc.net	3/14/2017
Mark Olson	mark.olson@nerc.net	3/14/2017

Mark Olson	mark.olson@nerc.net	3/15/2017
Mark Olson	mark.olson@nerc.net	3/16/2017
Mark Riley	mriley@aeci.org	3/14/2017
Mark Riley	mriley@aeci.org	3/14/2017
Mark Riley	mriley@aeci.org	3/14/2017
Mark Riley	mriley@aeci.org	3/14/2017
Mark Riley	mriley@aeci.org	3/15/2017
Mark Riley	mriley@aeci.org	3/16/2017
Mike Kraft	mkraft@bepc.com	3/14/2017
Mike Kraft	mkraft@bepc.com	3/14/2017
Mike Kraft	mkraft@bepc.com	3/15/2017
Mike Kraft	mkraft@bepc.com	3/15/2017
Munshik Park	parkm@coned.com	3/15/2017
Munshik Park	parkm@coned.com	3/15/2017
Nasheema	nasheema.santos@nerc.net	3/14/2017
Nichole Morgan	de@de.fe	3/14/2017
Nichole Morgan	ff@de.cok	3/15/2017
Patricia Eke	patricia.eke@ferc.gov	3/14/2017
Patricia Eke	patricia.eke@ferc.gov	3/14/2017
Patricia Eke	patricia.eke@ferc.gov	3/15/2017
Patricia Eke	patricia.eke@ferc.gov	3/16/2017
Radhika Chaturvedi(UL)	radhika.chaturvedi@ul.com	3/14/2017
Randy Wagner	rwagner@bepc.com	3/14/2017
Randy Wagner	rwagner@bepc.com	3/14/2017
Randy Wagner	rwagner@bepc.com	3/14/2017
Randy Wagner	rwagner@bepc.com	3/14/2017
Randy Wagner	rwagner@bepc.com	3/14/2017
Randy Wagner	rwagner@bepc.com	3/14/2017
Randy Wagner	rwagner@bepc.com	3/15/2017
Randy Wagner	rwagner@bepc.com	3/15/2017
Randy Wagner	rwagner@bepc.com	3/15/2017
Randy Wagner	rwagner@bepc.com	3/15/2017
Randy Wagner	rwagner@bepc.com	3/15/2017
Randy Wagner	rwagner@bepc.com	3/16/2017
Randy Wagner	rwagner@bepc.com	3/16/2017
Randy Wagner	rwagner@bepc.com	3/16/2017
Randy Wagner	rwagner@bepc.com	3/16/2017
Renee	rhanft@vectren.com	3/14/2017
Renee	rhanft@vectren.com	3/14/2017
Renee	rhanft@vectren.com	3/14/2017
Renee	rhanft@vectren.com	3/14/2017
Renee	rhanft@vectren.com	3/14/2017
Renee	rhanft@vectren.com	3/14/2017
Renee Hanft	rhanft@vectren.com	3/14/2017
Renee Hanft	rhanft@vectren.com	3/15/2017
Renee Hanft	rhanft@vectren.com	3/15/2017
Renee Hanft	rhanft@vectren.com	3/15/2017

Renee Hanft	rhanft@vectren.com	3/15/2017
Renee Hanft	rhanft@vectren.com	3/15/2017
Renee Hanft	rhanft@vectren.com	3/16/2017
Renee Hanft	rhanft@vectren.com	3/16/2017
Rhonda Dunfee	rhonda.dunfee@ferc.gov	3/14/2017
Rhonda Dunfee	rhonda.dunfee@ferc.gov	3/14/2017
Rhonda Dunfee	rhonda.dunfee@ferc.gov	3/15/2017
Rhonda Dunfee	rhonda.dunfee@ferc.gov	3/15/2017
Rhonda Dunfee	rhonda.dunfee@ferc.gov	3/15/2017
Rhonda Dunfee	rhonda.dunfee@ferc.gov	3/16/2017
Richard Watson	richard.watson@lge-ku.com	3/14/2017
Richard Watson	richard.watson@lge-ku.com	3/14/2017
scott	scott.hill@pacificorp.com	3/14/2017
Scott	scott.hill@pacificorp.com	3/14/2017
Scott	scott.hill@pacificorp.com	3/14/2017
Scott	scott.hill@pacificorp.com	3/14/2017
Scott Saunders	scott.saunders@exeloncorp.com	3/14/2017
Scott Saunders	scott.saunders@exeloncorp.com	3/16/2017
Scott Saunders (Exelon)	scott.saunders@exeloncorp.com	3/15/2017
Shamai Elstein	shamai.elstein@nerc.net	3/14/2017
Shamai Elstein	shamai.elstein@nerc.net	3/15/2017
Shamai Elstein	shamai.elstein@nerc.net	3/15/2017
Shamai Elstein	shamai.elstein@nerc.net	3/16/2017
Shawn Eck	seck@empiredistrict.com	3/15/2017
Shawn Eck	seck@empiredistrict.com	3/16/2017
Sheranee Nedd - PSEG	sheranee.nedd@pseg.com	3/14/2017
Simon Slobodnik	simon.slobodnik@ferc.gov	3/14/2017
Simon Slobodnik	simon.slobodnik@ferc.gov	3/14/2017
sophia combs	sophia.combs@srpnet.com	3/14/2017
Sophia Combs	sophia.combs@srpnet.com	3/14/2017
sophia combs	sophia.combs@srpnet.com	3/14/2017
sophia combs	sophia.combs@srpnet.com	3/14/2017
sophia combs	sophia.combs@srpnet.com	3/15/2017
sophia combs	sophia.combs@srpnet.com	3/15/2017
sophia combs	sophia.combs@srpnet.com	3/15/2017
sophia combs	sophia.combs@srpnet.com	3/15/2017
sophia combs	sophia.combs@srpnet.com	3/15/2017
sophia combs	sophia.combs@srpnet.com	3/16/2017
sophia combs	sophia.combs@srpnet.com	3/16/2017
Steen Fjalstad	sj.fjalstad@midwestreliability.org	3/14/2017
Steen Fjalstad	sj.fjalstad@midwestreliability.org	3/14/2017
Steen Fjalstad	sj.fjalstad@midwestreliability.org	3/15/2017
Steve Brain	steve.brain@dom.com	3/14/2017
Steve Brain	steve.brain@dom.com	3/14/2017
Steve Brain	steve.brain@dom.com	3/15/2017
Steve Brain	steve.brain@dom.com	3/16/2017
Steve Griffith	steve.griffith@nema.org	3/16/2017

Steven	sabriggs@tva.gov	3/15/2017
Steven	sabriggs@tva.gov	3/16/2017
T Zaragoza	ffzaragoza@iid.com	3/14/2017
T. Zaragoza	ffzaragoza@iid.com	3/14/2017
Tino Zaragoza	ffzaragoza@iid.com	3/15/2017
Tom Hofstetter	tom.hofstetter@nerc.net	3/14/2017
Tom Hofstetter	tom.hofstetter@nerc.net	3/14/2017
Tom Hofstetter	tom.hofstetter@nerc.net	3/14/2017
Tom Hofstetter	tom.hofstetter@nerc.net	3/15/2017
Tony	tony.bruton@oncor.com	3/15/2017
Tony	tony.bruton@oncor.com	3/15/2017
Tony	tony.bruton@oncor.com	3/15/2017
Tony Bruton	tony.bruton@oncor.com	3/14/2017
Tony Bruton	tony.bruton@oncor.com	3/14/2017
Tony Hall	tony.hall@lge-ku.com	3/14/2017
Tony Hall	tony.hall@lge-ku.com	3/14/2017
Tony Hall	tony-hall@lge-ku.com	3/14/2017
Tony Hall	tony.hall@lge-ku.com	3/16/2017
Tracie Bushman	tbushman@idahopower.com	3/15/2017
William Vesely	veselyw@coned.com	3/14/2017
William Vesely	veselyw@coned.com	3/14/2017
William Vesely	veselyw@coned.com	3/15/2017
William Vesely	veselyw@coned.com	3/16/2017
Ziel	ff@de.cok	3/16/2017