NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Summary Response to Comments

Project 2021-03 CIP-002 | Standard Authorization Request

Project Background

NERC Project 2021-03 CIP-002 currently has five assigned Standard Authorization Requests (SARs). The response to comments is based on the below SARs:

1. CIP-002-5.1a and CIP-014-2 – This SAR provides revisions to CIP-002 and CIP-014 to clarify the responsibility of Reliability Coordinators, Planning Coordinators, and Transmission Planners in identifying Facilities that warrant consideration under these Reliability Standards. As it relates to the Transmission Planner and Planning Coordinator functions, the language "critical to the derivation of Interconnection Reliability Operating Limits (IROLs)" should be replaced/updated to appropriately identify Facilities that, if somehow compromised, could significantly impact the reliability of the Bulk Electric System (BES). Additionally, this SAR includes a review of the applicability of Facilities identified by the Reliability Coordinator as critical to the derivation of IROLs to CIP-002 and CIP-014. The SC accepted this SAR on July 21, 2021.
2. Modifications to CIP-002 – This SAR seeks to revise CIP-002 to include identification and categorization of certain Cyber Assets (Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets) associated with high and medium impact BES Cyber Systems. The SC accepted this SAR on November 17, 2021.

Based on SAR additions and comments received, the project title has been updated to state "CIP-002" instead of "CIP-002 Transmission Owner Control Center."

SAR Posting

The "Modifications to CIP-002" and "CIP-002-5.1a and CIP-014-2" SARs were posted November 22 through December 21, 2022 for a 30-day informal comment period. All drafting team (DT) responses to the comments are outlined below.

Question 1: Do you agree with the proposed scope as described in the CIP-002 and CIP-014 SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

Industry Comment:

A commenter requested the DT provide clarification to the proposed SAR clarifying if this IROL is for identifying sites or systems? It was also recommended that the scope include IROLs that are shared among entities.

Drafting Team Response:
Thank you for your comment. This project provides revisions to CIP-002 and CIP-014 to clarify the responsibility of Reliability Coordinators, Planning Coordinators, and Transmission Planners in identifying Facilities that warrant consideration under these Reliability Standards. Identifying Facilities is not synonymous with identifying sites. NERC defines a Facility as "A set of electrical equipment that operates as a single BES Element (e.g., a line, a generator, a shunt compensator, transformer, etc.). The DT will look at additional information regarding Facilities and systems.

The DT will take into consideration the changes made to FAC-014 by the Project 2015-09 DT, which initiated the modifications of IROLs.

Industry Comment:
A commenter shared concern that the CIP-002 and CIP-014 IROL SAR is outside the scope of the Planning Coordinator (PC), Transmission Planner (TP), and Reliability Coordinator (RC), and "If Facilities are not being considered in the applicability section of the standard, [then] that should be addressed first. Interconnections which are the responsibility of the owners drives the inclusion in these standards, so the responsibility should be kept there. For the purpose of security owners to have the necessary information to assess the standards, the information necessary to assess does not sit with the PC, TP, or RC, nor should they. If issues exist with a facility and the location, the[n] it should be considered as a contingency and addressed in TPL-001."

Drafting Team Response:
Thank you for your comments, but the DT respectfully disagrees. The Facilities addressed by this SAR as of April 1, 2024, are determined by the RC consistent with FAC-014-3 requirements.

- For CIP-002, the SAR is to clarify the identification of assets integral for the development of IROL(s) and stability limits for elevating associated BES Cyber Systems from low impact to medium impact. Transmission Owners (TOs) do not have the responsibility for identifying IROL(s) or developing stability limits. Entities must rely on communication from their RC to apply criterion 2.6 which determines if IROL(s) are within scope.
- For CIP-014, as of April 1, 2024, IROL(s) are determined by the RC based on the criteria in CIP-002.
- For TPL-001, the objective is to identify system improvements necessary to address certain contingencies within the planning horizon, not informing the owners of generation and transmission Facilities of IROL impacts.

Industry Comment:
A commenter mentioned that this SAR is too vague and not clear on what risk is being addressed. We find no need or added value for the proposed SAR.

Drafting Team Response:
Thank you for your comments, but the DT respectfully disagrees. The CIP-002 and CIP-014 SAR was developed based on industry comments that the Project 2015-09 SDT (Establish and Communicate SOLs) received when proposing changes to the CIP Standards that contain IROL. The main purpose of Project 2015-09 was to retire the planning based IROLs within the respective operating and planning (O&P)

Standards and the CIP Standards. While the team had success with the O&P Standards, industry did not fully agree with removing IROLs from the CIP Standards. To allow the Project 2015-09 SDT to close out their scope of work, a new SAR (2021-03 CIP-002 and CIP-014) was developed and submitted to address the CIP-related recommendation to have planned IROLs removed.

The detailed description of the SAR provides in-depth details that help clarify the purpose. Those items are listed below. Revisions to CIP-002 and CIP-014 to include:

1. Identifying Functional Entities that identify Facilities applicable to CIP-002 and CIP-014.
2. Identifying Functional Entities responsible for the communication of the identified Facilities.
3. Applicability sections to be reviewed and revised accordingly.
4. Determine the appropriate Facilities for application of the CIP standard and include due consideration for those planning events that result in System instability, Cascading, or uncontrolled separation as identified in the PC and TP's Planning Assessment for the Near-Term Transmission Planning Horizon.
5. Determine the appropriateness of the identification of Facilities critical to the derivation of IROLs by the RC.

Industry Comments:

Many commenters expressed lack of support the proposed scope for this SAR because it is unclear the reliability gap associated with RC, PC, and TP responsibilities in the identification of critical facilities associated with IROLs. While these registered entities are not identified in CIP-002 or CIP-014 directly, the establishment, identification, and communication of IROLs is already contained in other NERC O&P Reliability Standards. Specifically, during Project 2015-09 (Establish and Communicate System Operating Limits) these obligations were addressed. Adding redundant requirements in CIP-002 and CIP-014 would only add unnecessary and duplicative obligations on registered entities. It is also important to note that the modifications made under Project 2015-09 to address these issues went into effect on April 1, 2024. FAC-014-3, Requirement R5 requires RCs to provide information to PCs, TPs, GOs and TOs (see subparts 5.2 & 5.6) and sub-part R5.6 requires RCs to provide "Each impacted Generator Owner or Transmission Owner, within its Reliability Coordinator Area, with a list of their Facilities that have been identified as critical to the derivation of an IROL and its associated critical contingencies at least once every twelve calendar months." The concerns expressed in this SAR are unnecessary and would add language to CIP-002 and CIP-014 that would create duplicative Requirements in those Reliability Standards and necessitate adding FAC-014-3 to the project scope in order to make conforming changes to that Reliability Standard. For these reasons, we do not support the proposed SAR.

Drafting Team Response:

Thank you for your comments, but the DT respectfully disagrees. Project 2015-09 identified CIP-002 and CIP-014 for necessary revisions in conjunction with revisions to FAC-014-3 and did attempt to make progress by converging their work along with Project 2016-02. However, this work was pulled back to allow Project 2016-02 to complete the final ballot of CIP-002. This SAR picks up the unfinished objectives of Project 2015-09.

Question 2: Do you agree with the proposed scope as described in the modifications to CIP-002 SAR? If you do not agree, or if you agree but have comments or suggestions for the project scope, please provide your recommendation and explanation.

Industry Comment:

A couple of commenters stated: "We do not feel the scope of this SAR is correct for Transmission Owner Control Centers (TOCC). The proposed SAR modifications dilute the project. If NERC or Industry feels like there needs to be identification of PACS, EACMS, and PCA under CIP-002, then there should be a separate specific project not scope creep on this project. This project's background and purpose have nothing to do with PACS, EACMS or PCAs. Adding this to the SAR will certainly extend this project beyond the timeline established for this project which is not acceptable."

Drafting Team Response:

The SARs associated with this project are separately filed and will be handled by the DT and NERC in a manner that successfully addresses all items in scope for Project 2021-03.

The Standards Committee (SC) authorized the following SARs be assigned to the Project 2021-03 DT:

- 2016-02 (TOCC Part of the SAR[1])
- CIP-002 and CIP-014 IROL SAR
- CIP-002 (EACMS, PACS, and PCAs)
- CIP-002 Communications Protocol Converters SAR
- CIP-002-5.1a Criterion 1.3 Revision SAR

NERC solicited for additional nominations from May 23, 2022 – June 22, 2022, and from July 20, 2023 – August 18, 2023, to supplement the DT members to provide additional members in addressing the additional SARs assigned to this team. NERC staff split this project into Group A and Group B. All SARs are under the same project as assigned by the DT; however, the team members who are unable to participate in the additional SARs remain on Group A and all other DT members plus the additional DT members are on Group B. The new DT members are not in Group A as that SAR has confidentiality agreements, and the project was too far along to add those additional members to Group A. Below lists out the assignments of each SAR to the respective Group.

- Group A:
  - 2016-02 SAR (TOCC part of the SAR)
- Group B:

[1] Language pulled directly from the 2016-02 SAR that pertains to the TOCC portion that was assigned to Project 2021-03
• Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations –
V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:
• The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.
• The definition of Control Center.
• The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria.

- CIP-002 and CIP-014 (IROL)
- CIP-002 (EACMS, PACS, and PCA)
- CIP-002 Communications Protocol Converters SAR
- CIP-002-5.1a Criterion 1.3 Revision SAR

Lastly, to address any confusion on the name of the project, Project 2021-03 has been updated from "Project 2021-03 TOCC" to "Project 2021-03 CIP-002.

Industry Comment:

Many commenters supported the following: "it is unclear the reliability gap that this SAR intends to close. While it is clear that responsible entities under CIP-002 must identify BES Cyber Systems and their associated BES Cyber assets, the current standard does not implicitly require the development of a list of those assets. This is because lists do not guarantee assets are protected. Moreover, administratively, mistakes in documentation can happen even when affected assets have been identified and properly protected. Additionally, this SAR proposes to move 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 a significant compliance burden and risk for responsible entities.

It is also worth considering whether the formal development of discrete lists of Cyber Assets is a forward-looking approach that will last as technology evolves. While over the life of the CIP standards, electronic access control has and will continue to morph from dedicated Cyber Assets (i.e., a discrete HW firewall, a discrete HW domain controller server, etc.) to a function performed in ever more distributed ways. Zero Trust principles may affect access policies. Zero Trust could also result in thousands of logical ESPs around sessions, and thus thousands of EACMS. The concept of EACMS as a discrete 'Cyber Asset' that you can be put on a list will lose meaning over time, rendering a standard obsolete. The technology is headed to electronic access control being a highly distributed function enforced throughout the infrastructure, not a list of dedicated Cyber Assets.

It is also worth noting that virtualization is abstracting 'programmable electronic devices' into a generic hardware resource pool, on top of which many functions are implemented. It is our understanding that the Project 2016-02 SDT is working to incorporate into the PCA definition not only the sharing of a local network, but the sharing of a hypervisor's CPU and memory resources. This type of change will result in dynamic system operation, with a virtual machine becoming a PCA based on where it is executing at the moment. Such a scenario will make the development of discrete lists of categorized BES Cyber Assets nearly impossible, possibly rendering the proposed changes obsolete before the Reliability Standard ever become enforceable."

Drafting Team Response:

Thank you for your comments. The DT agrees that the SAR is unclear and proposed edits have been incorporated. Auditors addressing missed identification of EACMS, PACS, and PCAs have found it difficult to keep potential findings of non-compliance relegated to a single standard for each finding. The intent of the SAR is to address this in a single standard to handle each case where failure to identify and provide appropriate protections has occurred.

The DT agrees with your comment regarding static cyber assets versus distributed functions. The SAR has been revised away from "Cyber Asset" identification and is now focused on systems and protected cyber assets.

Industry Comment:

One commenter stated: "the creation of a discrete list of Cyber Asset for [EACMS, PACS, and PCA] is going to be more difficult as virtualization expands within the industry. This will be especially true for EACMS as the firewall and access point move from specific devices to potentially every Cyber Asset. The SAR should be modified to address these trends so it does not restrict what a drafting team can do to satisfy NERC's desire to make sure all BCS associated Cyber Assets are identified and appropriately protected."

Drafting Team Response:

Thank you for your comment. The SAR has been revised to reflect your comment in that focuses on the systems performing the protective objectives for EACMS, PACS, and PCAs and not the discrete cyber assets that's located in a single location.

Industry Comment:

Several commenters stated this gap should not be addressed in CIP-002 as it would be better addressed in other CIP standards. "The ESP and PSP concepts are not relevant for the assessment performed in regard to the CIP-002 standard, nor EACMS, PCA, and PACS. Bringing these types of cyber assets and concepts into the scope of CIP-002 brings an undesirable burden on demonstrating compliance with the CIP-002 standard and would require even more multidisciplinary expertise to perform the assessment.
This gap should be filled in CIP standards that already address these concepts and types of cyber assets.

Recommend including Glossary changes to support this SAR.

Please consider the identification of 1) assets in the cloud, and 2) third-party cyber assets.

Request use cases for cyber assets a) on-site entity owned, b) on-site third party owned, c) off-site entity owned and d) off-site third-party owned. And conforming changes in the rest of the CIP Standards.

Request addressing other CIP-002 gaps like the threshold for new assets which have no prior history. Some existing thresholds depend on the prior year's information."

Drafting Team Response:

Thank you for your comments. The DT considered expansion of scope to other CIP standards but agreed that CIP-002 was best suited to address the objectives of the SAR. Further, the SAR has been revised and reflects your comment that the focus is not the discrete cyber assets that's located in a single location but rather pertinent to systems performing the protective objectives for EACMS, PACS, PCAS. The SAR provides latitude for the DT to consider off-site/third party owned. Additionally, the DT will take into consideration your comment during standards drafting.

Industry Comment:

A couple of commenters stated: "if adding PACS, PCA, and EACMS to the scope of CIP-002 then those should be updated as a part of Project 2016-02 as there are new Cyber Assets coming into scope under that project or make this a project post [for] Project 2016-02 approval. Further if as an industry we add to CIP-002's scope, not making this change as a part of 2016-02 will require programmatic changes again in the near future for the new asset and sub asset types creating increased and unnecessary compliance burden."

Drafting Team Response:

Thank you for your comments, but the DT respectfully disagrees. The DT will keep this SAR as assigned by the Standards Committee and will take into consideration your comment during standards drafting.

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

Industry Comment:

A commenter asked is there a Standard Drafting Team that addresses the IROL question, recommend that SDT include expertise in 1) IROLs and 2) CIP. This posting is confusing. These two SARs are project 2021-03. We expected a new project (web) page. These two SARs are on the page for project 2016-02 which is CIP-002 Transmission Owner Control Centers (TOCC). Project 2016-02 appears to have an approved SAR for TOCC. The two SARs for project 2021-03 do not explicitly address TOCC. There is only one comment form for project 2021-03. How many SDTs are expected (1, 2 or 3)?

Drafting Team Response:

Thank you for your comment. This DT is not conducting an assessment on the appropriateness of the IROL determination, but merely whether or not an IROL determination has been made. If it has, then that result can impact the assessment for TOCC applicability. In that other standards would be the determining factor for the declaration of an IROL, we will rely on those DT teams to appropriately defined the application for such an operating limit. The revisions to CIP-002 and CIP-014 will clarify the responsibility of Reliability Coordinators, Planning Coordinators, and Transmission Planners in identifying Facilities that warrant consideration under these Reliability Standards.

The Standards Committee (SC) authorized the following SARs be assigned to the Project 2021-03 SDT:

- 2016-02 (TOCC Part of the SAR[2])
- CIP-002 and CIP-014 IROL SAR
- CIP-002 (EACMS, PACS, and PCAs)
- CIP-002 Communications Protocol Converters SAR

[2] Language pulled directly from the 2016-02 SAR that pertains to the TOCC portion that was assigned to Project 2021-03

• Transmission Owner (TO) Control Centers Performing Transmission Operator (TOP) Obligations –

V5TAG is aware of multiple interpretations of the language "used to perform the functional obligation of" in CIP-002-5.1 Attachment 1, section 2.12 and recommends clarification of:

• The applicability of requirements on a TO Control Center that performs the functional obligations of a TOP, particularly if the TO has the ability to operate switches, breakers and relays in the BES.

• The definition of Control Center.

• The language scope of "perform the functional obligations of" throughout the Attachment 1 criteria. •

- CIP-002-5.1a Criterion 1.3 Revision SAR

NERC solicited for additional nominations from May 23, 2022 – June 22, 2022, and from July 20, 2023 – August 18, 2023 to supplement the DT members to provide additional members in addressing the additional SARs assigned to this team.

Industry Comment:

One commenter stated that the Transmission Planner and Planning Coordinator should not get involved in the CIP-002 standards. As for CIP-014, if there is a reliability issue it should be identified in the planning studies and addressed operationally through the SOLs. As IROLs are Operating limits this should be the responsibility of the RC. Perhaps the answer here is again to expand the scope of CIP-014 to facilities that have an identified IROL, but not the Functional Entities.

Drafting Team Response:

Thank you for your comment, but the DT respectfully disagrees. The DT does not feel that it is within our scope to make any determinations on how operating limits are established. If the operating limit is established, then that determination can have a bearing on the responsible entity's application of their CIP-002 assessment.

Industry Comment:

The MRO NSRF would like the SAR Drafting Team to consider the following:

- Re-defining EACMS as two separate definitions – Electronic Access Control Systems, and Electronic Access Monitoring Systems (EACS / EAMS). Separating them allows more granularity in the subsequent technical requirements in CIP-007 and CIP-010 (perhaps others). o
- The SAR should have "SAR Type" box "Add, Modify or Retire a Glossary Term" checked.
- The identification of these Cyber Assets is already required in order to meet and maintain compliance to CIP-005 and CIP-006. For example, the CIP Evidence Request Tool (ERT) version 6 already includes requests for these types of lists (EACMS & PACs) on the 'Cyber Assets' tab. However, the CIP ERT is not enforceable, so if these types of lists are to be requested, associated clear requirements are necessary.
- The MRO NSRF has concerns about creating a zero-defect requirements.

Drafting Team Response:

Thank you for your comment. Although splitting of EACMS into two separate items may have merit, expanding this SAR to accommodate an EACMS split goes beyond its scope and purpose. An EACMS split request should be submitted via a new SAR.

The DT determined the SAR is unclear regarding identification of EACMS, PACS, and PCAs and proposed edits have been incorporated. Auditors addressing missed identification of EACMS, PACS, and PCAs have found it difficult to keep potential findings of non-compliance relegated to a single standard for each finding. The intent of the SAR is to address this in a single standard to handle each case where failure to identify and provide appropriate protections has occurred. Further, revisions to the SAR have also been made to avoid mandating creation of zero-defect requirements.

Industry Comment:

The existing NERC CIP Evidence Request Tool already requires entities to provide a discreet asset list of EACMS, PACS, and PCAs. Therefore, adding additional requirements to identify these assets is unnecessary and duplicative to existing requirements.

Drafting Team Response:

Thank you for your comment, but the DT respectfully disagrees. The NERC CIP Evidence Request is an auditing tool outside of standard requirements. The objective of the SAR is not to incorporate audit processes into a standard or requirement but to address the identification of EACMS, PACS, and PCAs.

Industry Comment:

Several companies were thankful for the opportunity to respond and the SDT efforts.

Drafting Team Response:

Thank you for your comments.