NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Project Name: 2016-03 Cyber Security Supply Chain Management | SAR October 2016

Comment Period Start Date: 10/20/2016

Comment Period End Date: 11/18/2016

Associated Ballots:

There were 24 sets of responses, including comments from approximately 24 different people from approximately 23 companies representing 8 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the proposed scope for Project 2016-03 as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.

2. Provide any additional comments for the Standards Drafting Team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
ACES Power Marketing	Ben Engelby	6		ACES Standards Collaborators - CIP	Mike Brytowski	Great River Energy	1,3,5,6	MRO
					Ginger Mercier	Prairie Power, Inc.	3	SERC
					Tara Lightner	Sunflower Electric Power Corporation	1	SPP RE
					Shari Heino	Brazos Electric Power Cooperative, Inc.	1,5	Texas RE
					Bill Watson	Old Dominion Electric Cooperative	3,4	RF
					Cassie Williams	Golden Spread Electric Cooperative	3,5	SPP RE
					Scott Brame	North Carolina Electric	3,4,5	SERC

	Membership Corporation		
Ryan Strom	Buckeye Power, Inc.	3,4,5	RF
Bob Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	RF
Eric Jensen	Arizona Electric Power Cooperative, Inc.	1	WECC
Bill Hutchison	Southern Illinois Power Cooperative	1	SERC
Greg Froehling	Rayburn Country Electric Cooperative, Inc.	3	SPP RE
Kevin Lyons	Central Iowa Power Cooperative	1	MRO
Carl Behnke	Southern Maryland	3	RF

						Electric Cooperative		
					Susan Sosbe	Wabash Valley Power Association	3	SERC
Duke Energy	Colby Bellville	1,3,5,6	FRCC,RF,SERC	Duke Energy	Doug Hils	Duke Energy	1	RF
					Lee Schuster	Duke Energy	3	FRCC
					Dale Goodwine	Duke Energy	5	SERC
					Greg Cecil	Duke Energy	6	RF
Con Ed - Consolidated Edison Co. of New York	Dermot Smyth	3,4,5,6	NPCC	Con Edison	Dermot Smyth	Con Edison Company of New York	1,3,5,6	NPCC
					Edward Bedder	Orange & Rockland		NPCC
Lower Colorado River Authority	Michael Shaw	1,5,6		LCRA Compliance	Teresa Cantwell	LCRA	1	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Michael Shaw	LCRA	6	Texas RE
Southern Company - Southern Company Services, Inc.	Pamela Hunter	1,3,5,6	SERC	Southern Company	Katherine Prewitt	Southern Company Services, Inc.	1	SERC
					R. Scott Moore	Alabama Power Company	3	SERC

					William D. Shultz	Southern Company Generation	5	SERC
					Jennifer G. Sykes	Southern Company Generation and Energy Marketing	6	SERC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,10	NPCC	RSC	Paul Malozewski	Hydro One.	1	NPCC
					Guy Zito	Northeast Power Coordinating Council	NA - Not Applicable	NPCC
					Randy MacDonald	New Brunswick Power	2	NPCC
					Wayne Sipperly	New York Power Authority	4	NPCC
					David Ramkalawan	Ontario Power Generation	4	NPCC
					Glen Smith	Entergy Services	4	NPCC
					Brian Robinson	Utility Services	5	NPCC

Bruce Metruck	New York Power Authority	6	NPCC
Alan Adamson	New York State Reliability Council	7	NPCC
Edward Bedder	Orange & Rockland Utilities	1	NPCC
David Burke	UI	3	NPCC
Michele Tondalo	UI	1	NPCC
Sylvain Clermont	Hydro Quebec	1	NPCC
Si Truc Phan	Hydro Quebec	2	NPCC
Helen Lainis	IESO	2	NPCC
Laura Mcleod	NB Power	1	NPCC
MIchael Forte	Con Edison	1	NPCC
Quintin Lee	Eversource Energy	1	NPCC
Kelly Silver	Con Edison	3	NPCC
Peter Yost	Con Edison	4	NPCC
Brian O'Boyle	Con Edison	5	NPCC
Greg Campoli	NY-ISO	2	NPCC

					Kathleen Goodman	ISO-NE	2	NPCC
					Silvia Parada Mitchell	NextEra Energy, LLC	4	NPCC
					Sean Bodkin	Dominion	4	NPCC
					Michael Schiavone	National Grid	1	NPCC
					Michael Jones	National Grid	3	NPCC
Lower Colorado River Authority	Teresa Cantwell	1,5,6		LCRA Compliance	Michael Shaw	LCRA	6	Texas RE
					Dixie Wells	LCRA	5	Texas RE
					Teresa Cantwell	LCRA	1	Texas RE
Midcontinent ISO, Inc.	Terry BIlke	2		IRC-SRC	Kathleen Goodman	ISONE	2	NPCC
					Ben Li	IESO	2	NPCC
					Terry Bilke	MISO	2	RF
					Greg Campoli	NYISO	2	NPCC
					Mark Holman	PJM	2	RF
					Charles Yeung	SPP	2	SPP RE
Oxy - Occidental Chemical	Venona Greaff	7		Oxy	Venona Greaff	Occidental Chemical Corporation	7	SERC
					Michelle D'Antuono	Ingleside Cogeneration LP.	5	Texas RE

1. Do you agree with the proposed scope for Project 2016-03 as described in the SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope please provide your recommendation and explanation.	
Thomas Foltz - AEP - 3,5	
Answer	No
Comment	
AEP has two comments to offer. First, AEP suggests a broader approach to the drafting team's efforts to achieve the directive set forth by FERC. The specificity of the SAR leaves little room for debate and interpretation, as evidenced by the first draft of the standard. Specifically, AEP encourages the drafting team to allow for flexibility based on size of entity and size of vendor as well as the impact category and other attributes of the affected BES Cyber System(s). The SAR could include a statement that there are specific security vulnerabilities or controls to be addressed in a procurement or supply chain process. This may better focus the drafting team on implementing the most effective standard possible. Second, AEP recognizes the need to move quickly, but holding a technical conference on the first draft of the standard seems premature when the SAR is not yet agreed upon.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will consider your suggestions for allowing flexibility based on entity and vendor factors and asset impact category during standards development. The SAR provides the SDT with this flexibility as written. NERC determined that a technical conference could be beneficial to the SDT and industry by providing an early opportunity to discuss initial draft requirements and considerations for addressing the directives in Order No. 829. The approach has been used successfully in other projects with time-sensitive directives.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	No

Comment
We have suggestions on 1) Purpose, 2) Industry Need, 3) Brief Description 4) Detailed Description to better define this project's scope.   For Purpose, we have three recommendations A) change "supply chain management" to "supply chain risk management"; B) change "and implement a plan that includes security controls for supply chain management for" to "and implement measures for supply chain risk management for"; C) copy the final industry need sentence to the Purpose – "The new or modified Reliability Standard(s) is intended to reduce the risk of a cyber security incident affecting the reliable operation of the Bulk-Electric System." Supply chain management is the flow of goods, services and resources that involve the movement, storage and maintenance of material for work in progress. Supply chain risk management is a subset of supply chain management. For this SAR, supply chain risk management should focus on the risks associated with sourcing and servicing BES Cyber System Components from external entities. For Industry Need, we have one recommendation – change "On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven new or modified Reliability Standard(s) that addresses" to "On July 21, 2016, FERC issued Order No. 829 directing NERC to develop a forward-looking, objective-driven, risk-based new or modified Reliability Standard(s) that addresses"

For Brief Description, we have one recommendation – update the Brief Description to be consistent with our proposed changes to the Purpose and Industry Need. For Detailed Description, we have one recommendation – change “The plan may apply different controls based on the criticality of different assets (Order No. 829 at P44)” to “The plan may apply different measures based on the criticality of different assets (Order No. 829 at P44)”	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT agrees that the purpose of the project is to develop requirements that address supply chain *risk* management and has revised the SAR Purpose section and Brief Description section accordingly. The SDT does not believe the other suggested changes to the purpose section improve clarity or change the project scope. The purpose states that entities will be required to *develop and implement a plan*, which aligns with Order No. 829 directives (P 43 and 45). The SAR provides for the development of an equally effective and efficient alternative, which could include requirements for implementing measures instead of a plan. The SAR provides latitude to develop risk-based standard(s) as written. The suggested revision is not being incorporated in the SAR because it could be incorrectly attributed to FERC. The SDT does not believe the suggested change in the detailed description from 'controls' to 'measures' changes the project scope or provides additional clarity. Accordingly, the SDT is maintaining wording to align with Order No 829 P 44.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	No
Comment	
The technical guidelines may imply stricter requirements versus providing guidance.	

This has the potential to expand the scope for Low Impact BCS which impacts compliance resources. NRG strongly recommends to the SDT that they consider impact rating criteria first, and then factor in a risk based approach. NRG recommends that the SAR states correctly that the draft is a Supply Chain Risk Management Standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has incorporated 'Risk Management' wording throughout the SAR. NRG's comments will be considered during standards development.	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	
Answer	No
Comment	
Due to the possible complexity of creating a workable new standard, Reclamation recommends that a pilot program be developed to invite any entity to volunteer to test and implement a draft of the standard prior to it being finalized. During the pilot program, vendors are also invited to participate in order to work out any verification processes of the standard. Once the standard is finalized, the enforcement of the standard should apply to facilities that are rated as high impact facilities on the first year, facilities that are rated as medium impact on the second year, and facilities that are rated as low impact on the third year.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT is developing requirements to address FERC directives contained in Order No. 829 and must file new or modified standard(s) within 12 months. The SDT will not use a pilot program, but will resolve stakeholder issues using the standards development process. The SDT will consider U.S. Bureau of Reclamation's suggestions for implementation during standards development.	
faranak sarbaz - Los Angeles Department of Water and Power - 1,3,5,6	

Answer	No
Comment	

The project "**2016-03 Cyber Security Supply Chain Management "–** The four objectives listed under this new CIP standard can be better served by providing some updates in the current CIP Standards. Specifically, Objective 2 below, is already included in the current standard for CIP-005-5 R2 Interactive Remote Access Management for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity. This objective can be better served by providing updates to the CIP-005-5 Requirement R2.

Objective 3 is already provided at LADWP by its best practices processes of requiring any IT related purchases to go through a review and approval process by our Information Technology Systems Division. This objective can be better served through an update to the current CIP-003-6 Standard.

In summary, the Objectives of the Cyber Security Supply Chain Management can be efficiently and effectively implemented through updates on the current Version 5 and Version 6 CIP Standards.

Cyber Security Supply Chain Management Objectives:

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

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT is considering both development of new standards, and revisions to existing standards, in determining how to address the directives in Order No. 829.

Dermot Smyth - Con Ed - Consolidated Edison Co. of New York - 3,4,5,6 - NPCC, Group Name Con Edison	
Answer	Yes
Comment	
Answer above should be No. System not allowing me to change it. Con Edison Company of New York supports NPCC RSC's comments on this SAR.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT notes that Con Ed does not support the SAR. See response to NPCC above.	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	Yes
Comment	
Duke Energy agrees with the scope of the project, in that the scope of the project appears to stem directly from FERC Order 829. We agree with the SAR wherein the designation is made that there is a possibility that revisions to CIP standards may be a solution, and not just the creation of a new standard.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment.	
Maryclaire Yatsko - Seminole Electric Cooperative, Inc. - 1,3,4,5,6 - FRCC	
Answer	Yes

Comment	
Seminole supports the work of this team and the proposed SAR. Seminole further suggests that the SAR specifically address BES Cyber Security Information stored at vendor locations. As cloud information storage is the predominate trend, clarity of requirements for vendors related to both storage of information provided to vendors and vendor responsibilities for information stored in the cloud should be addressed at least in the Guidelines and Technical Basis.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will consider Seminole Electric Cooperative's comment during standards development.	
Johnny Anderson - IDACORP - Idaho Power Company - 1	
Answer	Yes
Comment	
Yes, we agree with the scope. However, we would like consideration given to the following: Idaho Power believes that tightening purchasing controls too tightly could also pose a risk because there are limited vendors that service its needs. The vendors that derive a large portion of their business from the electric industry would likely be willing to adapt to such new requirements. Providers that have a larger customer base may not be as willing to adjust to practices to meet any new requirements. Due to this concern, Idaho Power believes that the supply chain standard should be laid out in terms of requirements built around controls that are developed by the regulated entity rather than perspective requirements like many other CIP standards. Such flexibility would provide a foundation for the standard to evolve. Idaho Power believes that such a significant undertaking will take years to develop and implement. Idaho Power believes that such a proposal will need to clearly define the requirements of what materials should be impacted. It would also need to set forth the types of documentation that could be used to verify that requirements are met. Idaho Power and other entities would then need time to add language to its contracts to ensure compliance by its suppliers and any sub-suppliers. Idaho Power believes that such a process would require significant time, money, and resources and would result in higher costs for materials, which would impact Idaho Power's customers. Idaho Power believes it would be	

valuable for NERC to look into whether other regulatory agencies or industries have addressed such a requirement as a starting point for such reliability standards.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider them during standards development. The SDT agrees that the standard should provide flexibility for entities to determine approaches to meet the reliability objectives contained in Order No. 829. The SDT is considering guidance and reference material that includes input from government and other regulated sectors, including references cited in Order No. 829.	
Linsey Ray - Oncor Electric Delivery - NA - Not Applicable - Texas RE	
Answer	Yes
Comment	

Title of Proposed Standard(s): Cyber Security – Supply Chain Risk Management

Oncor recommends changing the title to more closely reflect the FERC directive. The intent is to manage risk associated with the supply chain. Calling out controls in the title could be interpreted as adding specific controls to the process and not fully evaluating the risks associated with the supply chain process. This is also called out in paragraph 1 of the order "… develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware…".

In addressing Objective 3 (Information system planning), the SDT shall develop requirement(s) that address the applicable entities' CIP Senior Manager (or delegate) identification and documentation of security risks for consideration by the applicable entity in proposed information system planning. (Order No. 829 at P 56)

Oncor recommends adding the word "security" to this statement. If taken out of context, the standard could be seen as opening it up to all risks associated with information system planning. This interpretation could be expanded greatly beyond the original intent of improving reliability through a secure Information Technology system. Examples of risks that should be considered 'out of scope' would include product

delivery timing and special packaging requirements. While paragraph 56 doesn't specifically call out security, the intent of Order 829 clearly focuses on ensuring the security of key BES cyber systems and components.

In addressing Objective 4 (Vendor risk management and procurement controls), the SDT shall develop requirement(s) for applicable entities to address the provision and verification of the following security concepts, at a minimum, in future contracts for industrial control system hardware, software, and computing and networking services associated with BES operations. (Order No. 829 at P 59)

Oncor recommends removing the phrase "at a minimum" from this section. The phrase could encourage an audit team to expect or request more evidence than intended by this objective. This phrase is not mentioned in paragraph 59; "verification of relevant security concepts_in future contracts for industrial control system hardware,".

Likes 0	
Dislikes 0	

Response. Thank you for your comment. The SDT has incorporated 'Risk Management' wording throughout the SAR. The SDT has revised the description for Objective 3 to address this comment. The phrase *at a minimum* in the description of objective 4 is from Order No. 829 (P 45). Because this is a SAR, the wording does not convey an obligation on entities. Oncor's comment will be considered during standards development.

Venona Greaff - Oxy - Occidental Chemical - 7, Group Name Oxy

Answer	Yes

Comment

Occidental Chemical Corporation agrees with the proposed scope of Project 2016-03 as described in the SAR but offers the following suggestions:

- Purpose section of SAR states that the project will cover "security controls for supply chain management" but should probably be revised to state that it will cover "security controls for supply chain *risk* management" to be consistent with FERC Order 829 and the Industry Need section of the SAR.

• Purpose section of SAR states that the new or modified Reliability Standard(s) will require entities to "develop and implement a plan" – the SAR shouldn't assume that the agreed upon approach will be a "plan" and should be revised to read "develop and implement measures". This will allow the SDT the most flexibility if it is later determined that a "plan" is not the best approach and will still allow for a "plan" if the entity determines that to be the best approach	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT has incorporated 'Risk Management' wording throughout the SAR. The purpose states that entities will be required to *develop and implement a plan*, which aligns with Order No. 829 directives (P 43 and 45). The SAR provides for the development of an equally effective and efficient alternative, which could include requirements for implementing measures instead of a plan.	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	Yes
Comment	
Thank you for this opportunity to provide comments on the Standards Authorization Request (SAR) written in response to Order No. 829 that will direct the development of a new or modified Reliability Standard for supply chain risk management to industrial control system hardware, software, and computing and networking services associated with Bulk Electric System (BES) operations. While FERC clearly wants to advance the state of supply chain security, we believe the inclusion of Low Impact Cyber Assets will delay the SDT's ability to make the one year filing deadline. We believe the SAR should narrow its focus to the 'highest watermark' first, to limit confusion, especially as entities prepare for implementing activities that address the Low Impact aspects of their programs. Other SDTs continue to enhance related NERC CIP standards based on changes to the definitions for Low Impact External Routable Connectivity and Transient Cyber Assets. All security advances and efficiencies designed for large-sized utilities, including their choice of software and hardware vendors, will eventually pass down to the Medium Impact Facilities, and ultimately to the Low Impact Facilities, through better IT security testing and best practices. This natural progression takes time and maturity to nurture, something we feel should be allowed reflected within in the SAR.	
Likes 0	

Dislikes 0	
Response. Thank you for your comment. The SDT will consider ACES' comments concerning Low Impact Cyber Assets during standards development.	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance	
Answer	Yes
Comment	
Objective 3 – Regarding Information System Planning - What is Information System Planning? It is not well understood. The SAR information does not adequately describe that beyond entities needing to document the risks we take into consideration. We would like to see additional description on Information System Planning.	
Likes 0	
Dislikes 0	
Response. Thank you for your comment. The SDT will consider LCRA's comment during standards development.	
Preston Walker - PJM Interconnection, L.L.C. - 2 - SERC,RF	
Answer	Yes
Comment	
PJM agrees with the language within the Project 2016-03 Cyber Security Supply Chain Management SAR and asks the SDT to consider the following comments when developing the standard. As stated within paragraph 42 of the order, PJM agrees with the APPA that the standard should be risk based as opposed to impact based. PJM also asks the SDT to consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within addressing the four objectives outlined in the order or by adding an additional objective.	
Likes 0	

Dislikes 0	
Response. Thank you for your comments. The SDT will consider PJM's comments during standards development.	
Sophia Combs - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Pamela Hunter - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	Yes
Comment	

Likes 0	
Dislikes 0	
Response	
John Williams - Tallahassee Electric (City of Tallahassee, FL) - 1,3,5	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Stephanie Little - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Leonard Kula - Independent Electricity System Operator - 2	
Answer	Yes
Comment	

Likes 0	
Dislikes 0	
Response	
Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Michelle Coon - Open Access Technology International, Inc. - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Comment	
Likes 0	
Dislikes 0	
Response	
Terry Bllke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	Yes

Comment	
Likes 0	
Dislikes 0	
Response	

2. Provide any additional comments for the Standards Drafting Team to consider, if desired.	
Teresa Cantwell - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance	
Answer	
Comment	
No additional comments	
Likes 0	
Dislikes 0	
Response	
Terry Bilke - Midcontinent ISO, Inc. - 2, Group Name IRC-SRC	
Answer	
Comment	
The IRC members ask the Standard Drafting Team (SDT) to consider the following comments when developing the standard. As stated within paragraph 42 of the order, the IRC members agree with the APPA that the standard should be risk based as opposed to impact based. The IRC members also ask the SDT to consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within the four objectives outlined in the order or by adding an additional objective.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider IRC's comments during standards development.	
Wendy Center - U.S. Bureau of Reclamation - 5 - WECC	

Answer	
Comment	
Reclamation recommends that the CIP language be written to account for existing Government procurement constraints; or exempt the government entities that are legally bound by federal procurement regulations.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider U.S. Bureau of Reclamation's comments during standards development.	
Kara Douglas - NRG - NRG Energy, Inc. - 3,4,5,6 - FRCC,MRO,WECC,Texas RE,NPCC,SERC,SPP RE,RF	
Answer	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Michelle Coon - Open Access Technology International, Inc. - NA - Not Applicable - NA - Not Applicable	
Answer	
Comment	
Open Access Technology international, Inc. (OATI) appreciates this opportunity to submit comments pertaining to the Cyber Security Supply Chain Management Standards Authorization Request (SAR). Tackling such a large and important issue is no easy feat. Yet, the standard drafting	

team has already demonstrated their commitment to this difficult and important task by creating a new draft standard for the most recent technical conference. Continued dedication to this effort will help ensure the new reliability standard is consistent and equally applicable to necessary areas of the bulk electric system.

As a committed provider of software solutions and services to the electric utility sector, OATI plans to participate in the standard drafting process to the fullest extent possible. There are significant challenges ahead that can benefit from OATI's perspective into all of the various aspects of the electric utility reliability. OATI has identified two significant challenges: consistency in application and manageability.

OATI observes a need to develop a consistent approach to applying this standard across the industry, large and small vendors, niche and cross-sector vendors. This will include taking into consideration the fact that some vendors which also focus heavily in other industries, may be less willing to accommodate a utility's need to meet this new NERC reliability standard. Smaller utilities, especially, could be presented with a "take it or leave it" proposition from vendors such as Microsoft, CISCO, or Dell. Additionally, there is a special issue presented by the widespread use of open source software in many software solutions today. A standard should not apply only to one subset of vendors/software. Rather, to avoid a discriminatory impact, the standard should be equally applicable to all in-scope vendors/ software solutions. While this issue of consistency presents many challenges, OATI stands eager to share ideas for reaching a reasonable resolution.

Another related challenge is one of manageability. To facilitate a manageable approach, OATI observes a need for NERC to establish a common baseline standard applicable to all in scope vendors/software. This should help avoid issues on both sides of the supply chain. Absent a baseline, utilities may each develop a variety of inconsistent approaches to meeting the objectives of the standard. Such inconsistency is likely to create major problems for vendors as they verify compliance with the standard. The downstream impact of such inconsistent approaches is an increased burden on vendors who may each develop a unique way to meet the objectives passed onto them. Fortunately, much work has already been completed by the Department of Energy and the National Institute of Standards and Technology in this area of supply chain security that will be helpful in defining the baseline for this industry. These existing approaches should be considered and leveraged in the development of this new CIP supply chain management standard.

OATI looks forward to working closely with NERC, industry members, and other vendors in shaping this new reliability standard. A special thanks to NERC for its inclusion of the vendors in this important and necessary effort. Together we can successfully develop a consistent and manageable standard to mitigate this cybersecurity vulnerability in the bulk electric system.

Likes 0	
Dislikes 0	

Response. Thank you for your comments and involvement in the standards development process.	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,10 - NPCC, Group Name RSC	
Answer	
Comment	
We also recommend that the SDT seriously consider updating existing CIP Standards in order to avoid creating double jeopardy for A) remote access (CIP-005 R2); B) patch management (CIP-007 R2); C) authentication (CIP-007 R5); D) vendor termination of employees (CIP-004 R5); We recommend that new Requirements do not jeopardize existing Requirements and their implementation timelines, and that new Requirements do not create additional paperwork with little value to the Reliable Operation of the Bulk Electric System.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT is considering both development of new standards, and revisions to existing standards, in determining how to address the directives in Order No. 829. The SDT will consider NPCC's comments during standards development.	
Ben Engelby - ACES Power Marketing - 6, Group Name ACES Standards Collaborators - CIP	
Answer	
Comment	

If the SDT proposes to modify Low Impact requirements, we recommend maintaining them in Attachment 1 of NERC Standard CIP-003-6. Additions to Section 3: Access Controls could be made for future patch management requirements. We believe Section 4: Cyber Security Incident Response could be modified to include vendor remote termination access within a specified timeframe. The new definition of Transient Cyber Device could also be used as the location for baseline configuration management.

We believe all Low Impact processes should be non-prescriptive and provide flexibility for registered entities to decide how to best defend against cyber security threats based on their risk analysis. There may be significant advantages and protection for industry to adopt new supply chain requirements for those entities that have multiple vendors and large support staff. We believe that BES risks and economies of scale for G&T cooperatives are minimal, based on their size and geographical location within the BES.

Thank you for your time and attention regarding this SAR.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT will consider ACES comments during standards development.

Allie Gavin - International Transmission Company Holdings Corporation - 1 - MRO,SPP RE,RF

Answer	

Comment

ITC Holdings finds this new standard to be ovrely burdensome for smaller utilities that do not have the infrastructure or staffing to perform the activities.

Likes 0	
Dislikes 0	

Response. Thank you for your comments. The SDT is developing requirements to address directives in Order No. 829. Your comments will be considered during standards development.

Leonard Kula - Independent Electricity System Operator - 2	
Answer	
Comment	
The IESO suggests the Standard Drafting Team (SDT) consider the following comments when developing the standard. As stated within paragraph 42 of the order, the IESO agrees that the standard should be risk based as opposed to impact based. The IESO also suggests the SDT consider addressing the additional threats outlined within the order in paragraphs 25 (e.g. counterfeits, tampering, etc.) and 50 (e.g. hardware integrity) either within the four objectives outlined in the order or by adding an additional objective.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider IESO's comments during standards development.	
Thomas Foltz - AEP - 3,5	
Answer	
Comment	
AEP suggests that any supply chain cyber security requirements applicable to low impact BES Cyber Systems be written in a revised CIP-003, Requirement R2, Attachment 1.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider AEP's comments during standards development.	
Michael Shaw - Lower Colorado River Authority - 1,5,6, Group Name LCRA Compliance	

Answer	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Colby Bellville - Duke Energy - 1,3,5,6 - FRCC,SERC,RF, Group Name Duke Energy	
Answer	
Comment	
We would like to point out the potential need for future modifications on other CIP standards as a result of this project. Specifically, there may be some language conflicts that arise, or duplicative controls put in place. Also, some ability will need to be afforded to entities allowing for the capability of verifying with a vendor, the integrity and authenticity of its software. Next, we feel like the language in the SAR should be revised to reflect a concentration on security controls for supply chain risk management, rather than just security controls for supply chain management. We feel the added emphasis on risk is appropriate in this context. Lastly, we want to point out to the drafting team the importance of keeping separate the topics of operations versus supply chain. We can see where instances may occur wherein the language of a standard can be intended to focus on supply chain aspects, but to the reader, may bleed over into the operations space.	
Likes 0	
Dislikes 0	
Response. Thank you for your comments. The SDT will consider Duke's comments during standards development.	

The SDT has incorporated 'Risk Management' wording throughout the SAR.
Rachel Coyne - Texas Reliability Entity, Inc. - 10
Answer
Comment
This SAR, if approved, allows the Standards Drafting Team (SDT) to develop new or modified Critical Infrastructure Protection (CIP) Standard(s) for supply chain management to address the Federal Energy Regulatory Commission (FERC) directives contained in Order No. 829. Texas RE supports developing new CIP Standard(s) to address supply chain management, which should be applicable to high, medium, and low impact BES Cyber Systems. Modifying existing CIP Standard(s) has caused confusion in the industry in regard to implementation dates. For example, CIP-003-6, added low impact Requirements, with multiple implementation dates.
Likes 0
Dislikes 0
Response. Thank you for your comments. The SDT will consider Texas RE's comments during standards development.