Standard Authorization Request (SAR)

Complete and submit this form, with attachment(s) to the NERC Help Desk. Upon entering the Captcha, please type in your contact information, and attach the SAR to your ticket. Once submitted, you will receive a confirmation number which you can use to track your request.

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:	Coordinated cyber attack controls for low impact BES Cyber Assets		
Date Submitted:	12/20/2022 **(Revised 07/25/2023)**		
SAR Requester			
Name:	Howard Gugel (LICRT) **(Revised by Jeffrey Sweet, Project 2023-04 SDT)**		
Organization:	~~NERC~~**Project 2023-04 Modifications to CIP-003 SDT**		
Telephone:	~~404-446-9693~~**614-716-3059**	Email:	~~Howard.gugel@nerc.net~~**jjsweet@aep.com**

SAR Type (Check as many as apply)	
☐ New Standard	☐ Imminent Action/ Confidential Issue (SPM Section 10)
☒ Revision to Existing Standard	☐ Variance development or revision
☒ Add, Modify or Retire a Glossary Term	☐ Other (Please specify)
☐ Withdraw/retire an Existing Standard	

Justification for this proposed standard development project (Check all that apply to help NERC prioritize development)	
☐ Regulatory Initiation	☐ NERC Standing Committee Identified
☒ Emerging Risk (Reliability Issues Steering Committee) Identified	☐ Enhanced Periodic Review Initiated
☐ Reliability Standard Development Plan	☒ Industry Stakeholder Identified

Industry Need (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):

In light of recent cybersecurity events and the evolving threat landscape, the NERC Board took action at its February 4, 2021 meeting to direct NERC staff, working with stakeholders, to expeditiously complete its broader review and analysis on facilities that house low impact BES Cyber Assets. Specifically, the degrees of risk presented by various facilities that house the low impact BES Cyber Assets and report on whether the low impact criteria should be modified. To assist in this evaluation, NERC staff assembled a team of cybersecurity experts and compliance experts representative of a cross section of industry, called the Low Impact Criteria Review Team (LICRT). The LICRT's primary purpose was to discuss the potential threat and risk posed by a coordinated cyber attack on low impact BES Cyber Systems. In its report, the LICRT documented the results of the review and analysis of degrees of risk presented by various facilities that meet the criteria that define low impact cyber facilities and recommends actions to address those risks. The Board accepted the LICRT's report at its November 2022 meeting and asked that the recommendations in the report be initiated. The report may be found here.

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
The LICRT conclusions regarding low impact BES Cyber Systems are as follows: • Individually, low impact BES Cyber Systems are truly low impact to BES reliability. This corresponds to the longstanding work of NERC and the stakeholders to design and operate the BES to withstand the loss of any of its individual assets. A medium or high impact BES Cyber System is more than an impact to a typical single BES Element/Facility. Therefore, the team does not recommend changing the CIP-002 impact rating criteria used in identifying and categorizing individual BES Cyber Systems. • The team recognizes that low impact BES Cyber Systems may introduce BES reliability risks of a higher impact where distributed low impact BES Cyber Systems are used for a coordinated attack. The team recommends enhancing the existing low impact category to further mitigate the coordinated attack risk.
Project Scope (Define the parameters of the proposed project):
Modify CIP-003-9 to add controls ~~to authenticate remote users, protect the authentication information in transit, and detect malicious communications assets~~ ~~containing low impact BES Cyber Systems with external routable connectivity.~~**as outlined in the Detailed Description section below.**
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):
Modify CIP-003-9 to add: • Requirement(s) for authentication of remote users before access is granted to networks containing low impact BES Cyber Systems ~~at assets containing those systems that have external~~**using a** routable ~~connectivity~~**protocol from outside the asset containing low impact BES Cyber Systems**. • Requirement(s) for protection of user authentication information in transit for remote access to **networks containing** low impact BES Cyber Systems ~~at assets containing those systems that have external~~**using a** routable ~~connectivity~~**protocol from outside the asset containing low impact BES Cyber Systems**. • Requirement(s) for detection of **known or suspected** malicious communications ~~to/between assets containing low impact BES Cyber Systems with external routable connectivity~~**for both inbound and outbound electronic access as defined in CIP-003-9 Attachment 1, Section 3.1**. To limit the scope of the requirements to only those that have external routable connectivity, the

[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.

Requested information
drafting team may need to create a new defined term or modify an existing defined term. For a complete technical justification and technical foundation, please refer to the Low Impact Criteria Review Report.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Cost impacts are unknown at this time.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
None
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):
Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Reliability Coordinator, Transmission Operator, Transmission Owner
Do you know of any consensus building activities[2] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
The white paper was developed by industry experts and posted for industry comment prior to being presented to the Board.
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)?
If not completed by the initiation of this SAR: 2016-02 Modifications to CIP Standards 2021-03 CIP-002 Transmission Owner Control Centers
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.

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.

[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.

Reliability Principles	
☐	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	none

For Use by NERC Only

SAR Status Tracking (Check off as appropriate).	
☐☒ Draft SAR reviewed by NERC Staff	☐ Final SAR endorsed by the SC
☐☒ Draft SAR presented to SC for acceptance	☐ SAR assigned a Standards Project by NERC
☐☒ DRAFT SAR approved for posting by the SC	☐ 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
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer