

To whom this may concern,

The Midwest Reliability Organization NERC Standards Review Forum would like to submit the following comment.

CAN-0007; CIP-004-2 & 3; Requirement R4.2 – Revocation of Access to CCAs

The proposed revisions to CAN-007 provided no additional clarification of the standard. They only raised more issues.

The purpose of CIP-004-3 is to ensure that personnel with a bona fide need to have access (cyber, unescorted physical or both) are afforded that access, as necessary, and controlled, as appropriate. Entities are required to conduct and document activities ensuring proper access, training and control is maintained. Among these activities is an Access Control requirement as defined in Requirement R4. Specifically in Requirement R4.2, Entities are instructed to revoke access to those individuals with CCA Access within 24 hours for cause, or within seven (7) days for those who no longer require access. CAN-0007 was intended to provide direction as to what constituted a revocation of access and what evidence was required to demonstrate compliance.

Overall, the CAN lacked focus and direction. It also answered so many unasked questions that the original question was lost.

As a suggested alternative response to the question in CAN-0007, NSRF offers the following:

NSRF proposed Alternative for CAN-0007, CIP-004-2

Under Requirement 4, Responsible Entities are required to maintain list(s) of personnel with authorized cyber and authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs.

Evidence Necessary for Compliance with Requirement R4.2 shall include but is not limited to the following:

Cyber & Physical Access

- Personnel Lists (as required by R4) updated per the requirement of R4.1 documenting that all personnel whose CCA Access (Cyber, Physical or Both) was revoked within the appropriate time period as indicated in R4.2.
- System database records extracted from the actual Access Control System[s] (Cyber and/or Physical as appropriate) are to be retained in sufficient detail in order to demonstrate that the personnel whose access was revoked met the appropriate timeframe. (i.e., 24-hours for Cause or within 7 days for any other status change)

Other Evidence that would further demonstrate compliance but is not necessary could include:

- Company correspondence documenting and demonstrating personnel status changes were appropriately communicated to System Managers designated as responsible for the Access Control Systems (Cyber, Physical or Both)

- Company correspondence confirming access was removed within the appropriate timeframe.
- Attestation from the Access Control system administrator (or manager) that access was removed per the requirement.

Local Access to CCAs

- Entities shall maintain accurate lists of Personnel afforded knowledge of CCA Password (i.e., Individual or Shared Password/Accounts) per R4.1.
- Unless otherwise exempted by an Approved TFE, Personnel Lists, defining those provided access to CCA Passwords (i.e., Individual or Shared); are to accurately reflect that access was revoked through the changing of the CCA Password in conformance with the timeframe identified in R4.2.
 - For those with Active TFE, approved Mitigation plans should be used and documented to demonstrate cyber risks have been mitigated.

NSRF believes that the response as provided above, simply and clearly describes to both the Industry and Regional Auditors what is expected. Nothing more is needed and nothing more should be provided. To do otherwise, risks over reaching or unintentionally interpreting the stated Reliability Standard requirements.

Finally, NSRF is concerned by the following statement contained in CAN-0007:

“For entities that have a Technical Feasibility Exception (TFE) in place, the requirements in CIP-004, R4.2 still apply.”

NSRF believes that the statement is incorrect and inappropriate and should be stricken in its entirety.