NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP Standards Efficiency Review

Working Recommendations & Justifications
August 2021

After analytical review of industry feedback the following CIP Standard Requirements were proposed for possible retirement and/or modification. Final disposition has not been determined, please see Standards Efficiency Review Report and Transition Plan for more information. Below are the recommendations and justifications crafted by the CIP Standards Efficiency Review (CIP SER) Team:

CIP-003 R3 Rationale (Recommended Retirement and Modification)

- Using a risk-based approach, the Standards Efficiency Review (CIP SER) Team evaluated NERC CIP Reliability Standard CIP-003 to identify potential efficiencies through retirement or modification of the Reliability Standard Requirements. The CIP SER determined that CIP-003, Requirement R3 does not provide System reliability benefit beyond that provided by other Reliability Standards, because the Requirement is primarily administrative in nature. NERC Reliability Standard CIP-003, Requirement R1; therefore, should be revised to indicate designation of a CIP Senior Manager to fulfill the duties as indicated in CIP-003 and other NERC CIP Reliability Standards as applicable; thereby facilitating the retirement of NERC Reliability Standard CIP-003, Requirement R3, as identification and documentation are unnecessary administrative documentation activities.
- CIP-003, Requirement R3 states that: "[e]ach Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change."
- NERC CIP Reliability Standards are but one of many tools that entities use to protect the Bulk Electric System (BES). Eliminating unnecessary documentation requirements that provide little protection to the reliable operations of BES to allow entities to focus on the reliability and security of the bulk power system will increase the efficiency of the ERO's compliance programs.
- The CIP SER considers the CIP Senior Manager identification and documentation requirement is an administrative item that alone provides minimal benefit to security because it does not necessarily correspond to the registered entity's commitment to an effective compliance program. While it is in the best interest of the entity to implement effective leadership oversight of cyber and physical security controls to ensure the reliability of their own operations, an entity's demonstration of compliance with the Requirement does not preclude an entity's failure to effectively implement the controls or foster broader leadership support within the organization.
- The CIP SER, likewise, as indicated in CIP-003, Measure M3, entity production of ". . . a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager," does not enhance an entity's effective implementation of security controls or necessarily foster broader leadership support within the organization. Evaluation of effective leadership oversight; therefore, is better placed with Regional Entities--through their

assessment of the entity's compliance program and internal controls--whereby the totality of the entity's commitment to protect the cyber and physical security of critical infrastructure may be considered. Nonetheless, the proposed retirement and facilitating revision does not preclude any entity from documenting an individual member of senior management by name, should the entity wish to preserve the identification of the designation, through maintaining associated documentation, to support the entity's internal control policies and procedures.

- Additionally, revising NERC Reliability Standard CIP-003, Requirement R1 to indicate designation of a CIP Senior Manager to fulfill the duties as indicated in particular NERC CIP Reliability Standard Requirements supports the CIP Cyber Security Policy objective of effective program governance. For example, NERC Reliability Standard CIP-007 Requirement R2, Part 2.4 requires CIP Senior Manager or Delegate approval of mitigation plan extensions by stating: ". . . unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate." Inclusion of CIP Senior Manager or Delegate references in particular NERC CIP Reliability Standard Requirements; therefore, further renders unnecessary the current identification and documentation Requirement of CIP-003 Requirement R3 and supports revision of CIP-003 Requirement R1 to align designation of the CIP Senior Manager with the overall CIP Cyber Security Policy.
- Finally, registered entities are required to meet the all applicable CIP standard requirements contained in CIP-003-7, Requirement R2, and CIP-004 through CIP-011, as appropriate, to maintain reliability and security, regardless of the administrative identification of a CIP Senior Manager. As described above, the administrative identification of a CIP Senior Manager acts as an internal control, supporting the substantive Reliability Standards and Requirements listed above, and is more appropriately addressed in an internal controls evaluation.

CIP-003 R4 Rationale (Recommended Retirement and Modification)

- Using a risk-based approach, the Standards Efficiency Review (CIP SER) Team evaluated NERC CIP Reliability Standard CIP-003 to identify potential efficiencies through retirement or modification of the Reliability Standard Requirements. The CIP SER determined that CIP-003, Requirement R4 does not provide System reliability benefit beyond that provided by other Reliability Standards, because the Requirement is primarily administrative in nature.
- The CIP SER determined that the requirement to document a process to delegate authority (if authority is delegated), as well as the requirement to document delegates, along with the associated required information and deadline is an administrative item that alone provides minimal benefit to security because it does not necessarily correspond to the Registered Entity's commitment to an effective compliance program. While it is in the best interest of the entity to implement effective leadership oversight--including prudent delegation of authority--of cyber and physical security controls to ensure the reliability of their own operations, an entity's demonstration of compliance with the Requirement does not preclude an entity's failure to effectively implement the controls or foster broader leadership support within the organization.

- Likewise, as indicated in CIP-003, Measure M4, entity production of ". . . a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items," does not enhance an entity's effective implementation of security controls or necessarily foster broader leadership support within the organization. Evaluation of effective leadership oversight--including applicable delegations of authority; therefore, is better placed with Regional Entities--through their assessment of the entity's compliance program and internal controls--whereby the totality of the entity's commitment to protect the cyber and physical security of critical infrastructure may be considered. Nonetheless, the proposed retirement and facilitating revision does not preclude any entity from documenting an individual member of senior management by name, should the entity wish to preserve the identification of the designation, through maintaining associated documentation, to support the entity's internal control policies and procedures.
- Additionally, revising NERC Reliability Standard CIP-003, Requirement R1 to indicate designation of a CIP Senior Manager to fulfill the duties as indicated in particular NERC CIP Reliability Standard Requirements supports the CIP Cyber Security Policy objective of effective program governance. For example, NERC Reliability Standard CIP-007 Requirement R2, Part 2.4 requires CIP Senior Manager or Delegate approval of mitigation plan extensions by stating: ". . . unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate." Inclusion of CIP Senior Manager or Delegate references in particular NERC CIP Reliability Standard Requirements; therefore, further renders unnecessary the current identification and documentation Requirement of CIP-003 Requirement R3 and supports revision of CIP-003 Requirement R1 to align designation of the CIP Senior Manager with the overall CIP Cyber Security Policy.
- Finally, Registered Entities are required to meet the all applicable CIP standard requirements contained in CIP-003-7, Requirement R2 and CIP-004 through CIP-011, as appropriate, to maintain reliability and security, regardless of the administrative identification of a CIP Senior Manager—or delegates. As described above, the administrative identification of a CIP Senior Manager—or delegate--acts an internal control, supporting the substantive Reliability Standards and Requirements listed above, and is more appropriately addressed in an internal controls evaluation.

CIP-007 R4.4 Rationale (Recommended Retirement)

- Using a risk-based approach, the Standards Efficiency Review (CIP SER) Team evaluated NERC CIP Reliability Standard CIP-007 to identify potential efficiencies through retirement or modification of the Reliability Standard Requirements. The CIP SER determined that CIP-007, Requirement R4.4 does not provide System reliability benefit beyond that provided by other Reliability Standards, because the Requirement is primarily administrative in nature.

- Existing defense in depth controls reduces inherent risk - security controls such as firewalls and IDS/IPS that monitor our ESPs and can detect anomalies in real time.
- Entities already receive alerts from BES Cyber Systems in R4.2.
- Certain Cyber Assets (relays, meters, PLCs, controllers, etc.,) elements are not able to be queried or reviewed from a login and required multiple tasks using multiple tools in order to review all 5 elements.
- Requirement does not consider residual risk in context of concurrent CIP controls or defense in depth.
- Entities have implemented multiple detective, preventive and corrective controls for High Impact BCS to reduce risk.
- Performing reviews every 15 days does not provide entities an effective timeframe to perform meaningful reviews.

CIP-007 R2 (Recommended Modification)

- Using a risk-based approach, the Standards Efficiency Review (CIP SER) Team evaluated NERC CIP Reliability Standard CIP-007 to identify potential efficiencies through retirement or modification of the Reliability Standard Requirements. The CIP SER determined that CIP-007, Requirement R2 should be modified to address the prescriptive language and promote a more objective/results based approach.
- The CIP SER determined that the 35 day requirement is arbitrary. Evaluating the release of a security patch creates a high administrative/low security control value given defense-in-depth, patch cycles, and redundant and concurrent controls such as CIP-010-3 R1.6. The patch sources are listed in
- The effort needed to ensure 100% compliance does not equate to the risk associated; recommend modifying VSL criteria for a threshold of allowable error per level (e.g., single isolated error vs. repeat occurrence). Consider integrating with CIP-010 R3 Vulnerability Assessments
- Consider consolidating R2.3 and 2.2, (e.g., at least once every 70 calendar days), evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1, and take one of the following actions for applicable patches: (1) Apply the applicable patches; or (2) Create a dated mitigation plan that includes the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations; or (3) Revise an existing mitigation plan.
- Consider consolidating CIP-007-6, R2, Part 2.4 with Part 2.3 to require implementation of the dated mitigation plan and remove the requirement to be approved by a CIP Senior Manager or delegate.

- The 35 day review and 35 day install/mitigate requirement is arbitrary. Depending on the vulnerability and the available solution, a sound security procedure could require installation several days after release or no installation at all. This could be modified to require a plan and methodology for installing patches in an appropriate timeframe, as determined and documented by the entity.
- Recommend changing the 35 day patch deployment and mitigation plans into the entity having a risk based methodology/plan on the patch deployment. There tends to be pressure to deploy patches prematurely to meet this timeline and avoid mitigation plan commitments, compliance auditing concerns, and interpretations on whether the plan was good, necessary, or conducted in a timely manner (amount of mitigation plans and length).
- Move parts of this requirement to CIP-010 (day to day patch management) continued use of the word "implement" for approved documented corporate process is unneeded.
- CIP-007 R1, R2, and R3 could potentially be combined into a single objective-based "system hardening" requirement that is outcome based with guidelines for achieving outcome.

CIP-007 R4.4 (Recommended Modification)

Same issues as detailed in the recommended retirement. Propose modifying language to:

- "Review a summarization or sampling of alerts, per Cyber Asset capability, as determined by the Responsible Entity at intervals no greater than quarterly to identify undetected Cyber Security Incidents."

CIP-010 R1.3 (Recommended Modification)

- Using a risk-based approach, the Standards Efficiency Review (CIP SER) Team evaluated NERC CIP Reliability Standard CIP-010 to identify potential efficiencies through retirement or modification of the Reliability Standard Requirements. The CIP SER determined that CIP-010, Requirement R1.3 should be modified to address the prescriptive language and promote a more objective/results based approach.
- The requirement to maintain (update) configuration baselines within 30 days creates a high administrative burden with low security value.
- Depending on the Cyber Asset operating system and hardware, configuration baselines require subject matter expert time managing documentation across large matrices of technology types.
- Some configuration baseline elements (e.g., R1.1.1 to R1.1.5) are not able to be automated – requiring manual processes. This includes the ability to gather all baseline elements from a given Cyber Asset. Manual processes are susceptible to errors and require resource hours to perform rote tasks with little security value. This can require multiple sub processes by multiple SMEs to gather individual configuration baseline elements (e.g., R1.1.1 to R1.1.5) and utilizing valuable Industry resources managing configuration baselines.

- Industry processes many violations annually for surpassing the 30 day requirement or just one element of the configuration baseline (i.e., network ports) resulting in high administrative overhead.
- Entities have implemented multiple detective, preventive and corrective controls to reduce risk – which is not taken into consideration.
- Recommend revising the standard to update baselines quarterly.

CIP-010 R2 (Recommended Modification)

- Using a risk-based approach, the Standards Efficiency Review (CIP SER) Team evaluated NERC CIP Reliability Standard CIP-010 to identify potential efficiencies through retirement or modification of the Reliability Standard Requirements. The CIP SER determined that CIP-010, Requirement R2 should be modified to address the prescriptive language and promote a more objective/results based approach.
- The CIP SER team determined the requirement create high administrative burden with low security value.
- Resource and administrative constraints cause challenges reviewing across large matrix of technology types, system designs and functions (e.g., hardware, software and application security patches) due diligence.
- Entities perform configuration management in CIP-010 R1
- Entities have implemented multiple detective, preventive and corrective controls for High Impact BCS to reduce risk
- Some High Impact BCS operate software and/or hardware which does not log or forward log events.
- Checking for unauthorized changes is a labor intensive with administrative tasks and offers low security value. There is already a control for authorization of all changes and risk is reduced by the defense in depth (i.e., concurrent CIP controls).
- This activity should already be happening in the configuration change management process. If unauthorized changes are detected, then it indicates a failure to implement the controls in R1. Therefore, this item could be better addressed in the Regional Entity's risk assessment of the entity.

CIP-013 R1.5 (Recommended Modification)

- The CIP SER team found the requirement’s unclear or ambiguous language results in implementation and interpretation issues. This results in high administrative overhead of resources for little security value.

- The CIP SER team thinks that the existing risk and defense in depth controls afforded in the other CIP Standard Requirements (CIP-005 and CIP-007) should be considered, including CIP-010-3 R1.6.
- Supply Chain Cyber Security activities occur prior to deployment of a BES Cyber System to operational state. The current language of this requirement – i.e., "verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System" – is written in a present tense and from an operational perspective. This creates confusion in interpretation and in entity programs.
- The current language requires entities to perform an operational activity – i.e., verify software integrity – when Supply Chain Cyber Security activities occur months before a system is live.
- The current language does not have controls for software development and distribution prior to distribution to the entity.
- Verification of software source and integrity for all software already occurs in CIP-010-3 R.1.6.
- Recommend revising CIP-013 R1.5 language to address Cyber Security Supply Chain verifications of software integrity prior to operations.

Overarching Recommendation

(From the Standards Efficiency Review Report and Transition Plan)

- The working team evaluated the set of CIP Standards and identified a list of three recommended retirements and six modifications. The team determined that there was not sufficient justification for retiring requirements that outweighed the reliability and security benefits of the requirements, particularly in light of past FERC directives and the evolving nature of cyber security. Therefore, the working team decided to change their focus and be more strategic. The overall recommendation from the CIP SER working team is for industry to create an initiative to align the CIP Standards with the results based framework. The timing, scope, and participants of a CIP standards alignment initiative will be determined at a later date.