NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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:	CIP-008 Reporting Threshold		
Date Submitted:	18 July, 2022 (April 12, 2023)		
SAR Requester			
Name:	Michaelson Buchanan (Revised by the Project 2022-05 SAR DT)		
Organization:	NERC		
Telephone:	470.725.5268	Email:	Michaelson.buchanan@nerc.net
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?):			
Improve awareness of existing and future cyber security risk to the BES.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
Since the effective date of CIP-008-6 there has not been a perceived ~~material~~ change in the number of Reportable Cyber Security Incidents or Cyber Security Incidents that were determined to be an attempt to compromise an applicable system. This project will identify and address potential gaps in CIP-008-6 permitting a subjective determination of attempt(s) to compromise.			
Project Scope (Define the parameters of the proposed project):			
The Standards Drafting Team (SDT) will modify the Reliability Standards and/or associated definitions as necessary to provide~~s~~ clarity on what constitutes an ~~a minimum expectation for thresholds to support the definition of~~ attempt to compromise. Modifications should be focused on CIP-008-6. The SDT will consider and modify if~~, however, it may be~~ necessary ~~to modify~~ other related standards ~~for consistency~~.			

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):
Reliability Standard CIP-008-6 became effective on January 1, 2021, in response to FERC Order No. 848[3] directing NERC to develop modifications to the Reliability Standards to require reporting of Cyber Security Incidents and attempt(s) to compromise a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS). In Q3 2021, the ERO Enterprise initiated a study to better understand how registered entities have implemented Reliability Standard CIP-008-6; specifically, how the registered entities have interpreted Reportable Cyber Security Incidents and defined attempt(s) to compromise. The study concluded the current language of the Reliability Standard permits the use of subjective criteria to define attempt(s) to compromise, and most programs include a provision allowing a level of staff discretion. Reliability Standard CIP-008-6 or definitions should be modified to provide a minimum expectation for thresholds defining attempt to compromise. ~~To accomplish this, CIP-008-6 R1 Part 1.2.1 could be modified to read, "…That include criteria to evaluate and define attempts to compromise which include, at a minimum, each of the following types of cyber security incidents:…". Conversely, it may be possible to modify the NERC Glossary definition of Reportable Cyber Security Incident to include attempt to compromise along with threshold criteria. There are other examples in the NERC Glossary of Terms, such as Removable Media which include minimum expectation examples. These are examples and not the only possible solutions. Regardless of the approach, thresholds should not be so prescriptive as to require the reporting of every internet facing firewall port scan, phishing email identified, or file alerted by endpoint anti-virus scans. Rather, the intent would be to right size the reporting threshold to improve awareness of existing and future cyber security risks to the BES.~~
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
~~No additional~~The cost impact to entities is unknown at this ~~outside of the~~ time, ~~and resources needed to serve on the Standard Drafting Team are expected. H~~however~~,~~ a question will be asked during all ~~the SAR~~ comment periods to receive entity input and ensure all aspects are considered.
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

[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
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.
In Q3-2021, the NERC Compliance Assurance and ERO Enterprise initiated a study to better understand how registered entities have implemented Reliability Standard CIP-008-6 in response to modifications; specifically, how the registered entities are interpreting Reportable Cyber Security Incidents and defining attempt(s) to compromise. The study team reviewed previous compliance monitoring engagements to analyze ERO Enterprise CMEP data and conducted a questionnaire engagement with approximately 30 registered entities through voluntary mechanisms (e.g., entity engagements, webinars, onsite visits, etc.). The questionnaires focused on four key areas: 1) criteria for reporting and key definitions, 2) organizational internal controls, 3) training and tools, and 4) reporting. The study concluded that the current language of the Reliability Standard permits the use of subjective criteria to define attempt to compromise, and most programs included a provision which allows a level of discretion by staff. Other aspects of the CIP-008 Reliability Standard were found to be sufficient.
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 includes modifications to the applicable systems listed in CIP-008-6. ~~Once approved, CIP-008-6 will increment to CIP-008-7.~~
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.
None.

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.

[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.
[3] Cyber Security Incident Reporting Reliability Standards, Order No. 848, 164 FERC ¶ 61,033 (2018).

Reliability Principles	
☒	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
N/A	

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
3	February 22, 2019	Standards Information Staff	Added instructions to submit via Help Desk
4	February 25, 2020	Standards Information Staff	Updated template footer