Comment Report

Project Name:	2023-09 Risk Management for Third-party Cloud Services | Standard Authorization Request
Comment Period Start Date:	5/10/2024
Comment Period End Date:	7/1/2024
Associated Ballots:	

There were 40 sets of responses, including comments from approximately 112 different people from approximately 85 companies representing 10 of the Industry Segments as shown in the table on the following pages.

Questions

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

2. Do you believe that other CIP standards will need to be modified for consistency to meet the goals laid out in the SAR? If so, please provide the standard recommendation and explanation.

3. Provide any additional comments for the drafting team to consider, if desired.

Organization Name	Name	Segment(s)	Region	Group Name	Group Member Name	Group Member Organization	Group Member Segment(s)	Group Member Region
MRO	Anna Martinson	1,2,3,4,5,6	MRO	MRO Group	Shonda McCain	Omaha Public Power District (OPPD)	1,3,5,6	MRO
					Michael Brytowski	Great River Energy	1,3,5,6	MRO
					Jamison Cawley	Nebraska Public Power District	1,3,5	MRO
					Jay Sethi	Manitoba Hydro (MH)	1,3,5,6	MRO
					Husam Al-Hadidi	Manitoba Hydro (System Preformance)	1,3,5,6	MRO
					Kimberly Bentley	Western Area Power Adminstration	1,6	MRO
					Jaimin Patal	Saskatchewan Power Coporation (SPC)	1	MRO
					George Brown	Pattern Operators LP	5	MRO
					Larry Heckert	Alliant Energy (ALTE)	4	MRO
					Terry Harbour	MidAmerican Energy Company (MEC)	1,3	MRO
					Dane Rogers	Oklahoma Gas and Electric (OG&E)	1,3,5,6	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Andrew Coffelt	Board of Public Utilities-Kansas (BPU)	1,3,5,6	MRO
					Peter Brown	Invenergy	5,6	MRO

					Angela Wheat	Southwestern Power Administration	1	MRO
					Bobbi Welch	Midcontinent ISO, Inc.	2	MRO
Eversource Energy	Joshua London	1,3		Eversource	Joshua London	Eversource Energy	1	NPCC
					Vicki O'Leary	Eversource Energy	3	NPCC
FirstEnergy - FirstEnergy Corporation	Mark Garza	1,4,5,6		FE Voter	Julie Severino	FirstEnergy - FirstEnergy Corporation	1	RF
					Aaron Ghodooshim	FirstEnergy - FirstEnergy Corporation	3	RF
					Robert Loy	FirstEnergy - FirstEnergy Solutions	5	RF
					Mark Garza	FirstEnergy-FirstEnergy	1,3,4,5,6	RF
					Stacey Sheehan	FirstEnergy - FirstEnergy Corporation	6	RF
California ISO	Monika Montez	2	WECC	ISO/RTO Council Standards Review Committee (SRC)	Monika Montez	CAISO	2	WECC
					Bobbi Welch	Midcontinent ISO, Inc.	2	RF
					Kathleen Goodman	ISO-NE	2	NPCC
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Helen Lainis	IESO	2	NPCC
					Charles Yeung	Southwest Power Pool, Inc. (RTO)	2	MRO
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
					Elizabeth Davis	PJM	2	SERC
Black Hills Corporation	Rachel Schuldt	1,3,5,6		Black Hills Corporation - All Segments	Micah Runner	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills	3	WECC

						Corporation		
					Rachel Schuldt	Black Hills Corporation	6	WECC
					Carly Miller	Black Hills Corporation	5	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
Northeast Power Coordinating Council	Ruida Shu	1,2,3,4,5,6,7,8,9,10	NPCC	NPCC RSC	Gerry Dunbar	Northeast Power Coordinating Council	10	NPCC
					Deidre Altobell	Con Edison	1	NPCC
					Michele Tondalo	United Illuminating Co.	1	NPCC
					Stephanie Ullah-Mazzuca	Orange and Rockland	1	NPCC
					Michael Ridolfino	Central Hudson Gas & Electric Corp.	1	NPCC
					Randy Buswell	Vermont Electric Power Company	1	NPCC
					James Grant	NYISO	2	NPCC
					Dermot Smyth	Con Ed - Consolidated Edison Co. of New York	1	NPCC
					David Burke	Orange and Rockland	3	NPCC
					Peter Yost	Con Ed - Consolidated Edison Co. of New York	3	NPCC
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					David Kwan	Ontario Power Generation	4	NPCC
					Silvia Mitchell	NextEra Energy -	1	NPCC

						Florida Power and Light Co.		
					Sean Cavote	PSEG	4	NPCC
					Jason Chandler	Con Edison	5	NPCC
					Tracy MacNicoll	Utility Services	5	NPCC
					Shivaz Chopra	New York Power Authority	6	NPCC
					Vijay Puran	New York State Department of Public Service	6	NPCC
					David Kiguel	Independent	7	NPCC
					Joel Charlebois	AESI	7	NPCC
					Joshua London	Eversource Energy	1	NPCC
					Emma Halilovic	Hydro One Networks, Inc.	1,2	NPCC
					Nicolas Turcotte	Hydro-Quebec (HQ)	1	NPCC
					Jeffrey Streifling	NB Power Corporation	1,4,10	NPCC
					Joel Charlebois	AESI	7	NPCC
					John Hastings	National Grid	1	NPCC
					Erin Wilson	NB Power	1	NPCC
					James Grant	NYISO	2	NPCC
					Michael Couchesne	ISO-NE	2	NPCC
					Kurtis Chong	IESO	2	NPCC
					Michele Pagano	Con Edison	4	NPCC
					Bendong Sun	Bruce Power	4	NPCC
					Carvers Powers	Utility Services	5	NPCC
					Wes Yeomans	NYSRC	7	NPCC
Western Electricity Coordinating Council	Steven Rueckert	10		WECC CIP	Steve Rueckert	WECC	10	WECC
					Morgan King	WECC	10	WECC
					Deb McEndaffer	WECC	10	WECC
					Tom Williams	WECC	10	WECC

1. Do you agree with the scope and objectives of this SAR? If not, please explain why you do not agree, and, if possible, provide specific language revisions that would make it acceptable to you.

Wendy Kalidass - U.S. Bureau of Reclamation - 1,5

Answer	No
Document Name	

Comment

Reclamation recognizes there are risks introduced with adopting cloud computing services for BES reliability operating services data storage and support services identified in the SAR. Cloud-based services could allow for new threats and vulnerabilities from nation state actors and entry-level hackers. If a cloud-based service operates critical High and Medium Impact BES services and does not properly vet its equipment supply chain, multiple registered entities could be threatened by a single zero-day vulnerability. Third party clouds often have administrative access for staff that an entity may not be able to account for or track.

If redundancies of physical hardware, long haul telecommunication pathways and supporting devices are in place, along with no mixed-trust environments, and vetted cloud services are used, the risk to the BES could be effectively mitigated. However, the risk drops significantly when cloud computing services are not used at all for Medium and/or High Impact BES Cyber Systems. Reclamation recommends cloud services be used for monitoring with a one-way data diodes or waterfalls in place and not for BES Cyber System management or control.

Likes 0	
Dislikes 0	

Response

Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC

Answer	No
Document Name	

Comment

Xcel Energy supports EEI comments.

Likes 0	
Dislikes 0	

Response

Roger Perkins - Southern Maryland Electric Cooperative - 1,3

Answer	No
Document Name	

Comment

SMECO agrees with comments provided by ACES:

There are not many Cloud Service Providers (CSP) capable and willing to meet the industry's the minimum security requirements for running a Bulk Electric System (BES) Cyber System (BCS) in the cloud; therefore, NERC/FERC/E-ISAC should manage the risk assessments associated with CSPs and provide a whitelist, a blacklist, and a process to get on/off the lists. ACES has a similar opinion regarding CIP-013 because it is pointless to have entities with significantly less information than E-ISAC, NERC, FERC, and other connected federal agencies with secret and top secret clearances complete risk assessments on CSPs.

There are no considerations in the SAR, the entity, entity's software vendor, or CSP to have resiliency across another CSP zone, region, etc. Further, there are a significant number of risks that have to be considered depending on how the entity's software vendor and/or entities choose to purchase/rent/leverage cloud services such as SaaS, PaaS, IaaS, and, depending on which model is used, how the vendor will work together is yet to be known. How a vendor will leverage CSP services will depend on what cybersecurity controls would be in control of the entity, software vendor, or CSP. Just the unknowns from the three cloud computing models makes it nearly impossible to construct requirements, as they all have different security requirements. SaaS presents the greatest risk to entities because the cyber security controls are completely unknown to the entity. SaaS has the largest return on investment (ROI), so vendors will likely choose that option. The other cloud service models will be just as expensive as on-premise solutions but will have more risk. While cloud computing has its advantages, the risks related to running the BES in the could greatly outweigh ANY potential financial or resiliency benefits. If electric utility software vendors no longer want to provide on-premise solutions or price them such that it forces entities to the cloud, another vendor will choose to provide the service for less, or another vendor will be created that will provide the service(s) at a reasonable cost.

If BCSs move to the cloud, the greatest risk to the BES will no longer be malicious actors, rather the greatest risk will be misconfiguration mistakes by entities that malicious actors abuse, not vulnerabilities. Gartner/the industry shows that more than 95% of cloud breaches are due to customer misconfiguration. This is primarily due to CSPs constantly introducing and modifying existing services with no control by the end user. On-premise solutions do not have these risks since entities have complete control of what changes in their environment.

The cost analysis portion of the SAR needs more information. The incremental costs of modifying a CIP program is minor compared to the costs to migrate BCS to the cloud and be able to meet the NERC CIP standards. The subject matter experts (SME) to support, operate, and secure cloud infrastructure are different. The tools used to manage, monitor, and secure cloud infrastructure are often different, requiring retooling, retraining, or hiring more SMEs, particularly if the entity has a hybrid on-premise/cloud infrastructure.

If using a CSP, the standards should require dedicated high speed multi-path communications to the CSP which is not discussed in the SAR and increases costs

Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Wesselkamper Amy
Dislikes 0	

Response

Alan Kloster - Evergy - 1,3,5,6 - MRO

Answer	No
Document Name	

Comment

Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) in response to question #1.

Likes 0	
Dislikes 0	

Response	
Dante Jackson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	

CEHE:

CenterPoint Energy Houston Electric, LLC (CEHE) does not agree with the scope and objectives of this SAR. The SAR does not identify the scope or specify which CIP standards or requirements prevent or must be modified to accommodate cloud services. This vague and undefined scope is unreasonable and may pose implementation challenges. Further, the suggestion of creating a new Standard along with the vague SAR scope will lead to unconstrained scope creep to the project, and inability to gain consensus among the industry. CEHE supports EEI's comments regarding question one.

Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	No
Document Name	
Comment	

EEI supports the effort to enable the use of cloud technology for additional NERC CIP use cases, however, we ask the drafting team to modify the SAR to include additional detail about the specific security risks associated with the use of cloud technology, and the aspects of the currently enforceable NERC CIP Standards that prevent its use. The additional detail will clearly define the scope of work associated with the SAR and support the drafting team in prioritizing revisions.

EEI proposes revising the Project Scope section of the SAR as follows:

- **Project Scope:** Suggest "The project scope is to **establish risk-based, outcome-driven requirements that will allow, but not require, use of cloud services for CIP-regulated systems including BES operations, associated cyber assets and BES Cyber System Information (BCSI) and addresses the following risks and considerations:**

o **Data Sovereignty: the country or locations where in-scope NERC CIP regulated systems, supporting cyber assets, and BCSI can be hosted, used, or stored by cloud service provider(s).**"

o **Supply Chain Risk Management: the requirements for assessing the security posture of third-party cloud services providers pre-procurement, post-procurement, and as needed throughout the business relationship. This may include but is not limited to:**

§ **Determining the role of independent third-party certifications and attestations (e.g. FedRAMP moderate or high, ISO 27001, SOC 1 and/or SOC 2) or equivalent where a third-party has not achieved a relevant third-party certification or attestation.**

§ **Consideration for determining the minimum contractual obligations between the CSP(s) and the entity to help support security and reliability.**

o **Shared Responsibility: the requirements for determining the role(s) of cloud service providers and entities for implementing and maintaining security controls when using cloud services for in-scope NERC CIP regulated systems, supporting cyber assets, and BCSI.**

§ **The drafting team should consider if or how these responsibilities change based on the cloud service model selected by the entity (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), or other models deemed relevant by the drafting team).**

o **Cloud services security requirements: requirements to address the security objectives (e.g. cloud security training, identity and access management, network security, system security management, physical security, incident response, resiliency, recovery, change management, vulnerability management, information protection, secure and resilient communications, supply chain risk management, internal network security monitoring, etc.) applicable to the use of cloud services for CIP-regulated systems including for BES operations, supporting cyber assets, and BCSI.**

o **Assessment of Applicability and compatibility with existing NERC CIP Standards:** Assess the applicability of the existing asset classifications **and NERC Glossary of Terms definitions** (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 **to address cloud services related concepts or risks** 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).

o **Resiliency: the requirements for cloud hosted systems or information to withstand or recover from disruptions. The drafting team could consider requirements related to the entity's architecture decisions (redundancy options such as deploying to multiple cloud data centers, the communications mechanisms selected (private network connection between the CSP and entity), and other factors to support reliability and business continuity.**

Additionally, new or revised NERC CIP Standards that enable the use of cloud and hybrid on-premises and cloud environments should continue to support the security of on-premises environments. The new or revised NERC CIP Standards must achieve security and reliability objectives at least equivalent to those applied for on-premises environments.

EEI proposes the following additional modifications to the SAR:

- Strike "strong recommendation" language for a standalone standard throughout the SAR. The DT has the responsibility to determine the approach to address the SAR.

- Strike references to "support the auditability" of the new or revised requirements throughout the SAR because the DT does not determine the audit approach.

- Strike recommendation to give particular consideration for EACMS because the assessment and prioritization of cloud solutions/risks to be addressed should be at the discretion of the drafting team.

- Strike target project timelines from the SAR and instead suggest that NERC and industry collaborate to determine the prioritization and associated target timelines because the timing for this project is driven by NERC's prioritization approach.

- Strike the "Flexibility" bullet in the Detailed Description section because the Standard Drafting Team's mechanism for addressing the scope of the SAR is through the development or revision of Standards.

EEI proposes revising the Supporting Documents section as follows:

- **Supporting documents:** EEI suggests adding the link to the SITES BES Operations in the Cloud whitepaper since it was approved and published after the SAR was submitted. We also ask the drafting team to consider adding relevant security guidelines and other relevant reference documents or

cloud specific resources such as: 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), and any others deemed relevant.

Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Wesselkamper Amy
Dislikes 0	

Response

Matt Carden - Southern Company - Southern Company Services, Inc. - 1

Answer	No
Document Name	

Comment

Southern appreciates and agrees that the CIP standards need to be modified to include the use of certain cloud services. However, we recommend the SAR be further refined with a clear and defined scope of work, prioritizing which of the many aspects of cloud computing it is authorizing the project team to accomplish. The SAR's current scope is a very broad "enable cloud services" and mentions numerous things from security tools to Control Center BCS. It states, "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." It is unclear, as a purpose statement, as to what "third-party resources" a drafting team is to get cloud services "on par" with. We assert the term "cloud" is an extremely large range of technologies, capabilities, service offerings, and issues and thus revisions of this magnitude should first have a prioritized plan that is then outlined as a scope of work within this or subsequent SARs. For example, "enable cloud services" could include all the following and more:

· Electronic access monitoring – Potentially a splitting of access monitoring from access control, along with a separation of the use of a service from including the servers, thus allowing the use of cloud-based SIEM-type services, including a review of any BCSI implications and the current use of EACMS throughout the standards.

· Electronic access control – viewing access control as a function, not a type of Cyber Asset, and allowing for the use of cloud-based services for functions such as multi-factor authentication (Duo, etc.) for access to ESP's and BCS, including a review of BCSI implications and the use of EACMS throughout the standards.

· Medium/high impact BCS in the cloud – a review of CIP definitions from the Cyber Asset definition on up would be needed as well as potentially fundamental shifts in many requirements.

· Various cloud service models – Modifying/creating requirements that can cover the widely varying topics and issues that arise from the range of cloud service models from IaaS to SaaS and mixtures of such models.

· Cloud technology can present issues whether hosted on or off premise. Does the SAR envision a review of CIP from the definitions up to account for BCS/EACMS/PACS, etc. functionality that are implemented as dynamic services rather than static servers (physical or virtual)? After which, the issues of off-premise implementation of such cloud services come in with all the CIP-004, CIP-006, and CIP-011 issues among others if implemented off-premise.

Additionally, the Auditability section of the Description says the DT will set out requirement language to allow the use of independent third-party certifications/attestations to support auditability. We understand that DTs write requirements for registered entities only, not Cloud Service Providers and what certifications they should present and cannot state in a standard what the ERO must accept in the CMEP for the CSP's part of the overall cyber security risk. The question of acceptability of 3rd party certifications or attestations and the concept of "shared responsibility models" are issues that need to be settled outside the standards drafting process which can then inform a drafting team as it drafts specific requirements.

The Timing section of the Description calls for filing with FERC within 12 to 18 months after the start of the DT work. That would only allow for possibly one or two drafts for revisions of a large magnitude. Either a far more concise scope of work should be created that could be accomplished in that

timeframe while allowing for adequate stakeholder feedback or such statements removed so there is no artificial deadline imposed on changes of this magnitude. We assert the complexity of this SAR's topic is much greater than writing a new standard that requires certain agreed upon terms with cloud service providers.

Likes 1	PNM Resources - Public Service Company of New Mexico, 3, Wesselkamper Amy
Dislikes 0	

Response

Kinte Whitehead - Exelon - 1,3

Answer	No
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	No
Document Name	

Comment

AEPC signed on to ACES comments below:

There are not many Cloud Service Providers (CSP) capable and willing to meet the industry's the minimum security requirements for running a Bulk Electric System (BES) Cyber System (BCS) in the cloud; therefore, NERC/FERC/E-ISAC should manage the risk assessments associated with CSPs and provide a whitelist, a blacklist, and a process to get on/off the lists. ACES has a similar opinion regarding CIP-013 because it is pointless to have entities with significantly less information than E-ISAC, NERC, FERC, and other connected federal agencies with secret and top secret clearances complete risk assessments on CSPs.

There are no considerations in the SAR, the entity, entity's software vendor, or CSP to have resiliency across another CSP zone, region, etc. Further, there are a significant number of risks that have to be considered depending on how the entity's software vendor and/or entities choose to purchase/rent/leverage cloud services such as SaaS, PaaS, IaaS, and, depending on which model is used, how the vendor will work together is yet to be known. How a vendor will leverage CSP services will depend on what cybersecurity controls would be in control of the entity, software vendor, or CSP. Just the unknowns from the three cloud computing models makes it nearly impossible to construct requirements, as they all have different security requirements. SaaS presents the greatest risk to entities because the cyber security controls are completely unknown to the entity. SaaS has the largest return on investment (ROI), so vendors will likely choose that option. The other cloud service models will be just as expensive as on-premise solutions but will have more risk. While cloud computing has its advantages, the risks related to running the BES in the could greatly outweigh ANY potential financial or resiliency benefits. If electric utility software vendors no longer want to provide on-premise solutions or price them such that it forces entities to the cloud, another vendor will choose to provide the service for less, or another vendor will be created that will provide the service(s) at a reasonable

cost.

If BCSs move to the cloud, the greatest risk to the BES will no longer be malicious actors, rather the greatest risk will be misconfiguration mistakes by entities that malicious actors abuse, not vulnerabilities. Gartner/the industry shows that more than 95% of cloud breaches are due to customer misconfiguration. This is primarily due to CSPs constantly introducing and modifying existing services with no control by the end user. On-premise solutions do not have these risks since entities have complete control of what changes in their environment.

The cost analysis portion of the SAR needs more information. The incremental costs of modifying a CIP program is minor compared to the costs to migrate BCS to the cloud and be able to meet the NERC CIP standards. The subject matter experts (SME) to support, operate, and secure cloud infrastructure are different. The tools used to manage, monitor, and secure cloud infrastructure are often different, requiring retooling, retraining, or hiring more SMEs, particularly if the entity has a hybrid on-premise/cloud infrastructure.

If using a CSP, the standards should require dedicated high speed multi-path communications to the CSP which is not discussed in the SAR and increases costs.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)

Answer	No
Document Name	

Comment

Purpose or Goal *(page 3, 3rd paragraph) – The ISO/RTO Council Standards Review Committee (SRC) agrees with what's stated and recommends adding a reference to the Department of Defense's* DOD Cybersecurity Reciprocity Playbook *(https://dodcio.defense.gov/Portals/0/Documents/Library/(U)2024-01-02DoDCybersecurityReciprocityPlaybook.pdf) in support of third-party certifications as detailed below.*

- *The goals also include addressing the role of third-party certifications as part of the auditability of the new or revised standards. Executed appropriately, reciprocity**[1]** reduces redundant testing, assessment and documentation, and the associated costs in time and resources.**[2]***

The benefits of reciprocity should also be cited under ***Cost Impact Assessment*** *(page 6).*

Finally, the SRC is concerned that the scope of the SAR is insufficiently clear, and as further detailed in its response to question 2, the SRC recommends that the SAR be revised to direct the drafting team to focus on creating a new CIP standard that addresses cloud services rather than attempting to modify the existing suite of CIP standards (with its focus on on-premises equipment) to also address cloud services. However, the SRC recognizes that even under this approach, some modifications to existing CIP standards may be necessary, and does not believe that the SAR should preclude the drafting team from making any such modifications as may be needed.

[1]*"Reciprocity" is the "agreement among participating organizations to accept each other's security assessments, to reuse system resources, and/or to accept each other's assessed security posture to share information."*

[2] *DOD Cybersecurity Reciprocity Playbook (https://dodcio.defense.gov/Portals/0/Documents/Library/(U)2024-01-*

02DoDCybersecurityReciprocity%20Playbook.pdf) page 4, section 3.1.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - RF	
Answer	No
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	No
Document Name	
Comment	
ERCOT joins the comments submitted by the ISO/RTO Council (IRC) Standards Review Committee (SRC) and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	No
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	

Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	No
Document Name	
Comment	

NEE support EEI's comment: "

EEI supports the effort to enable the use of cloud technology for additional NERC CIP use cases, however, we ask the drafting team to modify the SAR to include additional detail about the specific security risks associated with the use of cloud technology, and the aspects of the currently enforceable NERC CIP Standards that prevent its use. The additional detail will clearly define the scope of work associated with the SAR and support the drafting team in prioritizing revisions.

EEI proposes revising the Project Scope section of the SAR as follows:

{C}- **Project Scope:** Suggest "The project scope is to **establish risk-based, outcome-driven requirements that will allow, but not require, use of cloud services for CIP-regulated systems including BES operations, associated cyber assets and BES Cyber System Information (BCSI) and addresses the following risks and considerations:**

{C}o **Data Sovereignty: the country or locations where in-scope NERC CIP regulated systems, supporting cyber assets, and BCSI can be hosted, used, or stored by cloud service provider(s).**"

{C}o **Supply Chain Risk Management: the requirements for assessing the security posture of third-party cloud services providers pre-procurement, post-procurement, and as needed throughout the business relationship. This may include but is not limited to:**

{C}§ **Determining the role of independent third-party certifications and attestations (e.g. FedRAMP moderate or high, ISO 27001, SOC 1 and/or SOC 2) or equivalent where a third-party has not achieved a relevant third-party certification or attestation.**

{C}§ **Consideration for determining the minimum contractual obligations between the CSP(s) and the entity to help support security and reliability.**

{C}o **Shared Responsibility: the requirements for determining the role(s) of cloud service providers and entities for implementing and maintaining security controls when using cloud services for in-scope NERC CIP regulated systems, supporting cyber assets, and BCSI.**

{C}§ **The drafting team should consider if or how these responsibilities change based on the cloud service model selected by the entity (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), or other models deemed relevant by the drafting team).**

{C}o **Cloud services security requirements: requirements to address the security objectives (e.g. cloud security training, identity and access management, network security, system security management, physical security, incident response, resiliency, recovery, change management, vulnerability management, information protection, secure and resilient communications, supply chain risk management, internal network security monitoring, etc.) applicable to the use of cloud services for CIP-regulated systems including for BES operations, supporting cyber assets, and BCSI.**

{C}o **Assessment of Applicability and compatibility with existing NERC CIP Standards:** Assess the applicability of the existing asset classifications **and NERC Glossary of Terms definitions** (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 **to address cloud services related concepts or risks** 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).

{C}o **Resiliency: the requirements for cloud hosted systems or information to withstand or recover from disruptions. The drafting team could consider requirements related to the entity's architecture decisions (redundancy options such as deploying to multiple cloud data centers, the communications mechanisms selected (private network connection between the CSP and entity), and other factors to support reliability and business continuity.**

Additionally, new or revised NERC CIP Standards that enable the use of cloud and hybrid on-premises and cloud environments should continue to support the security of on-premises environments. The new or revised NERC CIP Standards must achieve security and reliability objectives at least equivalent to those applied for on-premises environments.

EEI proposes the following additional modifications to the SAR:

{C}- Strike "strong recommendation" language for a standalone standard throughout the SAR. The DT has the responsibility to determine the approach to address the SAR.

{C}- Strike references to "support the auditability" of the new or revised requirements throughout the SAR because the DT does not determine the audit approach.

{C}- Strike recommendation to give particular consideration for EACMS because the assessment and prioritization of cloud solutions/risks to be addressed should be at the discretion of the drafting team.

{C}- Strike target project timelines from the SAR and instead suggest that NERC and industry collaborate to determine the prioritization and associated target timelines because the timing for this project is driven by NERC's prioritization approach.

{C}- Strike the "Flexibility" bullet in the Detailed Description section because the Standard Drafting Team's mechanism for addressing the scope of the SAR is through the development or revision of Standards.

EEI proposes revising the Supporting Documents section as follows:

{C}- **Supporting documents:** EEI suggests adding the link to the SITES BES Operations in the Cloud whitepaper since it was approved and published after the SAR was submitted. We also ask the drafting team to consider adding relevant security guidelines and other relevant reference documents or cloud specific resources such as: 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), and any others deemed relevant."

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,4,5,6, Group Name FE Voter

Answer	No
Document Name	

Comment

FirstEnergy supports EEI's comments which state:

EEI supports the effort to enable the use of cloud technology for additional NERC CIP use cases, however, we ask the drafting team to modify the SAR to include additional detail about the specific security risks associated with the use of cloud technology, and the aspects of the currently enforceable NERC CIP Standards that prevent its use. The additional detail will clearly define the scope of work associated with the SAR and support the drafting team in prioritizing revisions.

EEI proposes revising the Project Scope section of the SAR as follows:

- Project Scope: Suggest "The project scope is to establish risk-based, outcome-driven requirements that will allow, but not require, use of cloud services for CIP-regulated systems including BES operations, associated cyber assets and BES Cyber System Information (BCSI) and addresses the following risks and considerations:

o Data Sovereignty: the country or locations where in-scope NERC CIP regulated systems, supporting cyber assets, and BCSI can be hosted, used, or stored by cloud service provider(s)."

o Supply Chain Risk Management: the requirements for assessing the security posture of third-party cloud services providers pre-procurement, post-procurement, and as needed throughout the business relationship. This may include but is not limited to:

 Determining the role of independent third-party certifications and attestations (e.g. FedRAMP moderate or high, ISO 27001, SOC 1 and/or SOC 2) or equivalent where a third-party has not achieved a relevant third-party certification or attestation.

 Consideration for determining the minimum contractual obligations between the CSP(s) and the entity to help support security and reliability.

o Shared Responsibility: the requirements for determining the role(s) of cloud service providers and entities for implementing and maintaining security controls when using cloud services for in-scope NERC CIP regulated systems, supporting cyber assets, and BCSI.

 The drafting team should consider if or how these responsibilities change based on the cloud service model selected by the entity (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), or other models deemed relevant by the drafting team).

o Cloud services security requirements: requirements to address the security objectives (e.g. cloud security training, identity and access management, network security, system security management, physical security, incident response, resiliency, recovery, change management, vulnerability management, information protection, secure and resilient communications, supply chain risk management, internal network security monitoring, etc.) applicable to the use of cloud services for CIP-regulated systems including for BES operations, supporting cyber assets, and BCSI.

o Assessment of Applicability and compatibility with existing NERC CIP Standards: Assess the applicability of the existing asset classifications and NERC Glossary of Terms definitions (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 to address cloud services related concepts or risks 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).

o Resiliency: the requirements for cloud hosted systems or information to withstand or recover from disruptions. The drafting team could consider requirements related to the entity's architecture decisions (redundancy options such as deploying to multiple cloud data centers, the communications mechanisms selected (private network connection between the CSP and entity), and other factors to support reliability and business continuity.

Additionally, new or revised NERC CIP Standards that enable the use of cloud and hybrid on-premises and cloud environments should continue to support the security of on-premises environments. The new or revised NERC CIP Standards must achieve security and reliability objectives at least equivalent to those applied for on-premises environments.

EEI proposes the following additional modifications to the SAR:

- Strike “strong recommendation” language for a standalone standard throughout the SAR. The DT has the responsibility to determine the approach to address the SAR.

- Strike references to “support the auditability” of the new or revised requirements throughout the SAR because the DT does not determine the audit approach.

- Strike recommendation to give particular consideration for EACMS because the assessment and prioritization of cloud solutions/risks to be addressed should be at the discretion of the drafting team.

- Strike target project timelines from the SAR and instead suggest that NERC and industry collaborate to determine the prioritization and associated target timelines because the timing for this project is driven by NERC’s prioritization approach.

- Strike the “Flexibility” bullet in the Detailed Description section because the Standard Drafting Team’s mechanism for addressing the scope of the SAR is through the development or revision of Standards.

EEI proposes revising the Supporting Documents section as follows:

Supporting documents: EEI suggests adding the link to the SITES BES Operations in the Cloud whitepaper since it was approved and published after the SAR was submitted. We also ask the drafting team to consider adding relevant security guidelines and other relevant reference documents or cloud specific resources such as: 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), and any others deemed relevant.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 1,3,5,6, Group Name Black Hills Corporation - All Segments

Answer	No
Document Name	

Comment

Black Hills Corporation agrees with EEI’s comments which support the effort to enable the use of cloud technology for additional NERC CIP use cases, however, we ask the drafting team to modify the SAR to include additional detail about the specific security risks associated with the use of cloud technology, and the aspects of the currently enforceable NERC CIP Standards that prevent its use. The additional detail will clearly define the scope of work associated with the SAR and support the drafting team in prioritizing revisions.

Black Hills Corporation agrees with EEI’s proposal for revising the Project Scope section of the SAR as follows, with additions:

- **Project Scope:** Suggest “The project scope is to **establish risk-based, outcome-driven requirements that will allow, but not require, use of cloud services for CIP-regulated systems including BES operations, associated cyber assets and BES Cyber System Information (BCSI) and addresses the following risks and considerations:**

o **Data Sovereignty: the country or locations where in-scope NERC CIP regulated systems, supporting cyber assets, and BCSI can be hosted, used, or stored by cloud service provider(s).**”

o **Supply Chain Risk Management: the requirements for assessing the security posture of third-party cloud services providers pre-procurement, post-procurement, and as needed throughout the business relationship. This may include but is not limited to:**

- **Determining the role of independent third-party certifications and attestations (e.g. FedRAMP moderate or high, ISO 27001, SOC 1 and/or SOC 2) or equivalent where a third-party has not achieved a relevant third-party certification or attestation.**

- **Consideration for determining the minimum contractual obligations between the CSP(s) and the entity to help support security and reliability.**

o **Shared Responsibility: the requirements for determining the role(s) of cloud service providers and entities for implementing and maintaining security controls when using cloud services for in-scope NERC CIP regulated systems, supporting cyber assets, and BCSI.**

- Black Hills Corporation agrees with EEI's proposal for the following considerations in addition to other concerns noted below:

- The drafting team should consider if or how these responsibilities change based on the cloud service model selected by the entity (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), or other models deemed relevant by the drafting team).

- Black Hills Corporation is especially concerned about the Cloud concentration risk; with multiple entities utilizing a particular Cloud provider, tools would not be available to a significant portion of utilities in the event of potential failure in internet connection or vendor operations which poses a massive risk to the reliability of the grid. We strongly encourage the drafting team to address the Cloud concentration risk at a higher level (possibly NERC level) than the individual utility. Vendors need to be accountable for continuity of business operations.

o **Cloud services security requirements: requirements to address the security objectives (e.g. cloud security training, identity and access management, network security, system security management, physical security, incident response, resiliency, recovery, change management, vulnerability management, information protection, secure and resilient communications, supply chain risk management, internal network security monitoring, etc.) applicable to the use of cloud services for CIP-regulated systems including for BES operations, supporting cyber assets, and BCSI.**

o **Assessment of Applicability and compatibility with existing NERC CIP Standards:** Assess the applicability of the existing asset classifications **and NERC Glossary of Terms definitions** (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 **to address cloud services related concepts or risks** 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).

o **Resiliency: the requirements for cloud hosted systems or information to withstand or recover from disruptions. The drafting team could consider requirements related to the entity's architecture decisions (redundancy options such as deploying to multiple cloud data centers, the communications mechanisms selected (private network connection between the CSP and entity), and other factors to support reliability and business continuity.**

o Black Hills Corporation suggests adding a requirement regarding Resiliency in operations independent of Cloud connection to address potential failure in internet connection or vendor operations. Vendors must provide capability for an on-premise component of Cloud solutions. Registered entities shall have to institute operational planning continuity plans focused on absence of connection to Cloud systems.

Additionally, new or revised NERC CIP Standards that enable the use of cloud and hybrid on-premises and cloud environments should continue to support the security of on-premises environments. The new or revised NERC CIP Standards must achieve security and reliability objectives at least equivalent to those applied for on-premises environments.

Black Hills Corporation agrees with EEI's proposal for the following additional modifications to the SAR:

- Strike "strong recommendation" language for a standalone standard throughout the SAR. The DT has the responsibility to determine the approach to address the SAR.

- Strike references to “support the auditability” of the new or revised requirements throughout the SAR because the DT does not determine the audit approach.

- Strike recommendation to give particular consideration for EACMS because the assessment and prioritization of cloud solutions/risks to be addressed should be at the discretion of the drafting team.

- Strike target project timelines from the SAR and instead suggest that NERC and industry collaborate to determine the prioritization and associated target timelines because the timing for this project is driven by NERC’s prioritization approach.

- Strike the “Flexibility” bullet in the Detailed Description section because the Standard Drafting Team’s mechanism for addressing the scope of the SAR is through the development or revision of Standards.

Black Hills Corporation agrees with EEI’s proposal for revising the Supporting Documents section as follows:

- **Supporting documents:** suggests adding the link to the SITES BES Operations in the Cloud whitepaper since it was approved and published after the SAR was submitted. We also ask the drafting team to consider adding relevant security guidelines and other relevant reference documents or cloud specific resources such as: 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), and any others deemed relevant.

Likes 0	
Dislikes 0	

Response

Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3

Answer	No
Document Name	

Comment

PNM and TNMP support the comments made by EEI and SMECO

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	Yes
Document Name	

Comment

BPA agrees with the objectives, but has concern about how the broad scope could affect all other CIP standards, including standards awaiting FERC approval, standards under development, and other SARs. Bonneville Power Administration suggests at a minimum waiting until the virtualization suite

of standards is approved by FERC before considering redlines to specific CIP standards.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports the scope of the SAR and the objectives. We encourage the Drafting Team to avoid incremental revisions in creating their development plan, and to aim for holistic revisions that accommodate the use of cloud for all CIP defined systems. In planning their revisions, the drafting team should consider if continued revisions to CIP-004 and CIP-011 might be needed to improve clarity on handling BCSI and whether the current scope would allow for that.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	Yes
Document Name	
Comment	
Constellation agrees with NAGF comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 5,6	
Answer	Yes
Document Name	
Comment	

Constellation agrees with NAGF comments.

Kimberly Turco on behalf of Constellation Segments 5 and 6.

Likes 0	
Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 1,3,6

Answer	Yes
Document Name	

Comment

Ameren supports the flexibility of having the option to use cloud services.

Likes 0	
Dislikes 0	

Response

David Buchold - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	Yes
Document Name	

Comment

No Comment

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	Yes
Document Name	

Comment

SPP is in support of the scope and objectives of this SAR. SPP strongly recommends the creation of a new CIP Standard.

SPP also supports the SRC's comment that recommends adding a reference to the Department of Defense's DOD Cybersecurity Reciprocity Playbook (https://dodcio.defense.gov/Portals/0/Documents/Library/(U)%202024-01-02%20DoD%20Cybersecurity%20Reciprocity%20Playbook.pdf) **in support of third-party certifications as detailed below.**

- **The goals also include addressing the role of third-party certifications as part of the auditability of the new or revised standards. Executed appropriately, reciprocity[1] reduces redundant testing, assessment and documentation, and the associated costs in time and resources.[2]**

[1] "Reciprocity" is the "agreement among participating organizations to accept each other's security assessments, to reuse system resources, and/or to accept each other's assessed security posture to share information."

[2] DOD Cybersecurity Reciprocity Playbook, (https://dodcio.defense.gov/Portals/0/Documents/Library/(U)%202024-01-02%20DoD%20Cybersecurity%20Reciprocity%20Playbook.pdf) page 4, section 3.1.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 1,3,5,6

Answer	Yes
Document Name	

Comment

AZPS supports the effort to allow for expanded use cases of cloud technology.

Likes 0	
Dislikes 0	

Response

Maggy Powell - Amazon Web Services - 7

Answer	Yes
Document Name	

Comment

AWS agrees with the scope and objectives in the SAR. The scope and description outline elements of the project and provides the SDT with the flexibility to determine the best approach to meet the objectives. Under the SAR, these new requirements will put cloud services, which Responsible Entities already use in many high security, non-CIP areas of their business, on par with other third-party resources already used for CIP-regulated systems. A risk-based, outcome-driven approach is important to achieve the security objectives of the SAR and allow Responsible Entities to adopt cloud services as they see best for their specific facts & circumstances in a manner that protects the reliability of the bulk-power system.

One unique benefit of this project is that it will develop requirements for the CIP use of new technology that, while widely used across critical infrastructure sectors, has not been used in the CIP environment due to the restrictions of the existing CIP Reliability Standards. The resulting requirements will allow, but not require, use of cloud services for CIP-regulated systems including BES operations and supporting cyber assets. When approved, the requirements will apply when a cloud deployment for regulated systems is put into production Therefore, the requirements can be effective upon approval.

One aspect of the SAR the drafting team will need to address is the method for accepting third-party certifications to ensure the presence and implementation of the necessary CIP-level security controls. Relying on third-party certifications to an appropriate degree presents an opportunity to drive security and simplify compliance by leveraging rigorous, cloud security focused certifications in a one-to-many arrangement so that Responsible Entities can know whether their cloud service vendors will be able to meet the required level of security controls before procuring and implementing those cloud services. Appropriate certifications can provide security assurance for cloud services and allow NERC compliance monitoring processes to focus on the Responsible Entity's operational systems and their security controls implementation.

Likes 0	
Dislikes 0	

Response

Martin Sidor - NRG - NRG Energy, Inc. - 5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	
Response	
Kevin Conway - Western Power Pool - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	

Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1,3, Group Name Eversource	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Leshel Hutchings - AEP - 3,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	

Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	

Texas RE appreciates the care in developing a SAR to address the increasing prevalence of cloud-based solutions for operating, controlling, and monitoring BES assets. Texas RE notes that the current opportunity for registered entities when implementing CIP applicable systems utilizing cloud services is:

1. Implementation of cloud services in a secure manner;

2. Ensuring and confirming Cloud Service Providers are adhering to the CIP Standard requirements; and

3. Demonstrating through evidence that Registered Entities are compliant with all applicable CIP Standard requirements through their cloud-service solutions in the same manner as on-premises solutions.

Texas RE believes that these objectives can be realized largely on the existing CIP Standard Requirements. As such, a measured approach to new, cloud-based standards is likely appropriate, particularly if it seeks to deviate from the core CIP requirements in a material way. Moreover, it may be appropriate to explore the use of cloud services for PACS and/or EACMS before addressing full BCS operations in the cloud because of the 15-minute impact a BCS can have on the BPS.

Likes 0	
Dislikes 0	
Response	

2. Do you believe that other CIP standards will need to be modified for consistency to meet the goals laid out in the SAR? If so, please provide the standard recommendation and explanation.

Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	No
Document Name	
Comment	
SRP is aware that possibly multiple standards may need modification to align with cloud usage as identified in the SAR. However, we strongly feel that rather to attempt in revising all standards to incorporate cloud security, it would be best to draft a whole new standard to minimize impact and make things less complicated.	
Likes 0	
Dislikes 0	
Response	

Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Martin Sidor - NRG - NRG Energy, Inc. - 5,6	
Answer	No
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

Maggy Powell - Amazon Web Services - 7	
Answer	Yes
Document Name	

Comment

AWS strongly recommends and supports creation of a separate stand-alone standard to address requirements for use of cloud services. Developing a new NERC CIP standard specifically for the use of cloud computing provides several key benefits compared to revising existing standards to allow for cloud usage.

- Responsible Entities adopting cloud for regulated systems will also continue to have on-premises systems subject to the existing standards. A separate standard allows Responsible Entities to incorporate cloud environments into their compliance programs without changing their on-prem compliance program. Similarly, no compliance program changes will be needed until cloud is adopted. Adopting cloud is an option not a requirement.

- A standalone cloud standard allows for security considerations and requirements tailored to cloud environments including recognition of aspects such as shared responsibility.

- The risk-based approach of the CIP-013 model is an agile approach and enables the Responsible Entity to evolve their security program based on their risk assessment cycle and update mitigations in response to a changing risk landscape. Cloud technologies and best practices continue to evolve. Prioritizing security capabilities requires flexibility.

- Overall, a dedicated cloud standard could result in stronger, more cloud-native security practices across the utility sector, supporting greater adoption of cloud computing's benefits.

- It avoids adding greater complexity to the existing standards and the challenge of posting many standards at once for ballot.

- It avoids the risk of introducing unnecessary knock-on effects with the existing standards, many of which have long-standing history and have significant standardization across the industry.

- It avoids requiring wholesale changes to Responsible Entity CIP compliance program documentation using the existing standard language, particularly for Responsible Entities that will not be using cloud-based services in their CIP environment.

- A standalone standard also supports potential simplification of applicable definitions.

While a standalone standard can fulfill the objectives, the SDT may determine that other existing standards be adapted for greater clarify and efficiency, such as, the SDT may decide to incorporate BCSI use of cloud into the new standalone standard to allow one standard to apply to cloud services. In that case, CIP-004 and CIP-011 may need revision.

In addition, the applicability sections of the existing CIP standards may need to be revised to make clear that assets covered by the new cloud services standard are exempt from one or more existing CIP standards to avoid confusion as to which standards apply to which assets.

Likes 0	
Dislikes 0	

Response

Marcus Bortman - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	Yes
Document Name	
Comment	
CIP-015 should be included based on the recent NERC Board Adoption.	
Likes 0	
Dislikes 0	
Response	
Amy Wesselkamper - PNM Resources - Public Service Company of New Mexico - 1,3	
Answer	Yes
Document Name	
Comment	
PNM and TNMP support EEI comments. CIP-015 should be included in potential impact	
Likes 0	
Dislikes 0	
Response	
Rachel Schuldt - Black Hills Corporation - 1,3,5,6, Group Name Black Hills Corporation - All Segments	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation agrees with EEI's suggestion of adding CIP-015 to the list of CIP standards that will need to be modified due to its recent NERC Board Adoption. Note that any changes to CIP-002 and the Control Center definition as a result of this work may have broader impacts within the overall NERC Reliability Standards in addition to the CIP Standards that should be considered. In addition to the CIP Standards, there may also be Operations and Planning Standards that could be impacted by use of cloud technology such as, TOP-001-4 R20, R21, R23, and R24 related to Control Center data exchange redundancy and testing, TOP-010 (i) R4 related to monitoring of EMS alarm processes, and BAL-005-1 R1 which requires RTU scan rates of 6 seconds or less for calculating ACE. The SDT should consider impacts to the O&P Standards as revisions/new Standards are drafted.	
Likes 0	
Dislikes 0	

Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,4,5,6, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy supports EEI's comments which state: EEI suggests adding CIP-015 to the list of CIP standards that will need to be modified due to its recent NERC Board Adoption. Note that any changes to CIP-002 and the Control Center definition as a result of this work may have broader impacts within the overall NERC Reliability Standards in addition to the CIP Standards that should be considered. In addition to the CIP Standards, there may also be Operations and Planning Standards that could be impacted by use of cloud technology such as, TOP-001-4 R20, R21, R23, and R24 related to Control Center data exchange redundancy and testing, TOP-010 (i) R4 related to monitoring of EMS alarm processes, and BAL-005-1 R1 which requires RTU scan rates of 6 seconds or less for calculating ACE. The SDT should consider impacts to the O&P Standards as revisions/new Standards are drafted.	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	Yes
Document Name	
Comment	
Physical security control objectives that would take an entity into a Cloud Service Providers 'underlay' environment should be considered for modification. CIP-002: R1.3 'Identify each asset that contains a low impact BES Cyber System' CIP-003: Attachment 1 Section 2 physical controls for low impact BCS and devices affording electronic access control. CIP-004: All requirements CIP-006: All requirements CIP-007: R1.2 CIP-008: The Standards use of the NERC defined term Cyber Security Incident includes physical security compromise. CIP-012: The technical rational states devices used to encrypt communication should be physically secured.	
Likes 0	

Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	Yes
Document Name	
Comment	
Minnesota Power supports EEI's comments.	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	Yes
Document Name	
Comment	
The SRC notes that other CIP standards tend to be scoped in terms of Applicable Systems, while cloud services, by their dynamic and virtual nature, are probably not going to support such a characterization. Consequently, the SRC recommends an approach of developing a single CIP standard focused on risk management and responsible security planning with respect to integration of cloud services as a part of critical infrastructure. This could include a risk-scaled approach that weighs the benefits and the risks that cloud services create when used to support various functions related to critical infrastructure (e.g., cloud services used for generation dispatch and other reliability operating services may require greater risk mitigation measures than cloud services used for electronic access control and monitoring functions). *To the extent that overlap in compliance and/or security concerns exists among present CIP standards, proposed new or revised CIP standards, and*	

NERC Glossary entries, any changes should be coordinated to support potential future uses of cloud services while preserving the value of existing security measures and compliance programs. For example, the SRC anticipates the following CIP standards (among others) may need to be revisited to address the identified areas and ensure consistency across all CIP standards.

- *Physical Security Perimeter (PSP) – CIP-006*
- *To address language that includes or implies specific physical hardware.*
- *Vendor connectivity – CIP-007 and CIP-013*
- *To address potential concerns with ensuring cloud services, and connections to cloud services, are reliable and secure.*
- *To ensure cloud services supply chain security risks are addressed.*
- *Configuration monitoring – CIP-010*
- *BCSI storage – CIP-004 and CIP-011*

To ensure that cloud storage of BCSI is handled consistently with the approach to cloud services taken in any new or revised standards developed as a result of this SAR.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	Yes
Document Name	

Comment

AEPC signed on to ACES comments below:

Yes, because of the complexity of CSP, type of cloud deployment by the entity, and/or software vendor, cloud implementation and cybersecurity tools, etc., it is not possible to determine which will need to be modified until the DT is closer to a final draft. Trying to determine and make changes in parallel with this project will be confusing and result in more work.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC

Answer	Yes
Document Name	

Comment

SPP recommends the creation of a new CIP standard focused on risk management and responsible security planning with respect to integration of cloud services as a part of critical infrastructure. From an efficiency standpoint, a stand-alone standard would be the best

approach and encourage backwards compatibility.	
Likes 0	
Dislikes 0	
Response	
David Buchold - Southern Indiana Gas and Electric Co. - 3,5,6 - RF	
Answer	Yes
Document Name	
Comment	
Yes, Southern Indiana Gas & Electric Co. d/b/a CenterPoint Energy Indiana South (SIGE) presumes that other CIP standards will need to be modified; however, specific NERC CIP standard recommendations and explanations cannot be determined at this time.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
EEI suggests adding CIP-015 to the list of CIP standards that will need to be modified due to its recent NERC Board Adoption. Note that any changes to CIP-002 and the Control Center definition as a result of this work may have broader impacts within the overall NERC Reliability Standards in addition to the CIP Standards that should be considered. In addition to the CIP Standards, there may also be Operations and Planning Standards that could be impacted by use of cloud technology such as, TOP-001-4 R20, R21, R23, and R24 related to Control Center data exchange redundancy and testing, TOP-010 (i) R4 related to monitoring of EMS alarm processes, and BAL-005-1 R1 which requires RTU scan rates of 6 seconds or less for calculating ACE. The SDT should consider impacts to the O&P Standards as revisions/new Standards are drafted.	
Likes 0	
Dislikes 0	
Response	
David Jendras Sr - Ameren - Ameren Services - 1,3,6	
Answer	Yes

Document Name	
Comment	
If BES assets are included in scope, many CIP standards will need to change. This includes CIP-004 for access granting, CIP-010 for baselines, CIP-003 for access controls, and CIP-005.	
Likes 0	
Dislikes 0	
Response	
Dante Jackson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
CEHE: Yes, allowing cloud services for in-scope Cyber Systems will bring challenges to comply with CIP-006 Physical Security requirements and will also make certain aspects of CIP-007 System Security Management infeasible for patch management, signature testing, and certain authentication controls in cases where the cloud provider provides managed services out of the customer's control.	
Likes 0	
Dislikes 0	
Response	
Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF	
Answer	Yes
Document Name	
Comment	
The NAGF requests the drafting team to consider reviewing the O&P standards for possible impacts regarding the use of 3rd Party Cloud Services (e.g., TOP-001-5 R20, R21, R23 and R24. BAL-005-1 R1 requires 6 second RTU scan rates for ACE related data).	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 5,6	

Answer	Yes
Document Name	
Comment	
Constellation agrees with NAGF comments. Kimberly Turco on behalf of Constellation Segments 5 and 6.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	Yes
Document Name	
Comment	
Constellation agrees with NAGF comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Leshel Hutchings - AEP - 3,5,6	
Answer	Yes
Document Name	
Comment	
AEP believes this SAR has the potential to affect multiple if not all CIP standards and suggests the Standard Drafting Team carefully consider how this Project will marry up with the recently (NERC Board) approved CIP virtualization changes (Project 2016-02).	
Likes 0	
Dislikes 0	
Response	

Alan Kloster - Evergy - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) in response to question #2.	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1,3	
Answer	Yes
Document Name	
Comment	
SMECO agrees with comments provided by ACES: The complexity of CSP, type of cloud deployment by the entity, and/or software vendor, cloud implementation and cybersecurity tools, etc., it is not possible to determine which will need to be modified until the DT is closer to a final draft. Trying to determine and make changes in parallel with this project will be confusing and result in more work.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	
Duke Energy supports EEI comments that CIP-015 should be added now that the Standard has been adopted by the NERC Board.	
Likes 0	
Dislikes 0	

Response	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Xcel Energy supports EEI comments and advocates for reliability standards to remain technology-agnostic and allow for backward compatibility. Xcel Energy opposes the creation of a standalone Third-party Cloud Service reliability standard.	
Likes 0	
Dislikes 0	
Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	Yes
Document Name	
Comment	
Other CIP standards tend to be scoped in terms of Applicable Systems, while cloud services by their dynamic and virtual nature are probably not going to support such a characterization. A single CIP standard focused on risk management and responsible security planning with respect to integration of cloud services as a part of critical infrastructure should be the industry approach to this opportunity. It may be the case that a risk-scaled approach should be taken with respect to how cloud services contribute to critical infrastructure and present risk based on the implemented functions (e.g. generation dispatch and other reliability operating services may require greater attention for risk mitigation measures as compared to electronic access control and monitoring functions). In areas of overlap in compliance and/or security concerns between present CIP standards, drafted CIP standards, and NERC Glossary entries, there should be some coordination of changes with respect to supporting potential future uses of cloud services while preserving present value of security measures and compliance programs.	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 1,5	
Answer	Yes
Document Name	
Comment	

Reclamation foresees addressing Cloud-Services impacting almost all NERC CIP Standards. (i.e. Access Management, Information Protection, System Security, Incident Response, Recovery, etc.)	
Likes 0	
Dislikes 0	
Response	
Joanne Anderson - Public Utility District No. 2 of Grant County, Washington - 1,4,5,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Western Power Pool - 4	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE support EEI's comment: " EEI suggests adding CIP-015 to the list of CIP standards that will need to be modified due to its recent NERC Board Adoption. Note that any changes to CIP-002 and the Control Center definition as a result of ths work may have broader impacts within the overall NERC Reliability Standards in addition to	

the CIP Standards that should be considered.

In addition to the CIP Standards, there may also be Operations and Planning Standards that could be impacted by use of cloud technology such as, TOP-001-4 R20, R21, R23, and R24 related to Control Center data exchange redundancy and testing, TOP-010 (i) R4 related to monitoring of EMS alarm processes, and BAL-005-1 R1 which requires RTU scan rates of 6 seconds or less for calculating ACE. The SDT should consider impacts to the O&P Standards as revisions/new Standards are drafted."

Likes 0	
Dislikes 0	

Response

Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - RF

Answer	
Document Name	

Comment

ITC supports the response submitted by EEI

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 1,3

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	
Document Name	

Comment

Other CIP standards tend to be scoped in terms of Applicable Systems, while cloud services by their dynamic and virtual nature are probably not going to support such a characterization. A single CIP standard focused on risk management and responsible security planning with respect to integration of cloud services as a part of critical infrastructure should be the industry approach to this opportunity. It may be the case that a risk-scaled approach should be taken with respect to how cloud services contribute to critical infrastructure and present risk based on the implemented functions (e.g. generation dispatch and other reliability operating services may require greater attention for risk mitigation measures as compared to electronic access control and monitoring functions). In areas of overlap in compliance and/or security concerns between present CIP standards, drafted CIP standards, and NERC Glossary entries, there should be some coordination of changes with respect to supporting potential future uses of cloud services while preserving present value of security measures and compliance programs.

A single CIP standard is good approach to focus specifically on the cloud system reality, that is on risk management and security planning against cloud services. If the decision is taken to allow the usage of CSP in the scope of any high or medium impact applicable systems, then a revision of the other CIP standards would necessary. Also, the standard drafting team for the new CSP standard must take into consideration the CIP-004 and CIP-011 standards which are the 2 standards for handling BCSI and its risk management. Supply Chain Risk Management (CIP-013) relative to CSP approach must be rethought and what would be sufficient address for managing cyber security risks for BCSI. For example, some points to consider are if there is another company or another group that will interact with one's data between that entity and the Cloud, how will the entity protect the data from A to Z and how will the entity be able to log, review and maintain everything in order.

As for BCS in the Cloud we believe most if not all standards regarding this new asset type can be inserted within this one single CIP standard. The drafting team should also take into consideration that it is also possible that other CIP standards that concern a special type of asset will have to be revised as well.

In both cases, the Supply Chain Risk Management (CIP-013) relative to the CSP approach must be rethought and consideration should be taken into sufficiently addressing and managing cyber security risks for BCSI.

Likes 0	
Dislikes 0	

Response

Matt Carden - Southern Company - Southern Company Services, Inc. - 1

Answer	
Document Name	

Comment

It is Southern's opinion that this project cannot be compartmentalized into a new standard as it strongly suggests. One small example is in CIP-002 where it states that high impact BCS are "used by and located at" the Control Center. If a move of BCS to cloud services is envisioned, location can't be a factor in determining whether a cloud-based control center system is or is not a BCS. We assert the approved glossary definitions and currently enforceable standards will still apply as they are "Cyber Asset" based and tie functions performed to such as practically every CIP glossary term begins with "One or more Cyber Assets that…". Thus, the DT may need to go through all the standards and address issues throughout that would preclude the use of any off-premises systems or services. A new standard it seems would be a new additional standard on top of all the rest. As has been stated by many across the industry of late, the current CIP paradigm does not contemplate off-premises systems belonging to non-registered entities and thus has requirements that to date preclude the use of cloud. It's difficult to envision a new standard that can somehow also address that root issue. Thus, we believe a far more detailed plan needs to be created and mapped out that can.

Likes 0	

Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE noticed the SAR states that a new standard should be drafted to allow existing CIP-002 through CIP-014 compliance programs to remain unchanged. While Texas RE understands the desire to lessen the impact of a new standard on registered entities, such a clear delineation may not always be possible. For example, a BES Cyber System (BCS) in the cloud would meet the BCS definition and therefore would be required to be compliant with the requirements in CIP-006. Additionally, if a new defined term was created to scope in BCS in the cloud (and conversely scope out on premises BCS) then the existing BCS glossary definition would likely need to be modified, which would in turn could impact existing compliance programs. Finally, incorporating an alternative, cloud-based compliance regime into the CIP Standards could also potentially raise a number of other demarcation issues, as well as unanticipated challenges associated with hybrid on-premises and cloud-based solutions.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	
Document Name	

Comment

The following CIP Standards have requirements directly tied to physical security or physical system configuration and will need to be addressed in some way by the standard drafting team, for example by adding language allowing alternative protection measures or modifying the “applicable systems” column:

CIP-002: R1.3

CIP-003: Attachment 1 (Low impact requirements)

CIP-004: All requirements

CIP-006: All requirements

CIP-007: R1.2

CIP-008: The definition of a Cyber Security Incident specifically includes a physical security compromise

CIP-012: All requirements. The technical rational explains that equipment used to encrypt communication should be physically secured.

The NSRF agrees with the idea to create a new separate standard to address requirements for the secure use of cloud systems. The existing CIP standards will need to be reviewed to ensure that there is no conflict with the new standard.

In addition, some vendors are offering “private cloud” or on-premise cloud solutions. This allows a cloud-based application to run on servers that reside locally in a company’s datacenter. This concept and technology should be addressed by the drafting team, especially as it relates to determining if the existing CIP requirements, or the new standard, should be applicable. There may be similar ambiguity between virtual Cyber Assets implemented using zero trust technology and cloud based Cyber Assets. All standards will need to be reviewed to ensure consistent requirements and protections regardless of the location of the Cyber Asset.

Likes 0	
Dislikes 0	

Response

Cain Braveheart - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

BPA believes it is too early, and the objectives are too broad, to be able to answer this question at this time.

Likes 0	
Dislikes 0	

Response

Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO

Answer	
Document Name	

Comment

The following CIP Standards have requirements directly tied to physical security or physical system configuration and will need to be addressed in some way by the standard drafting team, for example by adding language allowing alternative protection measures or modifying the “applicable systems” column:

CIP-002: R1.3

CIP-003: Attachment 1 (Low impact requirements)

CIP-004: All requirements

CIP-006: All requirements

CIP-007: R1.2

CIP-008: The definition of a Cyber Security Incident specifically includes a physical security compromise

CIP-012: All requirements. The technical rational explains that equipment used to encrypt communication should be physically secured.

Manitoba Hydro agrees with the idea to create a new separate standard to address requirements for the secure use of cloud systems. The existing CIP standards will need to be reviewed to ensure that there is no conflict with the new standard.

In addition, some vendors are offering “private cloud” or on-premise cloud solutions. This allows a cloud-based application to run on servers that reside locally in a company’s datacenter. This concept and technology should be addressed by the drafting team, especially as it relates to determining if the existing CIP requirements, or the new standard, should be applicable. There may be similar ambiguity between virtual Cyber Assets implemented using zero trust technology and cloud based Cyber Assets. All standards will need to be reviewed to ensure consistent requirements and protections regardless of the location of the Cyber Asset.

Likes 0	
Dislikes 0	

Response

3. Provide any additional comments for the drafting team to consider, if desired.	
Patricia Lynch - NRG - NRG Energy, Inc. - 5,6	
Answer	
Document Name	
Comment	
None	
Likes 0	
Dislikes 0	
Response	
Wendy Kalidass - U.S. Bureau of Reclamation - 1,5	
Answer	
Document Name	
Comment	
Reclamation understands the desire to push toward cloud based services for Medium and High Impact BES Cyber Systems but recommends that entities carefully consider the risks and not just the economic savings.	
Likes 0	
Dislikes 0	
Response	
Jay Sethi - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	
Document Name	
Comment	
The proposed modifications could affect many standards, which could make the implementation complex. Manitoba Hydro suggests incremental modifications may allow some of the objectives of the SAR to be met more efficiently. With the adoption of cloud services for some CIP Cyber Asset types such as EACMS, this may make it easier to reach consensus for other CIP Cyber Asset types.	
Likes 0	
Dislikes 0	

Response	
Jeffrey Streifling - NB Power Corporation - 1	
Answer	
Document Name	
Comment	

This is a great opportunity for industry to work in concert with regulators and service providers to scope a significant improvement in options available to implement and maintain critical infrastructure for the BES.

- Cloud services offer greater flexibility in support of geographic separation of redundant services that can increase reliability of functions.
- Such services allow for changes to configuration and implementation at greater speed than usually supported by on premise equipment and systems.
- Responsible entities can use cloud services to support contingency planning and scheduled exercise and testing of critical infrastructure in ways present on premise implementations tend to limit or make difficult.
- Cloud services provide significantly more resources for machine learning and generative AI applications than can easily be supported at a given entity and as those types of applications become more relevant and support critical infrastructure the need to incorporate cloud services into active compliance programs becomes even greater (e.g. modern security monitoring for network and extended host detection and response, aka NDR and XDR applications).
- Existing cloud services at assets that contain Low impact, distribution layer assets, and aggregators have already been implemented for DER and IBR and support tools for decision-making and analysis application should be considered in the proposed standard.

Likes 0	
Dislikes 0	
Response	
Joseph Gatten - Xcel Energy, Inc. - 1,3,5,6 - MRO,WECC	
Answer	
Document Name	
Comment	

Xcel Energy supports EEI comments.

Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
While new or modified CIP Standards will be the main work product of this team, it will be important to consider whether revisions to the NERC Rules of Procedure will need to be made in tandem for the revisions to be effective.We support EEI comments on this topic. We also encourage the team to consider leveraging a Field Test that can inform their revisions. A possible Field Test scenario could be to allow and study the implementation of cloud-based INSM solutions.	
Likes 0	
Dislikes 0	
Response	
Roger Perkins - Southern Maryland Electric Cooperative - 1,3	
Answer	
Document Name	
Comment	
Thank you to the DT for allowing us to comment.	
Likes 0	
Dislikes 0	
Response	
Joshua London - Eversource Energy - 1,3, Group Name Eversource	
Answer	
Document Name	
Comment	
Eversource believes that as the industry begins to transition to allow third party Cloud Services, consideration should be taken into requiring these vendors to own responsibility in protecting the data. These entities are able to participate in NERC standards development (Segment 7 and 8) and shape the regulatory environment, but at this point have no responsibility to protect the information. These entities should be audited and subjected to applicable NERC standards.	

Related to third party certifications, Eversource agrees with their use, but does not believe SOC 1 is thorough enough to be considered by the DT.

Likes 0	
Dislikes 0	

Response

Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group

Answer	
Document Name	2023-09_Unofficial_Comment_Form_05102024.docx

Comment

The proposed modifications could affect many standards, which could make the implementation complex. The NSRF suggests incremental modifications may allow some of the objectives of the SAR to be met more efficiently. With the adoption of cloud services for some CIP Cyber Asset types such as EACMS, this may make it easier to reach consensus for other CIP Cyber Asset types.

Likes 0	
Dislikes 0	

Response

Alan Kloster - Evergy - 1,3,5,6 - MRO

Answer	
Document Name	

Comment

Evergy supports and incorporates by reference the comments of the Edison Electric Institute (EEI) in response to question #3.

Likes 0	
Dislikes 0	

Response

Leshel Hutchings - AEP - 3,5,6

Answer	
Document Name	

Comment

While the scope and objectives of the SAR are clear, one consideration that remains is ERO endorsement of certifications of CSP's being recognized when it comes to being auditably compliant for CIP. Considering use of cloud has the potential to extend into multiple if not all CIP standards and also takes on many forms (e.g. SaaS, IaaS, etc.), the SAR and/or potential drafting team may consider including an objective that use case based as part of IG. Further, the SAR may consider specifically mentioning a connection to the whitepaper "BES Operations in the Cloud" published by the NERC Security Integration and Technology Enablement Subcommittee as it specifically eludes to CSP's and and Cloud Services, however is not formally part of any standard.

Likes 0	
Dislikes 0	

Response

Alison MacKellar - Constellation - 5,6

Answer	
Document Name	

Comment

Constellation suggests that this should be a NEW CIP Standard vs a revision to the current.

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Rachel Coyne - Texas Reliability Entity, Inc. - 10

Answer	
Document Name	

Comment

Texas RE encourages the SDT to carefully consider both the benefits and risks associated with the increasing integration of cloud-based solutions into Bulk Power System operations, including scenarios in which the risks outweigh the use of cloud-based solutions.

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 5,6

Answer	
Document Name	
Comment	

Constellation suggests that this should be a NEW CIP Standard vs a revision to the current.

Kimberly Turco on behalf of Constellation Segments 5 and 6.

Likes 0	
Dislikes 0	
Response	

Wayne Sipperly - North American Generator Forum - 5 - MRO,WECC,Texas RE,NPCC,SERC,RF

Answer	
Document Name	
Comment	

SAR Detailed Description section, page 6: This section references NERC's informational filing to FERC in December of 2012 and identifies several areas of interest via bullet points. The NAGF requests that the drafting team include Geofencing risks (access with the capability of affecting the BES from outside the US) along with Data Residency risks when considering new requirements.

Likes 0	
Dislikes 0	
Response	

Dante Jackson - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	
Document Name	
Comment	

CEHE:

To address the concerns associated with cloud services, CEHE recommends NERC to perform a study, develop a guidance document, and if needed, a new SAR with specific exceptions to relevant requirements that might be applicable in an industry wide. While the need to address the concerns of this SAR is recognized, a more defined scope would be beneficial. As written, it is unclear what the proposed standard or standard revision is, and there is no reference to the inadequacy of existing standard language. CEHE Supports EEI's comments regarding question three.

Likes 0	

Dislikes 0	

Response

David Jendras Sr - Ameren - Ameren Services - 1,3,6

Answer	
Document Name	

Comment

Regarding BES assets, Ameren would like more clarity on whether cloud services can be used for monitoring, control functions, or both.

Likes 0	
Dislikes 0	

Response

Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable

Answer	
Document Name	

Comment

EEI acknowledges that this SAR was submitted to address cloud use cases in general but asks the drafting team to consider including concepts specific to Artificial Intelligence given the increase in interest in the technology since the time the SAR was submitted and its dependence on the use of cloud technology. Concepts associated with AI include but are not limited to, the establishment of an AI risk management framework that incorporates model development, validation, and governance processes.

Additionally, EEI agrees and supports the use of third-party certifications and attestations as an important component of third-party risk-management for cloud technology. NERC's acceptance of third-party security certifications and attestations as direct evidence of compliance may not be an item that can be addressed directly, or singularly, by a Standard Drafting Team. While our proposed revisions to the SAR in response to Question 1 are meant to align the SAR with the DT's authority to address the challenge, we note that acceptance of independent third-party certifications and/or attestations may require additional work outside of the Standards Development process including revisions to the NERC Rules of Procedure, or via other legal or CMEP related mechanisms in coordination with NERC and/or FERC.

Lastly, we request minor non-substantive revisions to the SAR to align the terminology used such as changing Standard Drafting Team (SDT) to Drafting Team (DT) throughout, ensuring that the terms certifications and attestations are used consistently together throughout the document, and referring to third-party certifications as "independent third-party certifications and/or attestations."

Likes 0	
Dislikes 0	

Response

David Buchold - Southern Indiana Gas and Electric Co. - 3,5,6 - RF

Answer	
Document Name	
Comment	
No Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	
Document Name	
Comment	
Additional feedback for the SDT to consider: ***Holistic or incremental:*** SPP supports a Holistic approach. The flexibility lies with the responsible entity to determine the risk, and then implement how they see fit to insure the reliability of the BES. ***Timing*****:** SPP supports the projected 12–18-month submittal to FERC. ***Flexibility*****:** SPP recommends that SDT propose only what can be enforceable.	
Likes 0	
Dislikes 0	
Response	
Matt Carden - Southern Company - Southern Company Services, Inc. - 1	
Answer	
Document Name	
Comment	
Southern has concerns about how the current requirements for training, security, access, backgrounds, revocations, periodic verifications, etc., will be addressed for systems using cloud providers. If these requirements were to be measured with 3rd party certifications, one question is certification against what requirements in what standards? For example, a CSP is not going to have an entity's CIP Senior Manager approve changes to CIP-007 R2 patch mitigation plans for a security patch to their hypervisor, but that is a mandatory requirement if the system is on-premises. Another example is a CSP is not going to have incident response reporting requirements to the E-ISAC if an incident happens in the underlay, but that is the mandatory	

requirement for an on-premises system. Several requirements like these will need review and potential rewrite or rescoping to avoid inconsistencies between the same risks occurring on vs. off premise systems.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 1,2,3,4,5,6,7,8,9,10 - NPCC, Group Name NPCC RSC

Answer	
Document Name	

Comment

This is a great opportunity for industry to work in concert with regulators and service providers to scope a significant improvement in options available to implement and maintain critical infrastructure for the BES.

{C}· Cloud services offer greater flexibility in support of geographic separation of redundant services that can increase reliability of functions.

{C}· Such services allow for changes to configuration and implementation at greater speed than usually supported by on premise equipment and systems.

{C}· Responsible entities can use cloud services to support contingency planning and scheduled exercise and testing of critical infrastructure in ways present on premise implementations tend to limit or make difficult.

{C}· Cloud services provide significantly more resources for machine learning and generative AI applications than can easily be supported at a given entity and as those types of applications become more relevant and support critical infrastructure the need to incorporate cloud services into active compliance programs becomes even greater (e.g. modern security monitoring for network and extended host detection and response, aka NDR and XDR applications).

{C}· Existing cloud services at assets that contain Low impact, distribution layer assets, and aggregators have already been implemented for DER and IBR and support tools for decision-making and analysis application should be considered in the proposed standard.

For CIP-011-3, the new version is considering the cloud service reality, and the narrative of the standard has changed to include risk management and confidentiality breach. In our opinion, the second requirement for the reuse and disposal should be adapted, to include the elimination of client's data on the CSP end (ex: records concerning the elimination of BCSI client data prior to termination of contract).

We believe that that Cloud services need to address in a CIP standard as more and more services utilize cloud services.

We offer the following points for consideration:

-Localization of the entities data: Needs to be addressed in the initial CIP-013 contract thus ensuring that the entity knows where the data will be saved,

both for the main location and backup.

-What will happen during the contract if the entity decides to change cloud service providers? This should also be covered in CIP-013.

-What will happen if there's a breach on the cloud service provider's side? Will they inform us about when, how, and next steps?

-Forced to use your own key (BYOK) and have a process to manage keys.

-Provisions need to include in the event of termination of the cloud services contract and the handling of the entities data. What will happen to the entities data if you end the contract? A certificate needs to be provided by the cloud service provider specifying that provisions written in the contract have been successfully followed.

-How will the entity maintain NERC compliance with something they don't own?

Likes 0	
Dislikes 0	

Response

Kinte Whitehead - Exelon - 1,3

Answer	
Document Name	

Comment

Exelon is aligning with EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Jennifer Bray - Arizona Electric Power Cooperative, Inc. - 1

Answer	
Document Name	

Comment

Thank you for the opportunity to comment.

Likes 0	
Dislikes 0	

Response

Monika Montez - California ISO - 2 - WECC, Group Name ISO/RTO Council Standards Review Committee (SRC)	
Answer	
Document Name	

Comment

The SRC believes this is a great opportunity for industry to work in concert with regulators and service providers to leverage an increasing number of options available to implement and maintain critical infrastructure for the BES.

- *Cloud services offer greater flexibility in support of geographic separation of redundant services that can increase reliability of functions.*
- *Such services allow for changes to configuration and implementation at greater speed than usually supported by on-premises equipment and systems.*
- *Responsible entities can use cloud services to support contingency planning and scheduled exercise and testing of critical infrastructure in ways current on-premises implementations tend to limit or make difficult.*
- *Cloud services provide significantly more resources for machine learning and generative AI applications than can easily be supported at a given entity. This will become increasingly important as those types of applications become more relevant in supporting critical infrastructure and as the need to incorporate cloud services into active compliance programs becomes even greater (e.g. modern security monitoring for network and extended host detection and response, such as NDR and XDR applications).*
- *Existing cloud services at assets that contain Low impact, distribution layer assets, and at aggregator assets have already been implemented for DER and IBR and in support tools for decision-making and analysis. This application should be considered in the proposed standard.*
- *Ensure that cloud providers' auditability includes complementary reporting tools to meet our regulatory requirements. This would help reduce the workload on our staff by aligning with existing audit efforts.*

***Industry Need** (pages 2-4): The SRC recommends the SAR be expanded to cite and include a reference to the paper that SERC and RF co-authored on the risks of not leveraging cloud-based services: https://www.rfirst.org/resource-center/the-emerging-risk-of-not-using-cloud-services/.*

***Detailed Description** (page 5):*

- ***Auditability and use of third-party certifications** - the SRC suggests adding a reference to CSA STAR*
- *"Accepting independent third-party security assurance certifications/ attestations such as FedRAMP, SOC, ISO, CSA STAR, or others"*
- ***New or revised standard(s)** – We support hybrid solutions, i.e. use of cloud for some CIP-defined systems, while ensuring backwards compatibility for others.*
- ***Holistic or incremental** - We support this flexibility. Recognizing the SDT may find it difficult to develop requirements suitable to allow the use of cloud for all CIP-defined systems under the initial project, it may be easier to develop requirements applicable to the use of cloud for individual or groups of CIP-defined systems, e.g. Software as a Service (SaaS) applications, as a starting point.*
- ***Timing** – We strongly support the target deliverable date of 12-18 months for submittal to FERC to avoid the type of delays associated with Project 2016-02 (Virtualization).*

***Cost Impact Assessment** (page 6): Expand this section to acknowledge the benefits of reciprocity.*

- *Responsible Entities that implement CIP-regulated workloads in the cloud will incur costs related to compliance program revisions; however, these costs may be offset by the benefits of reciprocity.[1] Executed appropriately, reciprocity reduces redundant testing, assessment and documentation, and the associated costs in time and resources.[2]*

[1] "Reciprocity" is the "agreement among participating organizations to accept each other's security assessments, to reuse system resources, and/or to accept each other's assessed security posture to share information."

[2] DOD Cybersecurity Reciprocity Playbook (https://dodcio.defense.gov/Portals/0/Documents/Library/(U)2024-01-02DoDCybersecurityReciprocity%20Playbook.pdf) page 4, section 3.1.

Likes 0	

Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - RF	
Answer	
Document Name	
Comment	
ITC supports the response submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	
Document Name	
Comment	
ERCOT joins the comments submitted by the IRC SRC and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Hillary Creurer - Allete - Minnesota Power, Inc. - 1	
Answer	
Document Name	
Comment	
Minnesota Power supports EEI’s comments.	
Likes 0	
Dislikes 0	
Response	

Richard Vendetti - NextEra Energy - 5	
Answer	
Document Name	
Comment	
NEE support EEI's comment: " EEI acknowledges that this SAR was submitted to address cloud use cases in general but asks the drafting team to consider including concepts specific to Artificial Intelligence given the increase in interest in the technology since the time the SAR was submitted and its dependence on the use of cloud technology. Concepts associated with AI include but are not limited to, the establishment of an AI risk management framework that incorporates model development, validation, and governance processes. Additionally, EEI agrees and supports the use of third-party certifications and attestations as an important component of third-party risk-management for cloud technology. NERC's acceptance of third-party security certifications and attestations as direct evidence of compliance may not be an item that can be addressed directly, or singularly, by a Standard Drafting Team. While our proposed revisions to the SAR in response to Question 1 are meant to align the SAR with the DT's authority to address the challenge, we note that acceptance of independent third-party certifications and/or attestations may require additional work outside of the Standards Development process including revisions to the NERC Rules of Procedure, or via other legal or CMEP related mechanisms in coordination with NERC and/or FERC. Lastly, we request minor non-substantive revisions to the SAR to align the terminology used such as changing Standard Drafting Team (SDT) to Drafting Team (DT) throughout, ensuring that the terms certifications and attestations are used consistently together throughout the document, and referring to third-party certifications as "independent third-party certifications and/or attestations."	
Likes 0	
Dislikes 0	
Response	
Steven Rueckert - Western Electricity Coordinating Council - 10, Group Name WECC CIP	
Answer	
Document Name	
Comment	
none	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,4,5,6, Group Name FE Voter	
Answer	
Document Name	
Comment	

EEI acknowledges that this SAR was submitted to address cloud use cases in general but asks the drafting team to consider including concepts specific to Artificial Intelligence given the increase in interest in the technology since the time the SAR was submitted and its dependence on the use of cloud technology. Concepts associated with AI include but are not limited to, the establishment of an AI risk management framework that incorporates model development, validation, and governance processes.

Additionally, EEI agrees and supports the use of third-party certifications and attestations as an important component of third-party risk-management for cloud technology. NERC's acceptance of third-party security certifications and attestations as direct evidence of compliance may not be an item that can be addressed directly, or singularly, by a Standard Drafting Team. While our proposed revisions to the SAR in response to Question 1 are meant to align the SAR with the DT's authority to address the challenge, we note that acceptance of independent third-party certifications and/or attestations may require additional work outside of the Standards Development process including revisions to the NERC Rules of Procedure, or via other legal or CMEP related mechanisms in coordination with NERC and/or FERC.

Lastly, we request minor non-substantive revisions to the SAR to align the terminology used such as changing Standard Drafting Team (SDT) to Drafting Team (DT) throughout, ensuring that the terms certifications and attestations are used consistently together throughout the document, and referring to third-party certifications as "independent third-party certifications and/or attestations."

Likes 0	
Dislikes 0	
Response	

Israel Perez - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	

SRP strongly recommends the creation of a new CIP standard, plus provide clarity on the regulated Systems.
In addition:
• 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.
o Define Cloud Services and what scope is for each cloud service.
o Recommend new CIP standards applicability for Low Impact to begin.
o Will need provisions for continued monitoring.

• 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.
o Depending on applicability, could start from the ground up, i.e. low impact
o Recommend incremental.
o Need clarity and detail on this.

o Scope should not include high impact BCS assets as these should not be allowed to move to the cloud for reliability reasons which is the reason CIP standards exist. It is very likely that medium impact BCS assets not be allowed to move to the cloud due to negative reliability implications.

• Allow the use of third-party security certifications to support the auditability of the new or revised requirements.
o Concerned with third-party security certifications possibly being used as a means of manipulation.
o We think it would be acceptable to allow security management tools to help audit and configure. We don’t think it would be acceptable to allow cloud providers to audit themselves. We also do not think it is sufficient to allow industry standards such as FEDRAMP to be the benchmark. This would need to be layered, such as FEDRAMP plus independent security assessments of cloud services that audits the implementation and configuration.

• 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.
o Scope should include separating Electronic Access Control or Monitoring Systems into Electronic Access Control Systems and Electronic Access Monitoring Systems with specific definitions for each classification.

• Coordinate with other CIP project drafting teams on conflicts or continuity matters, as necessary.
The CIP standards classify systems only by means of "High", Medium, and Low impact based on VA and MW. This method of classification does allow differentiation of safety issues associated with moving control systems to third-parties. Decisions about moving to third-party services must include a full safety review and consequence review.
Scope should not include moving control of CIP High, Medium, and Low generation assets to third party cloud services due to the risk of life safety to communities surrounding generation facilities. As an example, some generation facilities include chemicals that have potential to kill entire communities of people if released. Critical safety systems must never be allowed to be operated remotely where a network connection might interfere with operating critical safety systems. In addition to chemicals, rotating mass of generators at facilities could have significant impact to life and property (think dams) which could have a very large impact to communities and the nation. It is the opinion of SRP that no control systems that have life safety consequences should be managed or hosted by third-parties. This is a safety control that must be maintained by any CIP standard regardless of the financial influences that come from these third parties.

Also, scope should not allow high impact BCS Transmission Control Centers to be managed or hosted by third-parties. Moving BCS Transmission assets to the cloud introduces additional fault domains which is highly likely to decrease reliability of the bulk electric system. If the CIP standards enable reduction in the reliability of the BES then the standards do not meet the stated goals of CIP regulations. There are components such as data hosting, data analysis, data analytics, digital twins, ICCP, and market operations that can be hosted or managed safely by third-parties, but control of transmission assets introduces too many variables to be considered reliable enough for the US transmission systems. These distinctions must be addressed by any change in this standard.
There could be situations of low impact distribution and generation systems that would make sense to be managed or hosted by third-parties. The "low impact" designation probably is not accurate enough to reflect all of the nuances associated with these systems. The standard should consider introducing new terms such as "micro impact" or specifying a megawatt or volt amp limit below which control systems could safely be hosted or managed by third-parties. We understand that there may be non-critical components of these control systems that could be managed by a third party without increasing risk of negative consequence (e.g. turbine performance monitoring, transformer monitoring, water treatment, compliance monitoring, cyber security monitoring, etc).

SRP recommends that the scope of this project be limited to allowing data associated with control systems such as historian, BCSI, etc. to be hosted and managed by third-parties. But allowing hosting and management to include control of BCS assets is not warranted or safe. The scope of this SAR should specifically disallow control of most BCS assets except, maybe, if enough justification and engineering value exists of smaller assets such as DERs, wind farms, micro solar, etc.

Likes 0	
Dislikes 0	

Response

Rachel Schuldt - Black Hills Corporation - 1,3,5,6, Group Name Black Hills Corporation - All Segments	
Answer	
Document Name	
Comment	

Black Hills Corporation agrees with EEI's statements, with additional input: EEI acknowledges that this SAR was submitted to address cloud use cases in general but asks the drafting team to consider including concepts specific to Artificial Intelligence given the increase in interest in the technology since the time the SAR was submitted and its dependence on the use of cloud technology. Concepts associated with AI include but are not limited to, the establishment of an AI risk management framework that incorporates model development, validation, and governance processes. Security of data, quality. New set of risks that need to be managed in a Cloud environment for AI.

Additionally, Black Hills Corporation agrees with EEI's support for the use of third-party certifications and attestations as an important component of third-party risk-management for cloud technology. NERC's acceptance of third-party security certifications and attestations as direct evidence of compliance may not be an item that can be addressed directly, or singularly, by a Standard Drafting Team. While our proposed revisions to the SAR in response to Question 1 are meant to align the SAR with the DT's authority to address the challenge, we note that acceptance of independent third-party certifications and/or attestations may require additional work outside of the Standards Development process including revisions to the NERC Rules of Procedure, or via other legal or CMEP-related mechanisms in coordination with NERC and/or FERC.

Lastly, we request minor non-substantive revisions to the SAR to align the terminology used such as changing Standard Drafting Team (SDT) to Drafting Team (DT) throughout, ensuring that the terms certifications and attestations are used consistently together throughout the document, and referring to third-party certifications as "independent third-party certifications and/or attestations."

Likes 0	
Dislikes 0	
Response	

Marcus Bortman - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	
Comment	

AZPS has no additional comments at this time.

Likes 0	
Dislikes 0	
Response	

Maggy Powell - Amazon Web Services - 7	
Answer	
Document Name	

Comment
The unique nature of this drafting work creates the opportunity to explore approaches to achieving the necessary level of bulk-power system security that differ from those used in the existing standards for the last decade-and-a-half. The SDT should be encouraged to consider ways to achieve the security objectives while requiring compliance controls that are suited to a third-party cloud environment. Also, engagement by the audit community in the standard drafting discussions can help address auditability considerations. Clarity on the compliance assessment approach aids in understanding of the compliance demonstration expectations and management of compliance risk. Because the compliance assessment expectations will be a key input to contractual arrangements between Responsible Entities and cloud service providers, it is essential that those expectations be clear and also that the compliance assessment approach enable a many-to-one approach so that cloud service providers need not have entity-specific requirements. Creation of this standard will give Responsible Entities the option, not the requirement to adopt cloud services for regulated systems. Because this standard will unblock use of technology rather than impose new requirements on existing use cases and the applicability occurs when a Responsible Entity puts into production cloud services for regulated systems, implementation of the requirements should be immediate upon FERC approval so that Responsible Entities that desire to do so can begin implementing cloud-based CIP-compliance services. For Responsible Entities that choose not to use cloud-based services for aspects of their CIP environment, the new standard will have no impact.

Likes 0	
Dislikes 0	

Response