NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Authorization Request (SAR)

Complete and please email this form, with attachment(s) to: sarcomm@nerc.net

The North American Electric Reliability Corporation (NERC) welcomes suggestions to improve the reliability of the bulk power system through improved Reliability Standards.

Requested information			
SAR Title:	BES Cyber System Information Access Management		
Date Submitted:	March 1, 2019		
SAR Requester			
Name:	Alice Ireland		
Organization:	Tri-State Generation and Transmission Association		
Telephone:	(303) 254-3120	Email:	aireland@tristategt.org
SAR Type (Check as many as apply)			
☐ New Standard ☒ Revision to Existing Standard ☐ Add, Modify or Retire a Glossary Term ☐ Withdraw/retire an Existing Standard		☐ Imminent Action/ Confidential Issue (SPM Section 10) ☐ Variance development or revision ☐ Other (Please specify)	
Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)			
☐ Regulatory Initiation ☐ Emerging Risk (Reliability Issues Steering Committee) Identified ☐ Reliability Standard Development Plan		☒ NERC Standing Committee Identified ☐ Enhanced Periodic Review Initiated ☒ Industry Stakeholder Identified	
Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
~~While there is no direct benefit to the reliability of the BES, t~~This initiative enhances BES reliability by creating increased choice, greater flexibility, higher availability, and reduced-cost options for entities to manage their BES Cyber System Information, by providing a secure path towards utili~~t~~zation of modern third-party data storage and analysis systems. In addition, the proposed project would clarify the protections expected when utilizing third-party solutions (e.g.,~~aka~~ cloud services).			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Clarifying the CIP requirements and measures related to both managing access~~ing~~ and securing BES Cyber System Information~~ access, to allow for alternative methods, such as encryption, to be utilized in the protection of BCSI~~.			
Project Scope (Define the parameters of the proposed project):			
The scope of this project is to consider ~~revisions modifications of~~ CIP-004 and CIP-011 modifications, and review the NERC Glossary of Terms as it pertains to Requirements addressing BCSI.			

Requested information
Detailed Description (Describe the proposed deliverable(s) with sufficient detail for a drafting team to execute the project. If you propose a new or substantially revised Reliability Standard or definition, provide: (1) a technical justification[1]which includes a discussion of the reliability-related benefits of developing a new or revised Reliability Standard or definition, and (2) a technical foundation document (*e.g.* research paper) to guide development of the Standard or definition):
CIP-004-6 Requirements ~~R4 Part 4.1.3~~ needs ~~to~~ be modified so ~~authorization~~ management of ~~and~~ access to BCSI is clarified to include a focus on the BCSI data and the controls deployed to limit access. In addition, the Standard should allow ~~multiple~~ various methods for controlling access to BES Cyber System Information, ~~rather than just electronic and physical access to the BES Cyber System Information~~ storage location(s). ~~For example, t~~The focus must be on BCSI and the ability to obtain and make use of it. This is particularly necessary when it comes to the utilization of a third party's system (e.g.~~aka~~ cloud services). ~~As currently drafted, t~~The current ~~r~~Requirements ~~is~~are focused on access to the "storage location", ~~and~~ but should not consider management of access to BCSI while in transit, storage, and in use. ~~therefore does not permit methods such as encryption and key management to be utilized in lieu of physical/electronic access controls. This wording also does not explicitly permit any flexibility in the audit approach.~~ In addition to ~~modifying~~ CIP-004-6 modifications, ~~Requirement R4 Part 4.1.3, Part 4.4, Part 5.3 and~~ CIP-011-2 ~~Requirement R1~~ should also be evaluated for any subsequent impacts ~~to the requirements, measures and/or the guidelines and technical basis~~.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Potential cost savings due to economies of scale and third party support.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g*. Dispersed Generation Resources):
SAR Drafting Team asserts there are no unique characteristics associated with BES facilities that will be impacted by this proposed standard development project.
To assist the NERC Standards Committee in appointing a drafting team with the appropriate members, please indicate to which Functional Entities the proposed standard(s) should apply (*e.g*. Transmission Operator, Reliability Coordinator, etc. See the most recent version of the NERC Functional Model for definitions):
Please see Section 4. Applicability of CIP-004-6 and CIP-011-2.
Do you know of any ~~i~~consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
An informal team, under the direction of the NERC Compliance Input Working Group, was assembled to review the use of encryption on BES Cyber System Information, and the impact on compliance, with a particular focus on such BES Cyber System Information being stored or utilized by a third party's system

[1] The NERC Rules of Procedure require a technical justification for new or substantially revised Reliability Standards. Please attach pertinent information to this form before submittal to NERC.

[2] Consensus building activities are occasionally conducted by NERC and/or project review teams. They typically are conducted to obtain industry inputs prior to proposing any standard development project to revise, or develop a standard or definition.

Requested information

(aka cloud). This team met every two weeks during Dec. 2018 – Feb. 2019. The development of this SAR was supported by all team members. The team consisted of the following individuals:

Name	Company
Alice Ireland (lead)	Tri-State Generation and Transmission
David Vitkus	Tucson Electric Power
Eric Hull	SMUD
Marina Rohnow	Sempra Utilities/ San Diego Gas & Electric
Paul Haase	Seattle City Light
Richie Field	Hoosier Energy REC, Inc.
Rob Ellis	Tri-State Generation and Transmission
Steve Wesling	Tri-State Generation and Transmission
Toley Clague	Portland General Electric
Ziad Dassouki	ATCO Electric
Joseph Baxter	NERC Observer
Lonnie Ratliff	NERC Observer
Brian Kinstad	MRO Observer
Holly Eddy	WECC Observer
Kenath Carver	Texas Reliability Entity, Inc. Observer
Michael Taube	MRO Observer
Mike Stuetzle	NPCC Observer
Morgan King	WECC Observer
Shon Austin	Reliability First Observer
Tremayne Brown	SERC Observer

Are there any related standards or SARs that should be assessed for impact as a result of this proposed project? If so which standard(s) or project number(s)?

Project 2016-02 Modifications to CIP Standards

Are there alternatives (e.g. guidelines, white paper, alerts, etc.) that have been considered or could meet the objectives? If so, please list the alternatives.

When evaluating ways to modify the requirement, other standards and requirements were identified, which provide examples on possible paths forward. These examples are not intended to limit the SDT from developing other more effective solutions.

Requested information

Of particular relevance are the following standards/requirements:

- CIP-006-6 Requirement R1 Part 1.10;
- CIP-010-2 Requirement R4, Attachment 1, Section 1.5;
- CIP-012-1 Requirement R1 (pending FERC approval).

As a means to assist the SDT, several possible options for revision to CIP-004-6 Requirement R4 Part 4.1.3 have been drafted and provided below:

EXAMPLE #1:
[Delete 4.1.3 and create a new subrequirement in either CIP-004 or CIP-011, that would read something like this:]
R4.X Process to prevent unauthorized access to BES Cyber System Information. The process shall include:
4.X.1. Identification of physical and electronic repositories utilized to store BES Cyber System Information. If electronic, indicate whether the repository is hosted by the Responsible Entity or a third-party and also whether it is in a virtual or non-virtual environment.;
4.X.2. Identification of security protection(s) used to prevent unauthorized access to BES Cyber System Information within each repository. Examples may include but are not limited to the following:

- Encryption and key management,
- Physical access management,
- Electronic access management,
- Data loss prevention techniques and rights management services.

4.X.3. The process to authorize access to BES Cyber System Information, based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances;

EXAMPLE #2:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;
4.1.3. Physical access to physical BES Cyber System Information storage locations;
4.1.4. Physical access to unencrypted electronic BES Cyber System Information storage locations;
4.1.5. Electronic access to unencrypted electronic BES Cyber System Information storage locations; and
4.1.6. Electronic access to BES Cyber System Information encryption keys for encrypted BES Cyber System Information.

EXAMPLE #3:
R4.1 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:
4.1.1. Electronic access;
4.1.2. Unescorted physical access into a Physical Security Perimeter;

Requested information
4.1.3. Physical access to physical BES Cyber System Information storage locations; 4.1.4. Access to electronic BES Cyber System Information.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability Interface Principles)? Please check all those 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.
☐	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.

Market Interface Principles	
Does the proposed standard development project 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

Identified Existing or Potential Regional or Interconnection Variances	
Region(s)/ Interconnection	Explanation
e.g. NPCC	

For Use by NERC Only

SAR Status Tracking (Check off as appropriate)	
☐ Draft SAR reviewed by NERC Staff ☐ Draft SAR presented to SC for acceptance ☐ DRAFT SAR approved for posting by the SC	☐ Final SAR endorsed by the SC ☐ SAR assigned a Standards Project by NERC ☐ SAR denied or proposed as Guidance document

Version History

Version	Date	Owner	Change Tracking
1	June 3, 2013		Revised
1	August 29, 2014	Standards Information Staff	Updated template
2	January 18, 2017	Standards Information Staff	Revised
2	June 28, 2017	Standards Information Staff	Updated template