Comment Report

Project Name:	2021-03 CIP-002 | Standard Authorization Request
Comment Period Start Date:	6/10/2025
Comment Period End Date:	7/9/2025
Associated Ballots:	

There were 40 sets of responses, including comments from approximately 114 different people from approximately 85 companies representing 8 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 CIP-002 is the right standard to address the goals of the SAR? If not, please provide the standard recommendation and explanation.

3. The cost impacts to address the objections of the SAR are unknown. What are the cost aspects associated with addressing the objections of the SAR? Please provide your explanation.

4. 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
					George Brown	Pattern Operators LP	5	MRO
					Amy Key	MidAmerican Energy Company (MEC)	1	MRO
					Seth Shoemaker	Muscatine Power & Water	1,3,5,6	MRO
					Michael Ayotte	ITC Holdings	1	MRO
					Peter Brown	Invenergy	5,6	MRO
					Angela Wheat	Southwestern Power Administration	1	MRO
					Joshua Phillips	Southwest Power Pool	2	MRO
					Patrick Tuttle	Oklahoma Municipal Power Authority	4,5	MRO
					Hayden Maples	Evergy	1,3,5,6	MRO
					Kirsten Rowley	MISO	2	MRO
					Andrew Coffelt	Kansas City Board of Public Utilities	1,3,5,6	MRO
Exelon	Daniel Gacek	1,3		Exelon	Daniel Gacek	Exelon	1	RF
					Kinte Whitehead	Exelon	3	RF

PJM Interconnection, L.L.C.	Elizabeth Davis	2	RF,SERC	ISO/RTO Standards Review Committee	Kirsten Rowley	Midcontinent ISO, Inc.	2	RF
					Gregory Campoli	New York Independent System Operator	2	NPCC
					Joshua Phillips	Southwest Power Pool, Inc. (RTO)	2	MRO
					Monika Montez	CAISO	2	WECC
					Thomas Foster	PJM Interconnection, L.L.C.	2	RF
					John Pearson	ISO New England, Inc.	2	NPCC
					Kennedy Meier	Electric Reliability Council of Texas, Inc.	2	Texas RE
Southern Company - Southern Company Services, Inc.	Jennifer Tidwell	1,3,5,6	SERC	Southern Company	Leslie Burke	Southern Company - Southern Company Generation	5	SERC
					Matt Carden	Southern Company - Southern Company Services, Inc.	1	SERC
					Ron Carlsen	Southern Company - Southern Company Generation	6	SERC
					Joel Dembowski	Southern Company - Alabama Power Company	3	SERC
Black Hills Corporation	Josh Schumacher	1,3,5,6		Black Hills Corporation Segments 1, 3, 5, 6	Trevor Rombough	Black Hills Corporation	1	WECC
					Josh Combs	Black Hills Corporation	3	WECC
					Sheila Suurmeier	Black Hills Corporation	5	WECC
					Josh Schumacher	Black Hills Corporation	6	WECC

FirstEnergy - FirstEnergy Corporation	Mark Garza	1,3,4,5,6		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
Northeast Power Coordinating Council	Ruida Shu	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
					Salvatore Spagnolo	New York Power Authority	1	NPCC
					Sean Bodkin	Dominion - Dominion Resources, Inc.	6	NPCC
					Silvia Mitchell	NextEra Energy - Florida Power and Light Co.	1	NPCC
					Sean Cavote	PSEG	4	NPCC

					Jason Chandler	Con Edison	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
					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
					Emma Halilovic	Hydro One	1,3	NPCC
					Philip Nichols	National Grid	1	NPCC
					Emma Halilovic	Hydro One	1,3	NPCC
					Caver Powers	Utility Services	5	NPCC
Dominion - Dominion Virginia Power	Steven Belle	1,3		Dominion	Steven Belle	Dominion Energy	1	NA - Not Applicable
					Victoria Crider	Dominion Energy	3	NA - Not Applicable
					Sean Bodkin	Dominion Energy	6	NA - Not Applicable
					Barbara Marion	Dominion Energy	5	NA - Not Applicable

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.

Kimberly Turco - Constellation - 5,6	
Answer	No
Document Name	
Comment	

Constellation does not agree with the scope and objectives of this SAR. Constellation disagrees with the identification and classification of the PACS, EACMS and PCAs occurring under the CIP-002 Standard.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	
Response	

James Keele - Entergy - 1,3,6	
Answer	No
Document Name	
Comment	

First, Entergy does not agree with the scope and objectives of the standard as currently described. The primary concern being that recent revisions to the NERC CIP standards, including newly created standards, have aligned with a more risk-based approach when considering the security and impact to the Bulk Electric System (BES), and a reduction in administrative/"paperwork" type requirements. As currently scoped the concern is that a "paperwork" error (e.g. mis-typing, mis-selecting a field in a system) could result in a NERC CIP violation and all the internal and external paperwork and review that accompanies it, even if there was not an identified security risk to the BES, and therefore the level of effort to maintain and/or report compliance with this standard may not be commensurate with risk-reduction.

For example, if an entity were to identify that an asset classification had been changed in their system of record from "EACMS" to "Non-CIP", yet every single other CIP required security control was still in-place and effective, would this be a reportable CIP violation? If yes, entities would be required to do their internal CIP reporting causual evaluations, report to their entity, collect data, create mitigation plans, discuss on calls, etc. and spend thousands of dollars for this documentation. Today this type of issue would be corrected, a quick review of how it happened done, maybe a stand-down or training, and entities continue their security work.

Additionally, as this is largely a manual process in some fashion, whether your repository is in a spreadsheet, database, or cutting edge system, application of a CIP classification is human dependent and therefore increasingly subject to human-error such as mis-clicks, mistypes, etc. This may

require entities to spend additional time and resources for constant peer-checks/reviews of asset classifications in their inventory (that may not be automateable for application of the CIP definitions) which depending on how those classifications are used in processes/tools may not be an efficient use of resources based on risk.

CIP Version 5 represented a more risk-based approach by having CIP-002 identify critical **systems** based on function rather that discrete assets, and was a welcomed change. However, to return to the CIP Version 3 expectation of discrete lists of assets at all times, even if security controls are applied, seems like a step back from the progress of the standards.

Entergy could support this potential new standard if care is given to take a risk-based approach to avoid/reduce the reportability of minor or administrative errors whether through the use of reasonable timelines or other methods in the standard, and reduce the expectation to monitor the classification of assets on a near-realtime basis. There is a huge risk difference between an asset being mis-classified in a database for a week and all security controls being in place vs. not classifying a clearly critical/CIP system as in-scope and not applying security controls because of it. Any standard should delineate between these two, and preferably minor/non-impact type issues be not reportable such that administrative errors are not overly punitive, whether by financial penalty and/or the administrative work required to report them.

Secondly, Entergy does not agree with the scope of the standard revision as written because it excludes BES Cyber Assets. The current version of CIP-002 requires entities to identify BES Cyber Systems in a list as required, but not BES Cyber Assets. This new requirement would result in entities still identifying BCS at the system level, but EACMS, PACS, PCA, at the individual asset level. Under the standard as proposed the Misclassification of a BCA, the systems most critical to the grid, would not be a violation but PCAs merely connected via a routable protocol would be a violation, regardless of the application of security controls. If the intent is to require the discrete identification of CIP Cyber Assets, then the standard should require the identification of all CIP Cyber Asset types at the asset level, including BCA.

Likes 0	
Dislikes 0	

Response

Alison MacKellar - Constellation - 5,6

Answer	No
Document Name	

Comment

Constellation does not agree with the scope and objectives of this SAR. Constellation disagrees with the identification and classification of the PACS, EACMS and PCAs occurring under the CIP-002 Standard.

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

Andrew Smith - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS is not opposed to the objectives of this SAR; however, the scope of the SAR does not allow the drafting team to determine the most efficient options for addressing the risks documented in the SAR. AZPS respectfully recommends removing specific solutions to address the gap to allow for the drafting team to explore all potential solutions.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
We appreciate the compliance issue that is raised when an EACMS, PACS, or PCA is not identified by an entity and there is not a single, clear requirement on which to associate the non-compliance (as there is with a BCS in CIP-002 R1). We also appreciate how inefficient it would be for all involved parties to turn this scenario into multiple dozens of individual violations against many requirements. It seems a simple fix would be to add an identification requirement similar to CIP-002 R1 for all these associated systems, such as: “Each Responsible Entity shall identify the EACMS, PACS, and PCAs associated with the high and medium impact BCS identified in R1.” However, we believe that such a fix is anything but simple and may indeed exacerbate other issues especially as we think about the types of technology to which it is increasingly applied. One issue is Cyber Assets today are increasingly multipurpose and it’s a problem to hang all the right “tags” of glossary terms on a Cyber Asset. A prime example as cyber security becomes embedded ever more is EACMS; it is increasingly hard to find a Cyber Asset that is not in some way “performing electronic access control or monitoring”. A goal of Zero Trust is to embed electronic access control into more and more policy enforcement points, creating an order of magnitude more “little ESPs” at a device or even individual service level. This will make it increasingly more difficult to create and maintain a list. A more strategic solution is needed because “electronic access control” is a function or service, not a dedicated electronic device type (the EACMS definition is essentially “One or more ‘programmable electronic devices’ that perform…”). This SAR further embeds that paradigm of EACMS as a device. On a related note, with a new “identify EACMS” requirement in CIP-002, if an entity has a device that is a BCS but is also performing some EACMS functions, is it a violation if the entity only lists it as a BCS? We foresee this SAR could create more future administrative non-compliances in CIP-002 when there is no difference in the cyber security posture of the system, it is merely a violation of requirements to identify Cyber Assets (all these definitions begin with “One or more Cyber Assets that…”) by function in an increasingly multifunction and dynamic world. Virtualization, containerization, and orchestration are large drivers of this. Cyber Assets are becoming “platforms” on which functions/apps are dynamically instantiated. Therefore, what a Cyber Asset “is” at any point in time may be changing based on what services or apps are dynamically	

instantiated on it. We are increasingly in a world where an annual process of identification of Cyber Assets and putting defined terms on them by function performed is problematic.

A second issue is PCAs are becoming far more dynamic. Today it is a Cyber Asset inside the ESP. Project 2016-02 added a new way for a VCA to become a PCA by adding the scenario of sharing CPU/RAM with a BCS VCA. So, if a VCA ever shares the same hypervisor with a BCS it becomes an associated PCA.

However, if you have a new CIP-002 requirement for the identification of PCAs, that does not simply mean list all the Cyber Assets within an ESP, it means knowing all current and future VCAs in a virtualized environment that may instantiate on a hypervisor with a BCS. That is a very dynamic scenario that entities will struggle with simply because the paradigm of “inventory of devices on a network switch in the ESP” does not match the evolving technology. It was designed such that entities could tag virtual workloads (VCAs) with differing tags and configure policy so that hypervisors keep the VCAs separated. The technology handles this through *policy*, but it does not lend itself to CIP-002 style identification and inventory.

A third issue is drafting teams are working on the issues of incorporating cloud services with examples in their SAR of “EACMS as a service” such as cloud-based MFA services (Duo, etc.). If an entity must list all Cyber Assets involved in electronic access control or monitoring in CIP-002, that doesn’t work in today’s Service-Oriented Architectures (SOA) where such services can be on or off-premise and dynamic by nature. A core issue is functionality of logic is increasingly not tied to a device or even an operating system instance.

We believe that the now 20+ year old "device model" of viewing the world as Cyber Assets dedicated to functions is causing issues with today's dynamic technology. It begs the question of should we be writing more requirements that further embed that paradigm?

We believe that a drafting team assigned to this SAR will have to deal with questions like the following as entities using or planning to use these technologies struggle to fit it into the static configuration mindset:

• Cyber Asset #1 is a Docker node in a Kubernetes cluster in my own data center. It may or may not therefore be a PACS depending on whether Kubernetes dynamically instantiates the SQL server container for my employee badging system on it. Am I in violation if I don’t “identify” it as a PACS during the time it had the container for the SQL server instantiated on it?

• Cyber Asset #2 currently has a BCS VCA executing on it. Within the hypervisor underlay, it is enforcing some zero trust policies for electronic access to the VCAs it hosts. Am I non-compliant if this Cyber Asset isn’t listed as both a BCS and an EACMS?

• I’ve used “Infrastructure as Code” tools and can recreate my entire environment (networks, firewalls, servers, applications, databases, etc.) at any data center within minutes. How do I handle this with CIP-002’s lists?

• My BCS has some on-premise components, but also has some components that are cloud-based. These all work together as one system. What do I include on my CIP-002 lists and how do I handle all the “electronic access control and monitoring” of the cloud provider’s environment that I configure but don’t control?

These questions are designed to show this is anything but a simple “The Responsible Entity shall identify its EACMS, PACS, and PCAs” in today’s world. The whole model of terms that begin with “One or more Cyber Assets that perform ” is becoming increasingly outdated and new requirements extending this paradigm may end up doing two things:

• Discouraging the use of technology that can increase the reliability and resiliency of functions and services that impact BES reliability as entities struggle to statically configure naturally dynamic environments merely for the sake of CIP lists.

• Keeping the focus at the wrong levels/layers instead of where the cyber risk has moved as technology marches on.

While this SAR may seem a fairly simple answer to handle a compliance monitoring issue, we believe it will raise far more complex issues as entities encounter the “devil in the details” implications in more modern technologies and architectures.

Likes 0	
Dislikes 0	

Response

Robert Brown - AEP - 1,3,5,6 - MRO,Texas RE,RF	
Answer	No
Document Name	

Comment
AEP recognizes the desire to reduce administrative burdens; however, we are concerned about how this may affect grid reliability. We believe that the current approach may prioritize documentation over the reliability of the grid. A thorough root cause analysis is necessary. How does CIP-015-1 already address this SAR? Future iterations of the CIP standards should consider classifications for EACMS, PACS, and PCAs. AEP suggests an amendment to CIP-002 to clearly identify either a system or an asset and to update the definitions of EACMS, PACS, and PCAs.

Likes 0	
Dislikes 0	

Response

Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	No
Document Name	

Comment
BPA supports the concept behind this SAR, however the scope should be expanded to include identification of new CIP categories being introduced in other NERC projects such as 2016-02 for virtualization. Under that project, CIP-002-7 has already been filed with FERC without language to identify “CIP applicable” systems.

Likes 0	
Dislikes 0	

Response

Erik Gustafson - TXNM Energy - 1,3 - WECC,Texas RE	
Answer	No
Document Name	

Comment
If an associated Cyber Asset is not properly identified, and a Self-Report is being filed for the Potential Non-Compliance (PNC), the reliability and security of the BES is not affected by the Standard under which the Self-Report is filed, whether it be CIP-002, CIP-010, or any other Standard. Additionally, TXNM believes that the identification of the associated Cyber Assets is implied, known, and expected. Tying the identification of these associated Cyber Assets to an enforceable Standard may create undue compliance risks. Furthermore, if this SAR fails, TXNM does not believe the

statement from the SAR which states failures to identify these devices would result in multiple violations across the CIP requirements is a tenable solution to either the Responsible Entity or the Regional Entity.

Additionally, PCA are typically identified during the identification of the ESP (CIP-005) which would technically occur after the proposed identification of the associated Cyber Asset(s) in CIP-002, if this SAR were to pass.

Likes 0	
Dislikes 0	

Response

Timothy Singh - Salt River Project - 1,3,5,6 - WECC

Answer	No
Document Name	

Comment

SRP mostly agree with the scope and objectives to this SAR. There is some reservations over the scope including PCAs as a requirement for CIP-002 Cyber Asset list inclusion, as some believe PCAs don't warrant enough of a potential impact to the BES to merit a required inclusion on the CIP-002 CA list.

Likes 0	
Dislikes 0	

Response

Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC

Answer	No
Document Name	

Comment

It is not clear to us the value of identifying EACMS, PCA, and PACS in CIP-002 in terms of security posture if violations are "rolled up" to CIP-002. The roll up needs to be explicitly allowed in the written language of the proposed revision of CIP-002 standard so to leave no room for confusion for the auditors. The verbiage on the SAR seems to imply that "roll up" is a common practice, in the proposed revision of CIP-002 it needs to be formalized so that it can become a standard practice.

Likes 0	
Dislikes 0	

Response

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

Answer	No
Document Name	
Comment	
ITC supports the comments submitted by EEI	
Likes 0	
Dislikes 0	
Response	
Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE	
Answer	No
Document Name	
Comment	
CenterPoint Energy Houston Electric, LLC (CEHE) suggests that a requirement be established for developing and maintaining a discrete list within CIP-002, which includes EACMS, PACS, and PCAs.	
Likes 0	
Dislikes 0	
Response	
TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 1,3,5,6 - RF	
Answer	No
Document Name	
Comment	
Southern Indiana Gas and Electric d/b/a CenterPoint Energy Indiana South (SIGE) suggests that a requirement be established for developing and maintaining a discrete list. SIGE also suggests that BCAs, (BES Cyber Assets), be included in addition to EACMS, PACS and PCA. Additionally, identification of BCAs, EACMS, PACS, and PCA should all be addressed in CIP-002 and not broken into multiple standards, except for adding a statement in CIP-003 that a discrete list is not required for low impact.	
Likes 0	
Dislikes 0	
Response	
Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	

Answer	No
Document Name	Project 2021-03 CIP-002 Comment_Form.docx
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Peters - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	Yes
Document Name	
Comment	
Manitoba Hydro suggest adding “add modify or retire Glossary Term” to the SAR. The SAR seeks to formalize identification of EACMS, PACS and PCA. The drafting team may find that some of the Glossary of Terms can be moved into a requirement (as was found in Project 2016-02), the scope of the SAR should allow this modification if required by the drafting team.	
Likes 0	
Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	Yes
Document Name	Project 2021-03 CIP-002 Identification Unofficial_Comment_Form.docx
Comment	
The MRO NSRF supports the scope and objectives of the SAR.	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC	
Answer	Yes
Document Name	

Comment
HQ supports the following NPCC TFIST comment: TFIST would request that an attachment be added to CIP-002 for the identification of categorization of CIP applicable system (EACMS, PACS, and PCAs).

Likes 0	
Dislikes 0	

Response

Lucinda Bradshaw - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	

Comment
N/A

Likes 0	
Dislikes 0	

Response

Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	Yes
Document Name	

Comment
TFIST would request that an attachment be added to CIP-002 for the identification of categorization of CIP applicable system (EACMS, PACS, and PCAs).

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 and objectives of the SAR.	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
ATC thanks the SDT for requesting modifications to bring clarity for Cyber Asset classification, and is supportive of modifications that both formalize this requirement and alleviate the administrative burden associated with having to prepare and manage multiple self-reports or findings that would spawn from a failure to identify and classify, or misclassification at the Cyber Asset level.	
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 for quesiton #1.	
Likes 0	
Dislikes 0	
Response	
Nick Leathers - Ameren - Ameren Services - 1,3,5,6 - MRO,SERC	
Answer	Yes
Document Name	
Comment	

Ameren believes this is a reasonable request for clarification. While EACMS, PACS, and PCAS are not required by the current standard it is something that is implied to be required to satisfy the other standards.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy agrees with the scope of the SAR and has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 10, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
The NPCC RSC requests that an attachment be added to CIP-002 to support the identification and categorization of CIP-applicable systems (EACMS, PACS, and PCAs).	
Likes 0	
Dislikes 0	
Response	
Josh Schumacher - Black Hills Corporation - 1,3,5,6, Group Name Black Hills Corporation Segments 1, 3, 5, 6	
Answer	Yes
Document Name	
Comment	

Black Hills Corporation is in agreement with EEI's Comments:

While EEI appreciates rolling up noncompliance under a single standard to streamline tracking and reduce administrative burden, we note that regardless of the tracking mechanism, entities are obligated to address all noncompliance associated with failure to identify EACMS, PACS and PCA. As noted in the SAR, this includes reviewing and assessing the asset against the 28 requirements applicable to EACMS (87 sub requirements), 22 requirements applicable to PACS (63 sub requirements), or 14 requirements applicable to PCA (49 sub requirements) in all instances of potential noncompliance associated with misidentification or failure to identify or classify an asset. Further, entities implement mitigations to address the risks identified.

EEI suggests that the drafting team consider multiple options for these revisions including requirements for a process for identifying EACMS, PACS and PCAs, or a requirement for developing and maintaining a discrete list. Additionally, as technology evolves and projects like Project 2023-09 Risk Management for Third-Party Cloud Services progress, asset classifications may be added, removed, or changed. Further, requirements for a discrete list moves CIP-002 away from a Risk-Based standard to one that is a zero-defect standard which does little to improve BES Reliability, while creating significant compliance burden and risk for responsible entities.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1,3, Group Name Exelon

Answer	Yes
Document Name	

Comment

Exelon is aligning with the EEI in response to this question.

Likes 0	
Dislikes 0	

Response

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

Answer	Yes
Document Name	

Comment

While EEI appreciates rolling up noncompliances under a single standard to streamline tracking and reduce administrative burden, we note that regardless of the tracking mechanism, entities are obligated to address all noncompliance associated with failure to identify EACMS, PACS and PCA. As noted in the SAR, this includes reviewing and assessing the asset against the 28 requirements applicable to EACMS (87 sub requirements), 22 requirements applicable to PACS (63 sub requirements), or 14 requirements applicable to PCA (49 sub requirements) in all instances of potential

noncompliance associated with misidentification or failure to identify or classify an asset. Further, entities implement mitigations to address the risks identified.

EEI suggests that the drafting team consider multiple options for these revisions including requirements for a process for identifying EACMS, PACS and PCAs, or a requirement for developing and maintaining a discrete list. Additionally, as technology evolves and projects like Project 2023-09 Risk Management for Third-Party Cloud Services progress, asset classifications may be added, removed or changed. Further, requirements for a discrete list moves CIP-002 away from a Risk-Based standard to one that is a zero-defect standard which does little to improve BES Reliability, while creating significant compliance burden and risk for responsible entities.

Likes 0	
Dislikes 0	

Response

Amy Key - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	Yes
Document Name	

Comment

We support the scope and objectives of the SAR

Likes 0	
Dislikes 0	

Response

Jessica Cordero - Unisource - Tucson Electric Power Co. - 1

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Jeremy Cannon - Intermountain REA - NA - Not Applicable - WECC

Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Steven Belle - Dominion - Dominion Virginia Power - 1,3, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
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	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - PJM Interconnection, L.L.C. - 2 - RF, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	

Likes 0	
Dislikes 0	
Response	
Devon Tremont - Utility Services, Inc. - 4 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	

2. Do you believe that CIP-002 is the right standard to address the goals of the SAR? If not, please provide the standard recommendation and explanation.

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

Answer	No
Document Name	

Comment

ITC supports the comments submitted by EEI

Likes 0	
Dislikes 0	

Response

Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC

Answer	No
Document Name	

Comment

Having an additional requirement to generate a discrete list of EACMS and PCAs may be better identified under CIP-005 than CIP-002 because the methodology/evaluation to determine EACMS and PCA is done under CIP-005. There is already an implicit need to generate this list in order to properly apply all the relevant controls in this section. Keeping this together would minimize the overlap required between individual standards.

PACS may be better identified under CIP-006 than CIP-002 because the methodology/evaluation to determine PACS is under CIP-006. In addition, CIP-006 R3 already calls for 24-month testing of PACS and may be better suited to have identification of PACS.

Likes 0	
Dislikes 0	

Response

Erik Gustafson - TXNM Energy - 1,3 - WECC,Texas RE

Answer	No
Document Name	

Comment

As TXNM does not agree with the scope and objective of the SAR, it is voting no on question 2.

Likes 0	

Dislikes 0	
Response	
Robert Brown - AEP - 1,3,5,6 - MRO,Texas RE,RF	
Answer	No
Document Name	
Comment	
AEP believes that EACMS, PACS, and PCAs may be applicable across multiple standards, and drafting teams should take this into account moving forward. Additionally, AEP feels that this will not affect the 15-minute impact assessment on the BES when determining if the function (software/hardware) should fall under CIP 002 requirements. AEP feels this could be a bigger change to multiple CIP Standards and that it would not only impact CIP-002.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	No
Document Name	
Comment	
CIP-002 may be the appropriate place for an eventual identification requirement, but the question is of a more strategic nature – WHAT should it be identifying? This may be a far more definitional issue than a simple CIP-002 requirement.	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	No
Document Name	
Comment	
AZPS agrees with comments submitted by EEI on behalf of its members that the drafting team should be allowed to modify the Standard(s) that they determine are the most efficient options for addressing the risk documented in the SAR.	

Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	No
Document Name	
Comment	

It is Constellation’s stance that the identification and classification of PACS, EACMS, and PCAs should be done under the Standards where they are addressed:

PACS are addressed in CIP-006, PCAs are addressed in CIP-005, and EACMS are addressed in both CIP-007 and CIP-005.

Constellation recommends an additional requirement to include their identification and classification be included in those Standards. This addition will facilitate the reporting of any potential noncompliance under the appropriate Standards.

Alison Mackellar on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 5,6	
Answer	No
Document Name	
Comment	

It is Constellation’s stance that the identification and classification of PACS, EACMS, and PCAs should be done under the Standards where they are addressed: PACS are addressed in CIP-006, PCAs are addressed in CIP-005, and EACMS are addressed in both CIP-007 and CIP-005. Constellation recommends an additional requirement to include their identification and classification be included in those Standards. This addition will facilitate the reporting of any potential noncompliance under the appropriate Standards.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	
Response	

Patrick Wells - OGE Energy - Oklahoma Gas and Electric Co. - 1,3,5,6	
Answer	No
Document Name	Project 2021-03 CIP-002 Comment_Form.docx
Comment	
Likes 0	
Dislikes 0	
Response	
Amy Key - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	Yes
Document Name	
Comment	
We support the MRO NERC Standards Review Forum comments	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
CIP-002 is one of many Standards that the drafting team may choose to consider when drafting these revisions. EEI suggests that there may be alternatives to consider such as CIP-003, especially if the drafting team chooses an approach that focuses on a process. Additionally, the drafting team may want to consider revisions to CIP-005 – to identify EACMS & PCA and CIP-006 – to identify PACS. EEI suggests revising the SAR to allow the drafting team to modify the Standard(s) that they determine are the most efficient options for addressing the risk documented in the SAR.	
Likes 0	
Dislikes 0	
Response	

Daniel Gacek - Exelon - 1,3, Group Name Exelon	
Answer	Yes
Document Name	
Comment	
Exelon is aligning with the EEI in response to this question.	
Likes 0	
Dislikes 0	
Response	
Josh Schumacher - Black Hills Corporation - 1,3,5,6, Group Name Black Hills Corporation Segments 1, 3, 5, 6	
Answer	Yes
Document Name	
Comment	
Black Hills Corporation is in agreement with EEI's Comments: CIP-002 is one of many Standards that the drafting team may choose to consider when drafting these revisions. EEI suggests that there may be alternatives to consider such as CIP-003, especially if the drafting team chooses an approach that focuses on a process. Additionally, the drafting team may want to consider revisions to CIP-005 – to identify EACMS & PCA and CIP-006 – to identify PACS. EEI suggests revising the SAR to allow the drafting team to modify the Standard(s) that they determine are the most efficient options for addressing the risk documented in the SAR.	
Likes 0	
Dislikes 0	
Response	
Ruida Shu - Northeast Power Coordinating Council - 10, Group Name NPCC RSC	
Answer	Yes
Document Name	
Comment	
The NPCC RSC expects a process or methodology to be developed by the project, rather than a repetition of the definitions for EACMS, PACS, and PCAs. The SAR should also address the relationship between the retired reference models in CIP-003.	
Likes 0	
Dislikes 0	
Response	

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	Yes
Document Name	
Comment	
FirstEnergy supports EEI's comments which state: CIP-002 is one of many Standards that the drafting team may choose to consider when drafting these revisions. EEI suggests that there may be alternatives to consider such as CIP-003, especially if the drafting team chooses an approach that focuses on a process. Additionally, the drafting team may want to consider revisions to CIP-005 – to identify EACMS & PCA and CIP-006 – to identify PACS. EEI suggests revising the SAR to allow the drafting team to modify the Standard(s) that they determine are the most efficient options for addressing the risk documented in the SAR.	
Likes 0	
Dislikes 0	
Response	
Timothy Singh - Salt River Project - 1,3,5,6 - WECC	
Answer	Yes
Document Name	
Comment	
SRP believes this is the correct standard to address the goals of the SAR.	
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 for quesiton #2.	
Likes 0	
Dislikes 0	

Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	Yes
Document Name	
Comment	
Since CIP-002 sets the population of BES Facilities and BES Cyber Systems, (BCS) CIP-002 offers a centralized place to capture the Cyber Asset-level classification and ATC is supportive of this approach given this is the Standard that calls for a methodology to identify and categorize BCS. That said, ATC could also support a distributed approach through modification to CIP-002 to add a BES Cyber Asset (BCA) classification requirement; modifications to CIP-005 to add classification requirements for Electronic Access Control or Monitoring Systems (EACMS), Protected Cyber Assets (PCA), and Shared Cyber Infrastructure (SCI); and modifications to CIP-006 to add a classification requirement for Physical Access Control Systems (PACS).	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Western Power Pool - 4	
Answer	Yes
Document Name	
Comment	
We agree that CIP-002 is currently the right standard, but we would prefer a separate standard that is focused specifically on EACMS, PACS and PCAs. This woud be a cleaner solution once the BES Cyber Systems and associated Cyber Assets are identified, then the appropriate EACMS, PACS and PCAs can be focused on. By using CIP-002 there may be other systems identified not associated with protected cyber systems and assets that could be inadvertantly included in the CIP-002 assessment.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	Yes
Document Name	
Comment	

Duke Energy agrees that CIP-002 is likely the appropriate standard to address the intended objective but supports EEI's recommendations to modify the SAR, allowing the Drafting Team greater flexibility in determining where to implement revisions.	
Likes 0	
Dislikes 0	
Response	
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5	
Answer	Yes
Document Name	
Comment	
TFIST is expecting a process or methodology from the project and not a repeat of the EACMS, PACs, and PCAs definitions. The SAR should account for the relationship between the retired reference models in CIP-003.	
Likes 0	
Dislikes 0	
Response	
Lucinda Bradshaw - Oncor Electric Delivery - 1 - Texas RE	
Answer	Yes
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC	
Answer	Yes
Document Name	
Comment	

HQ supports the following NPCC TFIST comment:

TFIST is expecting a process or methodology from the project and not a repeat of the EACMS, PACs, and PCAs definitions. The SAR should account for the relationship between the retired reference models in CIP-003.

Likes 0	
Dislikes 0	

Response

Kennedy Meier - Electric Reliability Council of Texas, Inc. - 2

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

TRACEY JOHNSON - Southern Indiana Gas and Electric Co. - 1,3,5,6 - RF

Answer	Yes
Document Name	

Comment

Likes 0	
Dislikes 0	

Response

Lan Nguyen - CenterPoint Energy Houston Electric, LLC - 1 - Texas RE

Answer	Yes
Document Name	

Comment

Likes 0	

Dislikes 0	
Response	
Devon Tremont - Utility Services, Inc. - 4 - NA - Not Applicable	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Nick Leathers - Ameren - Ameren Services - 1,3,5,6 - MRO,SERC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - PJM Interconnection, L.L.C. - 2 - RF, Group Name ISO/RTO Standards Review Committee	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC	
Answer	Yes

Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Dwanique Spiller - Berkshire Hathaway - NV Energy - 5	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	

Response	
Steven Belle - Dominion - Dominion Virginia Power - 1,3, Group Name Dominion	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
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	
Jeremy Cannon - Intermountain REA - NA - Not Applicable - WECC	
Answer	Yes
Document Name	

Comment	
Likes 0	
Dislikes 0	
Response	
James Keele - Entergy - 1,3,6	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Jessica Cordero - Unisource - Tucson Electric Power Co. - 1	
Answer	Yes
Document Name	
Comment	
Likes 0	
Dislikes 0	
Response	
Randy Peters - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	
Document Name	
Comment	
Yes.	
Likes 0	
Dislikes 0	

Response

3. The cost impacts to address the objections of the SAR are unknown. What are the cost aspects associated with addressing the objections of the SAR? Please provide your explanation.

Randy Peters - Manitoba Hydro - 1,3,5,6 - MRO

Answer	
Document Name	

Comment

There are no significant costs to the SAR as it aims to take requirements that are currently captured in the NERC “Glossary of Terms” and bring these formally into the CIP-002 standard.

Likes 0	
Dislikes 0	

Response

Kimberly Turco - Constellation - 5,6

Answer	
Document Name	

Comment

Constellation has no comments.

Kimberly Turco on behalf of Constellation Segments 5 and 6

Likes 0	
Dislikes 0	

Response

James Keele - Entergy - 1,3,6

Answer	
Document Name	

Comment

The cost could be minimal if the requirement is for only Medium and High Impact BCS but could be costly if they include low BCS.

Likes 0	

Dislikes 0	
Response	
Anna Martinson - MRO - 1,2,3,4,5,6 - MRO, Group Name MRO Group	
Answer	
Document Name	
Comment	
The MRO NSRF declines to answer this question as its intent is unclear. Is the SDT truly asking for the cost impacts of “objections of the SAR” or was this intended to read “objectives of the SAR”.	
Likes 0	
Dislikes 0	
Response	
Lucinda Bradshaw - Oncor Electric Delivery - 1 - Texas RE	
Answer	
Document Name	
Comment	
Oncor has no objection to this SAR moving forward and currently expects only minimal cost impacts from addressing the objectives of this SAR.	
Likes 0	
Dislikes 0	
Response	
Rebika Yitna - MEAG Power - 1,3 - SERC	
Answer	
Document Name	
Comment	
It cannot be determined at this time what the cost impacts would be to address the objectives of this SAR.	
Likes 0	
Dislikes 0	
Response	

Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy does not have any additional feedback to provide regarding cost.	
Likes 0	
Dislikes 0	
Response	
Kevin Conway - Western Power Pool - 4	
Answer	
Document Name	
Comment	
No, cost impacts would be limited to the administration of the change in standards by the compliance departments. SMEs should be currently identifying and assessing the EACMS, PACS, and PCAs.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	
Document Name	
Comment	
Constellation has no comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	

Amy Wilke - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
This would be soft costs, such as hours and administrative overhead.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
n/a	
Likes 0	
Dislikes 0	
Response	
Robert Brown - AEP - 1,3,5,6 - MRO,Texas RE,RF	
Answer	
Document Name	
Comment	
There is an overall reduction in time, but it is more pronounced concerning CIP-002. This appears to raise more of a risk-related question. Additionally, for AEP, there are implications for various Internal tools.	
Likes 0	
Dislikes 0	
Response	
Erik Gustafson - TXNM Energy - 1,3 - WECC,Texas RE	

Answer	
Document Name	
Comment	
N/A	
Likes 0	
Dislikes 0	
Response	
Elizabeth Davis - PJM Interconnection, L.L.C. - 2 - RF, Group Name ISO/RTO Standards Review Committee	
Answer	
Document Name	
Comment	
The ISO/RTO Council (IRC) Standards Review Committee (SRC) is unaware of any significant incremental costs associated with addressing the objectives of the SAR.	
Likes 0	
Dislikes 0	
Response	
Timothy Singh - Salt River Project - 1,3,5,6 - WECC	
Answer	
Document Name	
Comment	
SRP mostly believes there is minimal to no cost impact to addressing this SAR, as many classify all of their CIP assets in the scope of CIP-002 already through the use of the BROS. Some believe there would be a significant cost impact with the inclusion of PCAs, as they believe additional time and resources would be needed to sufficiently include PCAs they own on their CIP-002 CA classification list.	
Likes 0	
Dislikes 0	
Response	
Nick Leathers - Ameren - Ameren Services - 1,3,5,6 - MRO,SERC	

Answer	
Document Name	
Comment	
Ameren does not foresee any cost impacts for this standard. We already review and categorize these devices. This would most likely just require a simple change to the procedure.	
Likes 0	
Dislikes 0	
Response	
Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter	
Answer	
Document Name	
Comment	
FirstEnergy has no additional comments.	
Likes 0	
Dislikes 0	
Response	
Josh Schumacher - Black Hills Corporation - 1,3,5,6, Group Name Black Hills Corporation Segments 1, 3, 5, 6	
Answer	
Document Name	
Comment	
Black Hills Corporation will not comment on cost.	
Likes 0	
Dislikes 0	
Response	
Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC	
Answer	
Document Name	

Comment	
It is not clear if there will be any cost impact to us without knowing the details of the proposed standard.	
Likes 0	
Dislikes 0	
Response	
Gail Elliott - International Transmission Company Holdings Corporation - NA - Not Applicable - MRO,RF	
Answer	
Document Name	
Comment	
ITC supports the comments 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 ISO/RTO Council (IRC) Standards Review Committee (SRC) for this question and adopts them as its own.	
Likes 0	
Dislikes 0	
Response	
Kristine Martz - Edison Electric Institute - NA - Not Applicable - NA - Not Applicable	
Answer	
Document Name	
Comment	

EEI does not comment on cost.	
Likes 0	
Dislikes 0	
Response	
Amy Key - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3	
Answer	
Document Name	
Comment	
We support the MRO NERC Standards Review Forum position on this item	
Likes 0	
Dislikes 0	
Response	

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

Amy Key - Berkshire Hathaway Energy - MidAmerican Energy Co. - 1,3

Answer	
Document Name	

Comment

We support the MRO NERC Standards Review Forum comments

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

On th SAR Form, there is no box checked under “Justification for this proprosed standard development project.” Please check all that apply.

Standard revisions to address this SAR will require industry resources at a time when there are multiple ongoing high (6), medium (5), and low (8) priority projects, and it will be the fourth SAR assigned to a single drafting team. Due to the administrative nature of the revisions, EEI asks the NERC and the Standards Committee to consider making this a low priority project to allow the Project 2021-03 drafting team to complete other SARs already assigned.

Additionally, it is not clear from the SAR if alternatives to Standards revisions have been considered including adjustments to noncompliance tracking systems, tools, or mechanisms to achieve similar outcomes as those sought in the SAR which may provide a more expedient resolution for industry and regulators alike.

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 for this question and adopts them as its own.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

ITC supports the comments submitted by EEI

Likes 0	
Dislikes 0	

Response

Ijad Dewan - Hydro One Networks, Inc. - 1 - NPCC

Answer	
Document Name	

Comment

Given the standards meant to be security focused, is there a benefit in rolling up violations under just one standard? Modifying a CIP-002 should have a security benefit to electricity infrastructure and as such the identification of EACMS, PCAs and PACS may be better identified in other CIP Standards if required. If roll-ups are allowed, it needs to be formalized in the standard to provide the same guidance to all auditors to leave no room for doubts on the legitimacy of rolling up violation requirements.

Likes 0	
Dislikes 0	

Response

Daniel Gacek - Exelon - 1,3, Group Name Exelon

Answer	
Document Name	

Comment

Exelon is aligning with the EEI in response to this question.

Likes 0	
Dislikes 0	

Response

Devon Tremont - Utility Services, Inc. - 4 - NA - Not Applicable

Answer	
Document Name	

Comment

Utility Services believes that there should be clarification or guidance provided that the intent to "roll up" these violations into a single CIP-002 violation will maintain the same process that currently exists for rolling these up to CIP-010 R1. We are hearing concerns that while the idenfication of EACMS/PACS/PCAs will now be formalized into CIP-002 (if this SAR continues), that NOT formalizing the process of "rolling up" these violations into a single violation might be shortsighted and and may not completely solve the problem.

Likes 0	
Dislikes 0	

Response

Josh Schumacher - Black Hills Corporation - 1,3,5,6, Group Name Black Hills Corporation Segments 1, 3, 5, 6

Answer	
Document Name	

Comment

Black Hills Corporation is in agreement with EEI’s Comments:

On the SAR Form, there is no box checked under “Justification for this proposed standard development project.” Please check all that apply.

Standard revisions to address this SAR will require industry resources at a time when there are multiple ongoing high (6), medium (5), and low (8) priority projects, and it will be the fourth SAR assigned to a single drafting team. Due to the administrative nature of the revisions, EEI asks NERC and the Standards Committee to consider making this a low priority project to allow the Project 2021-03 drafting team to complete other SARs already assigned.

Additionally, it is not clear from the SAR if alternatives to Standards revisions have been considered. Including adjustments to noncompliance tracking systems, tools, or mechanisms to achieve similar outcomes as those sought in the SAR which may provide a more expedient resolution for industry and regulators alike.

Likes 0	
Dislikes 0	

Response

Ruida Shu - Northeast Power Coordinating Council - 10, Group Name NPCC RSC

Answer	
Document Name	

Comment
The NPCC RSC agrees with the short-term goals of the SAR but expects that a long-term solution for updating the standards may require a comprehensive revision in the future. We believe that the glossary of terms should not be altered. We also believe that there should be a process component, not just the creation of an inventory. The SDT should consider scenarios involving mixed-trust environments and layered devices that perform monitoring functions—for example, the categorization of an Intermediate System supporting an IRA.

Likes 0	
Dislikes 0	

Response

Mark Garza - FirstEnergy - FirstEnergy Corporation - 1,3,4,5,6, Group Name FE Voter

Answer	
Document Name	

Comment
On the SAR Form, there is no box checked under “Justification for this proposed standard development project.” Please check all that apply.

Likes 0	
Dislikes 0	

Response

Elizabeth Davis - PJM Interconnection, L.L.C. - 2 - RF, Group Name ISO/RTO Standards Review Committee

Answer	
Document Name	

Comment
This SAR proposes appropriate and much-needed improvements in CIP-002. The industry should strive to implement more objective-focused and efficient standards to support secure operation of the BES. This SAR supports that goal by leveraging CIP-002 to address categorization, tracking, and reporting the entire set of cyber assets associated with CIP standards instead of the current subset of HIGH, MEDIUM, and LOW impact BCS.

The IRC SRC believes it is important to ensure the drafting team provides clear guidance regarding the kind of evidence that will be needed for the CIP-002 annual review under the revisions proposed in this SAR (e.g., would entities need to conduct a full accounting/category review for each EACMS, PACS, and PCA every year?).

CIP-002 has long been the foundational standard of all CIP Standards. To appropriately apply all CIP-required protections, an entity must first implement CIP-002. The purpose of CIP-002-5.1a is *"to identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES."*

Even though BES Cyber Assets are not included in the actual Requirement R1 language, the NERC definition of BES Cyber Systems ("one or more BES Cyber Assets . . .") indicates that BES Cyber Assets are inherently included within the requirement. However, this logic does not apply to

EACMS, PACS, or PCAs. In past versions of the CIP Reliability Standards, the NERC-defined term Critical Cyber Assets was used as an all-encompassing defined term to identify all Cyber Assets essential to the reliable operation of Critical Assets. This term was retired during the v5 transition in 2016, leaving a gap in requirement language for identifying EACMS, PACS, and PCAs associated with BES Cyber Systems. In its place is an implied requirement, as entities must identify these Cyber Assets to be compliant with other CIP Reliability Standards. Entities have relied on the definitions within the NERC Glossary of Terms to mold their CIP-002 programs for identifying these Cyber Assets, which has resulted in inconsistent understanding and application of these terms across the industry. Without explicit requirements for identifying these Cyber Assets, it is difficult to ensure these Cyber Assets are identified consistently across the industry, which ultimately increases the risk of vulnerabilities remaining unaddressed and adversely impacting the BES.

Additionally, these misalignments and misunderstandings are not confined to EACMS, PACS, and PCAs. There are other NERC-defined types of systems or devices with implied identification requirements, such as EAPs, ESPs, PSPs, Intermediate Systems, BCSI storage locations, and TCAs, along with the implied requirement in Attachment 1, Criterion 2.3 for Planning Coordinators and Transmission Planners to designate generation Facilities as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year. Failure to properly and consistently identify these types of assets, systems, or Facilities will also lead to downstream compliance issues. The drafting team should seek to minimize the use of these types of implied identification requirements and should provide updated technical guidance to aid entities in identifying these systems or devices, as the currently available guidance is located in the Background section of CIP-002-5.1a, Lessons Learned documents, ERO-endorsed guidance, and other outreach documents, all of which are non-enforceable, outdated, and will not be highly useful in implementing the changes proposed in Project 2016-02, *Modifications to CIP Standards*, that introduce new NERC-defined terms such as Virtual Cyber Asset and Shared Cyber Infrastructure.

Explicit standard language brings uniformity to application and enforcement, but quality application guidance is also important, especially now that systems are far more complex than they were in 2016 when CIP-002-5.1a became effective. The IRC SRC recommends that the drafting team consider the changes made within project 2016-02, *Modifications to CIP Standards*, along with the revisions underway in project 2023-09, *Risk Management for Third-Party Cloud Services*, to find a balance between explicit requirement language and associated implementation guidance.

Likes 0	
Dislikes 0	

Response

Erik Gustafson - TXNM Energy - 1,3 - WECC,Texas RE

Answer	
Document Name	

Comment

If this SAR passes, TXNM requests that the changes to CIP-002 succinctly reflect the intended outcome of the SAR without bringing in unintended or unnecessary effects. The change in language could be simply stated, as an example:

R1.1. Identify each of the high impact BES Cyber Systems (and their associated EACMS, PACS, and PCA) according to Attachment 1, Section 1, if any, at each asset;

R1.2. Identify each of the medium impact BES Cyber Systems (and their associated EACMS, PACS, and PCA) according to Attachment 1, Section 2, if any, at each asset;

Or the drafting team could consider a requirement for a process to identify the associated Cyber Assets.

Likes 0	
Dislikes 0	

Response

Ronald Hoover - Bonneville Power Administration - 1,3,5,6 - WECC

Answer	
Document Name	

Comment

BPA appreciates the opportunity to comment. Generally speaking, BPA is supportive of the SAR for project 2021-03 regarding CIP-002. BPA looks forward to working with the drafting team to complete the project.

Likes 0	
Dislikes 0	

Response

Robert Brown - AEP - 1,3,5,6 - MRO,Texas RE,RF

Answer	
Document Name	

Comment

AEP Has no additional comments.

Likes 0	
Dislikes 0	

Response

Mia Wilson - Southwest Power Pool, Inc. (RTO) - 2 - MRO,WECC	
Answer	
Document Name	
Comment	
Southwest Power Pool (SPP) endorses the response submitted by the SRC for this question.	
Likes 0	
Dislikes 0	
Response	
Jennifer Tidwell - Southern Company - Southern Company Services, Inc. - 1,3,5,6 - SERC, Group Name Southern Company	
Answer	
Document Name	
Comment	
n/a	
Likes 0	
Dislikes 0	
Response	
Andrew Smith - APS - Arizona Public Service Co. - 1,3,5,6	
Answer	
Document Name	
Comment	
AZPS agrees with comments submitted by EEI on behalf of its members that due to multiple ongoing projects the Standards Committee considers this to be a low priority project to allow the Project 2021-03 drafting team to complete other SARs already assigned. AZPS also agrees with EEI's comments that it is unclear whether alternatives to Standard revisions are being considered to include adjustments to the noncompliance tracking system (Align), tools, or mechanisms to achieve similar outcomes which may provide a more expedient resolution for industry and regulators. Changes to the reporting system may allow a streamlined approach, for example an option to submit a report for a missed asset category rather than the single option of selecting one requirement.	
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 for quesiton #4.	
Likes 0	
Dislikes 0	
Response	
Amy Wilke - American Transmission Company, LLC - 1	
Answer	
Document Name	
Comment	
ATC requests the SDT take a risk-based approach to the incorporation of this requirement to assure the VRF is right-sized, the requirement language is written so as not to force binary VSLs with zero tolerance, and takes into consideration factors such as 1) volume of errors in classification, 2) the type of Cyber Asset, as well as 3) documentation only errors vs the true absence of implemented security controls. As some examples: 1) Failure to identify, classify, and apply protections to one BCA poses less risk than a failure to identify, classify, and apply protections to ten BCAs; 2) Failure to identify, classify, and apply protections to one PCA poses less risk than failure to identify, classify, and apply protections to one BCA; 3) Failure to properly document the identification and classification of one BCA (administrative error only) poses less risk than the failure to identify, classify, and apply protections to one BCA.	
Likes 0	
Dislikes 0	
Response	
Alison MacKellar - Constellation - 5,6	
Answer	
Document Name	
Comment	
Constellation has no additional comments. Alison Mackellar on behalf of Constellation Segments 5 and 6	

Likes 0	
Dislikes 0	
Response	
Kevin Conway - Western Power Pool - 4	
Answer	
Document Name	
Comment	
Consideration needs to be given to low impact systems and how EACMS, PACS, and PCAs should be protected for these assets.	
Likes 0	
Dislikes 0	
Response	
Rachel Coyne - Texas Reliability Entity, Inc. - 10	
Answer	
Document Name	
Comment	
Texas RE supports the purpose and scope of this SAR.	
Likes 0	
Dislikes 0	
Response	
Ellese Murphy - Duke Energy - 1,3,5,6 - Texas RE,SERC,RF	
Answer	
Document Name	
Comment	
Duke Energy does not have any additional comments for the Drafting Team. Thank you for considering our comments.	
Likes 0	
Dislikes 0	

Response
Rebika Yitna - MEAG Power - 1,3 - SERC
Answer
Document Name
Comment
No additional comments
Likes 0
Dislikes 0
Response
Junji Yamaguchi - Hydro-Quebec (HQ) - 1,5
Answer
Document Name
Comment
TFIST agrees with the short-term goals of the SAR but, expects that the long term solution to updating the standards may need a comprehensive revision in the future. TFIST believes that the glossary of terms should not be altered. TFIST believes that there should be a process component and not just the creation of an inventory. The SDT should consider situations of mix trust environments and layers of devices that perform monitoring functions. For example, categorization of an Intermediate System supporting IRA.
Likes 0
Dislikes 0
Response
Lucinda Bradshaw - Oncor Electric Delivery - 1 - Texas RE
Answer
Document Name
Comment
None

Likes 0	
Dislikes 0	

Response

Chantal Mazza - Hydro-Quebec (HQ) - 1 - NPCC

Answer	
Document Name	

Comment

HQ supports the following TFIST comments:

- TFIST agrees with the short-term goals of the SAR but, expects that the long term solution to updating the standards may need a comprehensive revision in the future.
- TFIST believes that the glossary of terms should not be altered.
- TFIST believes that there should be a process component and not just the creation of an inventory.
- The SDT should consider situations of mix trust environments and layers of devices that perform monitoring functions. For example, categorization of an Intermediate System supporting IRA.

Likes 0	
Dislikes 0	

Response

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

Answer	
Document Name	

Comment

The Project 2021-03 webpage lists four items that Phase Two of this project is intended to address. However, this SAR only appears to address one issue from that list (#4): “Modifications to CIP-002 Identification - This SAR seeks to centralize the identification of Protected Cyber Assets (PCA), Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS) as “CIP applicable" systems in a single standard.” The MRO NSRF would appreciate clarification that this is intentional and that the full scope of this SAR is just to address this individual item.

The MRO NSRF, while supporting the objectives and scope of the SAR, does not support NERC Staff using the section of the SAR reserved for explaining the risk/benefit to the BES to forecast negative consequences to industry (in the form of the ERO significantly increasing the number of violations issued) if the SAR and associated eventual revisions to CIP-002 fail to advance.

Likes 0	
Dislikes 0	

Response

Jeremy Cannon - Intermountain REA - NA - Not Applicable - WECC	
Answer	
Document Name	
Comment	
CORE agrees with the scope and objectives of this SAR as it provides better clarity and improved categorization of BES cyber systems, however, it would be helpful to provide a clearer definition of “contiguous Elements” in Attachment 1 – Impact Rating Criteria, section 2.12. Please provide examples of demarcation lines of Elements that are not contiguous. System diagrams of contiguous and non-contiguous Elements would help provide clarity to ensure we understand the scope of this exclusion.	
Likes 0	
Dislikes 0	
Response	
Kimberly Turco - Constellation - 5,6	
Answer	
Document Name	
Comment	
Constellation has no additional comments. Kimberly Turco on behalf of Constellation Segments 5 and 6	
Likes 0	
Dislikes 0	
Response	
Randy Peters - Manitoba Hydro - 1,3,5,6 - MRO	
Answer	
Document Name	
Comment	
The current CIP-002 does not require an annual review of EACMS, PACS or PCA. To address any concerns over the cost of the change, the drafting team can aim to retain this state. This allows industry to perform an annual review as an internal control without the administrative burden of audit reporting.	
Likes 0	
Dislikes 0	

Response