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		
SAR Requester			
Name:	• Rudolf Pawul, Vice President Information & Cyber Security Services • Joseph Mosher, NERC Portfolio Manager		
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	☐ 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?):

From a security perspective, the electric industry landscape is facing an increase in the number and sophistication of cyberattacks and security teams are seeking tools and capabilities to improve their security programs. Security solutions with greater 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 increased availability including resiliency due to the scalability, redundancy, high availability, and fault tolerance. Cloud services play a critical role in providing greater capability across the security domains. Additionally, as noted in the 2020 FERC Notice of Inquiry[1], the vast majority of

[1] Docket No. RM20-8-000 Virtualization and Cloud Computing Services, February 20, 2020, paragraphs 12 and 19.

Requested information

new products from vendors are cloud-based solutions placing increased pressure on NERC registered entities to securely operate the BES.

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.

The U.S. Energy Information Administration projects that renewable generation will supply 44% of U.S. electricity by 2050[2]. To fully realize the national energy system decarbonization goals established by U.S. Federal and state Government Agencies, rapid deployment and integration of net zero energy systems will rely on advanced monitoring, control, and data methodologies, such as machine learning (ML) that require scalable computing power. Entity operations for assets across the NERC CIP impact levels will be facing the growing demands for compute 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 are essential in 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[3]. As renewable installations grow, site classifications may change from low to medium impact levels, putting operators at risk of having to revert to on-premises resources to meet compliance language rather than benefitting from the cloud services available to lower impact sites.

The advent of Phasor Measurement Units (PMUs), and 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 expanded simulation capabilities and development environments that can help meet patching cycles and testing requirements for on-premises assets under the CIP requirements.

Cloud computing is a priority for the US government as underscored by the CloudSmart strategy to accelerate government agency adoption of cloud-based solutions. Cloud has proven its value in other critical industries such as financial services, defense, and healthcare, and is a fitting option for grid applications. Cloud services offer fault-tolerant system design capabilities in which operations and data

[2] https://www.eia.gov/todayinenergy/detail.php?id=51698#:~:text=EIA%20projects%20that%20renewable%20generation,of%20U.S.%20electricity%20by%202050&text=Note%3A%20Biofuels%20are%20both%20shown,in%20petroleum%20and%20other%20liquids.

[3] https://www.iea.org/reports/renewables-2022/executive-summary

Requested information
can be replicated and run in independent application stacks in geographically dispersed locations along with other benefits, including reliability, resilience, and security. NERC standards revisions to CIP-004 and CIP-011 allow for the use of cloud storage for BES Cyber System information (BCSI). Comparable consideration is due other systems under the other regulated definitions or functions.
Purpose or Goal (How does this proposed project provide the reliability-related benefit described above?):
The project purpose is to establish risk-based, outcome-driven requirements that place cloud services on par with other third-party resources already used for CIP-regulated systems including for BES operations and supporting cyber assets. This project will allow, but not require, use of cloud services for CIP-regulated systems including BES operations and supporting cyber assets. This SAR proposes to create a new standard(s) or revise existing CIP Standards to address the language that includes or implies specific physical hardware and is preventing adoption of cloud services for regulated systems. 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. The goals are to develop specific modifications to the CIP Standards, or create a new standard(s), to add clarity in allowing for the adoption and auditability of cloud services used for the BES. Creation of a new CIP Standard is strongly recommended. The goals also include addressing the role of third-party certifications as part of the auditability of the new or revised standards. These revisions will increase reliability and security to the Bulk Electric System (BES) by allowing the use of advanced technologies that support Entities in managing grid modernization and the changing grid landscape as well as making available to security teams all 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 to allow for adoption of cloud services for CIP-regulated systems. Creation of a new CIP standard is strongly recommended. • Require applicable entities that are procuring cloud services for CIP-regulated systems to develop and implement a plan to address the security objectives applicable to the use of cloud services for CIP-regulated systems including for BES operations and supporting cyber assets. • 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

Requested information
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). • Allow the use of third-party security certifications to support the auditability of the new or revised requirements. • Assess the applicability of the existing asset classifications (e.g., BES Cyber Assets (BCAs), BES Cyber Systems (BCS), and supporting cyber assets such as Electronic Access Control or Monitoring Systems (EACMS), Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs), and Transient Cyber Assets (TCAs)) to determine which definitions apply with the new or revised standard(s), if any; determine if they require revision and, if so, revise accordingly; and, to determine if new definitions are needed and draft accordingly. Consider whether the function of systems within the definition classifications plays a relevant role in the standard(s) applicability (i.e. control functions versus non-control functions). • 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[4] 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 following describes the proposed deliverables for this project: • New or revised standard(s) – the SDT will create risk-based and outcome-driven requirements within a new CIP standard(s) or in a revised CIP standard(s) to clarify the adoption of cloud services for CIP applicable systems and for regulated information[5]. It is strongly recommended that a new standard be created to allow entities to maintain their compliance programs for on-premises systems and assets under the existing CIP-002 thru CIP-014 suite of standards and to avoid conflicts that may occur in attempting to apply requirement language to physical and to cloud services. • The standard(s) will require applicable entities that are procuring cloud services for CIP-regulated systems to develop and implement a plan that addresses, at a minimum, the following specific objectives as they relate to cloud services for CIP applicable systems including for BES operations and supporting cyber assets: ○ Cloud service vendor risk management ○ Procurement controls The plan may apply different controls based on the criticality of different assets.

[4] 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.

[5] Use of cloud for BES Cyber System Information is already covered by CIP-004 and CIP-011. Inclusion of BCSI in this revision project is at the discretion of the drafting team.

Requested information

Requirements developed by the SDT will be aimed at the protection of aspects of the cloud service that are within the control of the responsible entities.

- Holistic or incremental - The SDT 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). The SDT will define a development plan for the project, giving particular consideration for EACMS defined systems as a top priority for revision because the existing CIP language prevents adoptions of security solutions with greater visibility, detection, correlation, analytics, and responsiveness available using cloud services.

- Auditability and use of third-party certifications – the SDT will set out requirement language to allow the use of independent third-party certifications/attestations to support auditability of the new or revised requirements and will incorporate language in the standard(s) as needed to clarify their use. Accepting independent third-party security assurance certifications/ attestations such as FedRAMP, SOC, ISO, or others is a valuable opportunity to set a high security standard for CSPs, recognize the rigor and cloud-security specific nature of such certifications, streamline the adoption and compliance demonstration process for regulated Entities, and support CIP auditor focus on assessing the power and utility operations and governance.

- Timing – the current CIP language applicable to assets that contain high and medium BES Cyber Systems includes or implies physical hardware that must reside within physical security perimeter (PSP), which is preventing adoption of cloud services that benefit security (i.e. security event monitoring solutions) and reliability (i.e. predictive maintenance solutions) today. The revised or new standard(s) is to be delivered in a timely manner and completed for submittal to FERC 12-18 months from the start of the SDT deliberations. As well, the implementation plan is to allow the possibility for early adoption ahead of any proposed enforceability date.

- Flexibility - The SDT may, as an alternative to a new or revised standard(s), propose equally efficient and effective means to meet the objectives. The drafting team may choose not to write standards and instead choose an alternate vehicle to allow for use of cloud services for CIP-regulated systems.

The following may serve as supporting documents for the SDT:

- SITES BES Operations in the Cloud whitepaper (pending publication)
- IEEE Practical Adoption of Cloud Computing in Power Systems- Drivers, Challenges, Guidance, and Real-world Use Cases

Requested information

• NERC in an informational filing to FERC in December 2021 identified the following areas of interest as potential educational topics about cloud environments, associated risks, and the risk mitigation measures when considering the new requirements:
  • Quality of Service and Resilience
  • Data Residency
  • Evaluation Criteria for Selection of Cloud Service Providers
  • Registered Entities Conducting Risk Assessments
  • Security Responsibilities
  • Compliance Oversight and Audit Processes

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 will incur costs related to compliance program revisions.
Please describe any unique characteristics of the BES facilities that may be impacted by this proposed standard development project (*e.g.*, Dispersed Generation Resources):
Submitter asserts there are no 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 most recent version of the NERC Functional Model for definitions):
Reliability Coordinator, Balancing Authority, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator
Do you know of any consensus building activities[6] 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. This project also has the potential to impact Project 2016-02, Project 2023-03, Project 2021-03. As well, additional SARs may be in development on related topics (e.g. Revisions to appropriate CIP Standards to include Multi-factor Cloud-based Authentication services.)
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.

[6] 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.

Requested information
No

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
e.g., NPCC	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

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