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:	Cyber Security - Risk Management for Third-Party Cloud Services		
Date Submitted:	July 25, 2023 (Revised November 14,2024)		
SAR Requester			
Name:	• Rudolf Pawul, Vice President Information & Cyber Security Services • Joseph Mosher, NERC Portfolio Manager • (Revised by the 2023-09 Drafting Team)		
Organization:	• ISO New England and the ISO-RTO Council IT Committee • EDF Renewables		
Telephone:	R. Pawul: 413-540-4249 J. Mosher: 470.985.4050	Email:	rpawul@iso-ne.com joseph.mosher@edf-re.com
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	
What is the risk to the Bulk Electric System (What Bulk Electric System (BES) reliability benefit does the proposed project provide?):			
From a security perspective, the electric industry landscape is facing an increase in the number and sophistication of cyberattacks. Security teams are seeking tools and capabilities to improve their security programs. Security solutions with additional visibility, detection, correlation, analytics, and responsiveness are available using cloud services to help security teams to reduce potential impacts of security events and speed recovery while also protecting data confidentiality and integrity. Cloud services can provide additional solutions for increased resiliency scalability, redundancy, high availability, and fault tolerance. Cloud services play a critical role in providing increased vendor choices			

Requested information
for security solutions. Additionally, as noted in the 2020 FERC Notice of Inquiry[1], "SPP stated that it evaluated a number of products that would enable it to do a better job of protecting system data. SPP asserted the view that the currently effective CIP Reliability Standards do not allow cloud-based technologies despite the fact that the vast majority of new products from many of its vendors are cloud-based." Concurrently, from an operational and reliability perspective, the modern power grid landscape is changing, driven by rapid grid modernization, digital transformation, decentralization of electric resources and decarbonization targets. These factors are increasing the data volumes required to continue operating a reliable and resilient grid and thus increasing the need for data analytics and resources such as computing, network, and storage. As explained in NERC's 2019 whitepaper on "Virtualization and Future Technologies," the reliance on physical assets in the current standards prevents the use of cloud services in a compliant manner for some systems such as those defined as BES Cyber Systems or EACMS. Entity operations for assets across the NERC CIP impact levels will be facing the growing demands for computing capacity to manage the increasing volumes of data to respond to grid variability and maintain reliable grid operations. Agility and scalability will be a growing necessity to meet changing demands of grid operations, and cloud resources offer solutions to meeting such demands. Renewable capacity expansion is accelerating. The International Energy Agency updated its growth projections in 2022, to an estimate of 359.5 GW in renewable capacity growth in the US, 2022-2027[2]. As renewable installations grow, site classifications may change from low to medium impact levels, putting operators at risk of having to implement on-premises resources to meet compliance language rather than continuing to utilize the cloud services available to lower impact sites. With the advent of Phasor Measurement Units (PMUs), and other modeling sources, the unprecedented need for rapid simulations to integrate renewables into a constrained network demand unprecedented amounts of data storage. Increasing data storage requirements and processing requirements of grid modernization are driving the need for cloud services. Cloud resources provide Entities with feasible options for simulation and analysis. Cloud services offer additional options for fault-tolerant system design capabilities in which operations and data, such as BCSI can be replicated and run in geographically dispersed locations.
Purpose or Goal (What are the reliability gap(s) or risk(s) to the Bulk Electric System being addressed, and how does this proposed project provide the reliability-related benefit described above?):
The project purpose is to establish risk-based, outcome-driven requirements that enable but not require cloud services to be used for CIP-regulated systems while maintaining reliability, resiliency and security.

[1] Docket No. RM20-8-000 Virtualization and Cloud Computing Services, February 20, 2020, paragraph 12.
[2] https://www.iea.org/reports/renewables-2022/executive-summary

Requested information

The goals also include consideration of the role of third-party certifications.

These revisions will maintain reliability and security to the Bulk Electric System (BES) while allowing the use of cloud-based technologies that support Entities in managing the changing grid landscape, as well as providing security teams resources that can reduce potential impact and speed recovery from security events.

Project Scope (Define the parameters of the proposed project):

The project scope is to:

- Create a new CIP standard(s) or revise the existing CIP standards, as appropriate, to allow for adoption of cloud services for CIP-regulated systems while maintaining appropriate levels of reliability, resiliency and security.
- Determine a development plan to define whether revisions will be made to accommodate use of cloud for all CIP defined systems (such as EACMS, PACS, BCS, etc.) or if an incremental revisions approach will be taken to allow use of cloud for individual or groups of CIP-defined systems (such as first revising the standards to allow for EACMS use of cloud services).
- Assess the applicability of the existing glossary terms and revise existing terms or create new ones as needed for use with third-party cloud services.
- Coordinate with other CIP project drafting teams on conflicts or continuity matters, as necessary.

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[3] of developing a new or revised Reliability Standard or definition, which includes a discussion of the risk and impact to reliability-of the BES, and (2) a technical foundation document (*e.g.,* research paper) to guide development of the Standard or definition):

The following describes the proposed deliverables for this project:

The DT will strive to minimize impacts to existing requirements for on-premises systems and assets under the existing CIP-002 through CIP-015 suite of standards.

The Drafting Team will consider risks related to cloud services for CIP applicable systems, including but not limited to:

- Procurement / supply chain controls
- Reliability / operational risk / resilience
- Compliance / enforcement risk
- Data sovereignty
- Life cycle
- Key management
- Cloud ramping / communications

[3] 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
○ Concentrated Span of control ○ Reliance on indirect services ○ Multi-tenancy ○ Regional considerations ○ Blackstart scenarios • Holistic or incremental - The DT will evaluate revision approaches and determine whether to develop requirements applicable to use of cloud for all CIP-defined systems (such as EACMS, PACS, BCS, etc.), or to develop incremental revisions to allow use of cloud for individual or groups of CIP-defined systems (for example, first revising the standards to allow for EACMS use of cloud services). • Auditability and use of third-party certifications – the DT will consider the role of third-party certification and attestations and will consider incorporating language in the standard(s) as appropriate to clarify their use. • Timing – The revised or new standard(s) is to be delivered in a timely manner and the team will consider the possibility for early adoption ahead of any proposed effective date. The following list, which is not meant to be all-inclusive, may serve as reference documents for the DT: • SITES BES Operations in the Cloud whitepaper • IEEE Practical Adoption of Cloud Computing in Power Systems- Drivers, Challenges, Guidance, and Real-world Use Cases • NERC informational filing to FERC in December 2021 • The NIST Definition of Cloud Computing • Security Guideline for the Electricity Sector – Supply Chain • Security Guideline BCS Cloud Encryption • Implementation Guidance: Usage of Cloud Solutions for BES Cyber System Information (BCSI) • DOD Cybersecurity Reciprocity Playbook
Cost Impact Assessment, if known (Provide a paragraph describing the potential cost impacts associated with the proposed project):
Responsible Entities that implement CIP-regulated workloads in the cloud may incur costs related to compliance program revisions, as implementation of Cloud use will be optional.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
DT asserts there are no currently identified 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 NERC Rules of Procedure Appendix 5A:
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider

Requested information
Do you know of any consensus building activities[4] in connection with this SAR? If so, please provide any recommendations or findings resulting from the consensus building activity.
This SAR was informally shared with a wide network of stakeholders across industry to gather feedback. Updates were made to refine the SAR content based on that feedback. Respondents support development of this SAR and its submittal to NERC.
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)?
This project has the potential to impact current versions of the following NERC CIP Standards: CIP-002, CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, CIP-009, CIP-010, CIP-011, CIP-012, CIP-013, CIP-014, and CIP-015. This project also has the potential to impact Project 2021-03.
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 with the benefits of using them.
No alternatives were identified. As explained in NERC's 2019 whitepaper on "Virtualization and Future Technologies," the reliance on physical assets in the current standards prevents the use of cloud services in a compliant manner for some systems such as those defined as BES Cyber Systems or EACMS.

Reliability Principles	
Does this proposed standard development project support at least one of the following Reliability Principles (Reliability 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.

[4] 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.

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
None Identified.	

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
Risk Tracking.	
☐ Grid Transformation ☐ Resilience/Extreme Events	☐ Energy Policy ☐ Critical Infrastructure Interdependencies
☐ Security Risks	

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
5	August 14, 2023	Standards Development Staff	Updated template as part of Standards Process Stakeholder Engagement Group
6	June 4, 2023	Standards Information Staff	Updated link to the NERC Reliability Principles