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:	Internal Network Security Monitoring (INSM)		
Date Submitted:	March 7, 2023		
SAR Requester			
Name:	Michaelson Buchanan, Dan Goodlett, Larry Collier		
Organization:	NERC		
Telephone:	470.725.5268, 470.522.7367, 470.716.2923	Email:	Michaelson.buchanan@nerc.net Dan.goodlett@nerc.net Larry.Collier@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?):			
While the CIP Reliability Standards require monitoring of the Electronic Security Perimeter and associated systems for high and medium impact Bulk Electric System (BES) Cyber Systems, the CIP-networked environment remains vulnerable to attacks that bypass network perimeter-based security controls traditionally used to identify the early phases of an attack. This presents a gap in the currently effective CIP Reliability Standards. To address this gap, CIP Reliability Standards should be created or modified to require INSM for all high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC) to ensure the detection of anomalous network activity indicative of an attack in progress. These provisions will increase the probability of early detection and allow for quicker mitigation and recovery from an attack. Current CIP Reliability Standards are insufficient to protect against insider threats or vulnerabilities that are exploited through supply chain attacks such as SolarWinds.			

Requested information
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
As directed by FERC Order No. 887, modify or create new Standard(s) that require INSM within a trusted Critical Infrastructure Protection networked environment for all high impact BES Cyber Systems with and without ERC and medium impact BES Cyber Systems with ERC.
Project Scope (Define the parameters of the proposed project):
The Standard Drafting Team (SDT) will create or modify the Reliability Standards and associated definitions as necessary to comply with the FERC order. The scope of the project will include: • All high impact BES Cyber Systems, and • All medium impact BES Cyber Systems with ERC The scope of the project should not extend to: • medium Impact BES Cyber Systems without ERC or • low impact BES cyber systems The ERO is in the process of completing a feasibility study, pursuant to the Order, which will examine the risks, challenges and potential solutions for those BES Cyber systems not in scope.
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):
Create new or modified existing CIP Reliability Standards that are forward-looking, objective-based, and that address the following three security objectives that pertain to INSM. First, any new or modified CIP Reliability Standards should address the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment. Second, any new or modified CIP Reliability Standards should address the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment. And third, any new or modified CIP Reliability Standards should require responsible entities to identify anomalous activity to a high level of confidence by: (1) logging network traffic (note that packet capture is one means of accomplishing this goal); (2) maintaining logs and other data collected regarding network traffic; and (3) implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices.
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):

[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
Beyond the time and resources needed to serve on the Standard Drafting Team, the cost to entities will vary based on their current system architecture. While many entities may have the controls in place, others may not which could require a significant cost investment depending on their footprint.
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):
Applicability will be the same as current CIP standards - Balancing Authority, Distribution Provider, Generator Operator, Generator Owner, Interchange Coordinator, Interchange Authority, 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 SAR has been developed in response to FERC Order No. 887. The final Order was consistent with feedback provided by NERC and industry through the NOPR process. NERC and the ERO Enterprise have convened a response team to address directives in the FERC Order which included a review of this SAR.
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)?
The following projects and Reliability standards should be assessed for impact: • Projects 2016-02, 2019-03 and 2022-05 • Reliability Standards CIP-005-7, CIP-010-4, and CIP-013-2
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.
This Standards Authorization Request has been developed pursuant to FERC Order No. 887.

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.

[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	
☐	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
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