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:	Revisions to CIP-008-5 Cyber Security- Incident Reporting and Response Planning		
Date Submitted:	August 6, 2018		
SAR Requester			
Name:	Soo Jin Kim		
Organization:	NERC		
Telephone:	404.831.4765	Email:	Soo.jin.kim@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?):			
On July 19, 2018, the Federal Energy Regulatory Commission (FERC) issued Order No. 848 in order to augment the mandatory reporting of Cyber Security Incidents.			
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):			
This project will address the directives issued by FERC in Order No. 848 in order to augment mandatory reporting of Cyber Security Incidents, including attempts that might facilitate subsequent efforts to harm the reliable operation of the Bulk Electric System (BES). FERC directed NERC to develop and submit modifications that would "require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMs)." NERC was directed to submit the modifications within 6 months of the effective date of the final order.			

Requested information
Project Scope (Define the parameters of the proposed project):
The Standards Drafting Team (SDT) for Project 2018-02 will address FERC's directives in Order No. 848 that require developing or modifying existing Reliability Standards and associated definitions to augment the reporting of Cyber Security Incidents. The scope of any new reporting requirement will be tailored to provide better information on cyber security threats and vulnerabilities without imposing an undue burden on responsible entities.
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):
The SDT shall address the Order No. 848 directives. The Reliability Standard(s) developed or revised will include the 4 elements outlined by FERC: 1. responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS; 2. required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; 3. establish deadlines for filing Cyber Security Incidents that are commensurate with incident severity; and 4. Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). With regard to identifying EACMS for reporting purposes, the Commission stated that the reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. The Commission specified that, at a minimum, those functions must include: 1. authentication; 2. monitoring and logging; 3. access control; 4. interactive remote access; and 5. alerting.

[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
With regard to the definition of "attempted compromise" for reporting purposes, the Commission stated that it considers attempted compromise to include unauthorized access attempts or other confirmed suspicious activity. With regard to content to be included in each report, the Commission stated that the minimum set of attributes to be reported must include: 1. The the functional impact, where possible to determine, that the Cyber Security Incident achieved or attempted to achieve; 2. the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and 3. the level of intrusion that was achieved or attempted as a result of the Cyber Security Incident.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
No additional cost outside of the time and resources needed to serve on the Standard Drafting Team are expected. However, a question will be asked during the SAR comment period to 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
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.
No consensus building has been completed to date.
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 is currently working on addressing FERC directives and the V5TAG Transition document which include potential modifications to the ESP and EACMS definitions.
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.

NA

[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	
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
NA	

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