NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standards Authorization Request Form

When completed, email this form to:
sarcomm@nerc.com

NERC welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards. Please use this form to submit your request to propose a new or a revision to a NERC's Reliability Standard.

Request to propose a new or a revision to a Reliability Standard			
Title of Proposed Standard(s):	Cyber Security - Supply Chain Controls		
Date Submitted:	September 28, 2016		
SAR Requester Information			
Name:	Corey Sellers		
Organization:	Southern Company / Chair, SAR and Standards Drafting Team		
Telephone:	205-257-7531	E-mail:	mcseller@southernco.com
SAR Type (Check as many as applicable)			
☒ New Standard		☐ Withdrawal of existing Standard	
☒ Revision to existing Standard		☐ Urgent Action	

SAR Information
Purpose (Describe what the Standard action will achieve in support of Bulk Electric System reliability.):
The goal of this project is to establish forward-looking, objective-driven new or modified Reliability Standard(s) requiring entities to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and computing and networking services that impact Bulk Electric System (BES) operations. The project will address the Federal Energy Regulatory Commission (FERC) directives contained in Order No. 829.
Industry Need (What is the industry problem this request is trying to solve?):
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 supply chain risk management for industrial control system hardware, software, and computing and networking services associated with BES operations. The supply chains for information and communications technology and industrial control systems present risks to the BES by providing potential opportunities for the introduction of

SAR Information
cybersecurity vulnerabilities. The new or modified Reliability Standard(s) is intended to reduce the risk of a cybersecurity incident affecting the reliable operation of the Bulk-Power System.
Brief Description (Provide a paragraph that describes the scope of this Standard action.)
The Standards Drafting Team (SDT) shall develop new or modified Critical Infrastructure Protection (CIP) Standard(s) to require applicable entities to develop and implement a plan that includes security controls for supply chain management of industrial control system hardware, software, and computing and networking services that impact BES operations as described in Order No. 829. The work will include development of an Implementation Plan, Violation Risk Factors, Violation Severity Levels, and supporting documents, within the 12-month deadline established by FERC in Order No. 829.
Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR. Also provide a justification for the development or revision of the Standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the Standard action.)
The SDT shall address each of the Order No. 829 directives. The Reliability Standard(s) developed or revised in the project will require applicable entities to develop and implement a plan that addresses, at a minimum, the following four specific objectives as they relate to supply chain cybersecurity of the BES (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 plan may apply different controls based on the criticality of different assets (Order No. 829 at P 44). Requirements developed by the SDT will be aimed at the protection of aspects of the supply chain that are within the control of responsible entities (Order No. 829 at P 10). The new or modified Reliability Standard will also require periodic reassessment of the applicable entity's selected controls by the applicable entity's CIP Senior Manager at least every 15 months (Order No. 829 at P 46). In addressing Objective 1 (Software integrity and authenticity), the SDT shall develop requirement(s) for applicable entities to address verification of: (1) the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; and (2) the integrity of the software and patches before they are installed in the BES Cyber System. (Order No. 829 at P 48) In addressing Objective 2 (Vendor remote access), the SDT shall develop requirement(s) for applicable entities to address logging and controlling all third-party (i.e., vendor) initiated remote access sessions. The objective covers both user-initiated and machine-to-machine vendor remote access. Additionally,

SAR Information
applicable entities' controls must provide for rapidly disabling remote access sessions to mitigate a security event, if necessary. (Order No. 829 at P 51 and 52) 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 risks for consideration by the applicable entity in proposed information system planning. (Order No. 829 at P 56) 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) • Vendor security event notification processes; • Vendor personnel termination notification for employees with access to remote and onsite systems; • Product/services vulnerability disclosures, such as accounts that are able to bypass authentication or the presence of hardcoded passwords; • Coordinated incident response activities; and • Other related aspects of procurement that the SDT determines should be addressed for supply chain cyber security risk management as stated in Order No. 829. The SDT may, as an alternative, propose an equally efficient and effective means to meet the objectives in Order No. 829.

Reliability Functions	
The Standard will Apply to the Following Functions (Check each one that applies.)	
☐ Regional Reliability Organization	Conducts the regional activities related to planning and operations, and coordinates activities of Responsible Entities to secure the reliability of the Bulk Electric System within the region and adjacent regions.
☒ Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
☒ Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.

Reliability Functions		
☐	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
☐	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
☐	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
☐	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
☐	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
☒	Transmission Owner	Owns and maintains transmission facilities.
☒	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
☒	Distribution Provider	Delivers electrical energy to the End-use customer.
☒	Generator Owner	Owns and maintains generation facilities.
☒	Generator Operator	Operates generation unit(s) to provide real and Reactive Power.
☐	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
☐	Market Operator	Interface point for reliability functions with commercial functions.
☐	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Reliability and Market Interface Principles	
Applicable Reliability Principles (Check all that apply).	
☐	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
☐	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and Reactive Power supply and demand.

Reliability and Market Interface Principles	
☐	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
☐	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
☒	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
☐	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
☐	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
☒	8. Bulk power systems shall be protected from malicious physical or cyber attacks.

Does the proposed Standard comply with all of the following Market Interface Principles?	Enter (yes/no)
1. A Reliability Standard shall not give any market participant an unfair competitive advantage.	YES
2. A Reliability Standard shall neither mandate nor prohibit any specific market structure.	YES
3. A Reliability Standard shall not preclude market solutions to achieving compliance with that Standard.	YES
4. A Reliability Standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with Reliability Standards.	YES

Related Standards	
Standard No.	Explanation
CIP-002-5	Cyber Security - BES Cyber System Categorization. Specifies categorization of BES Cyber Systems and BES Cyber Assets to support appropriate protection against compromises that could lead to misoperation or instability in the BES.
CIP-003-6	Cyber Security - Security Management Controls. Establishes responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in BES
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-007-6	Cyber Security - System Security Management

Related Standards	
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security - Information Protection

Related SARs	
SAR ID	Explanation

Regional Variances	
Region	Explanation
FRCC	
MRO	
NPCC	
RF	
SERC	
SPP RE	
Texas RE	
WECC	