MIDWEST RELIABILITY ORGANIZATION

380 St. Peter St, Suite 800
Saint Paul, MN 55102
www.MRO.net
651-855-1760

CMEP Summary Report

Midwest Reliability Organization
December 31, 2023

This document was prepared to provide a summary of areas addressing key issues, trends, and significant events in the MRO region related to its delegated authorities set forth in the Compliance Monitoring and Enforcement Program (CMEP).

Key Issues in Compliance, Risk Assessment and Mitigation, and Enforcement

Compliance Oversight Plans (COPs)

A Compliance Oversight Plan (COP) is an entity-specific oversight strategy that begins with an assessment of the entity's inherent risk, existing controls, and prior performance. This process includes a detailed review of the entity's registration, compliance history, system performance and event history, and other risk factors. The resulting COP identifies what reliability standards are the focus for future compliance monitoring activities based on the entity's risk. The COP also identifies the appropriate interval for MRO's monitoring activities and the type of tools that should be expected during oversight. MRO continues to innovate the COP process by integrating it closely with Align and is developing tools for analyzing COPs to identify trends and develop outreach opportunities.

2023 Compliance Audit Status

MRO completes periodic Compliance Audits to assess registered entities' compliance with the NERC Reliability Standards. MRO staff have completed all 14 scheduled Compliance Audits for 2023 and assisted in six Coordinated Oversight audits (led by another regional entity).Coordinated Oversight is a joint engagement with other regions for multi-regional registered entities that have been approved to participate in Coordinated Oversight. Coordinated Oversight Compliance Audits allow for more efficient monitoring activities for the regions. MRO utilizes these engagements to identify and share best practices with the other Regional Entities.

Self-Certifications

MRO revised the Self-Certification scoping process and implemented a guided Self-Certification process. The risks identified in the MRO Regional Risk Assessment and the ERO Enterprise CMEP Implementation Plan are the two primary considerations that Compliance uses when determining the scope for the guided Self-Certifications. One advantage of the guided Self-Certification process is that it allows MRO to address both continent-wide and region-wide risks through a single process at a more frequent interval than Compliance Audits. MRO's Self-Certification schedule is available on its website.

WebCDMS Transition to ALIGN

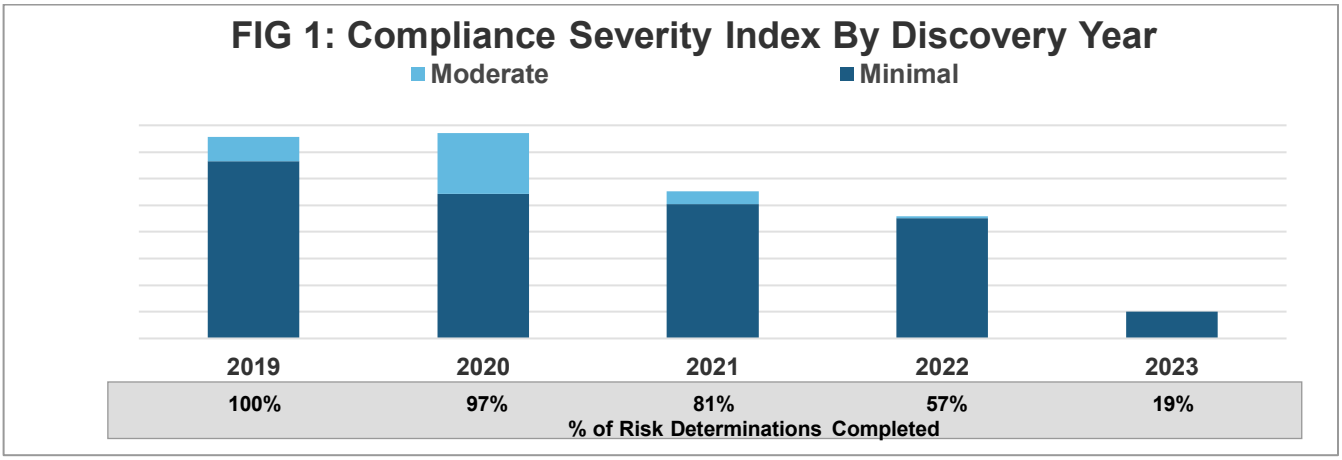
The transition to ALIGN from webCDMS, as MRO's primary CMEP tracking/communication tool, was determined complete as of December 31, 2023.This significant effort included data migration for both US and Canadian entities in both Q3 and Q4 2023. Registered entities should no longer be using webCDMS.

Risk Assessment and Mitigation Trends

In the following charts and statistics, the numbers reflect all historic issues of noncompliance in the expanded MRO region.

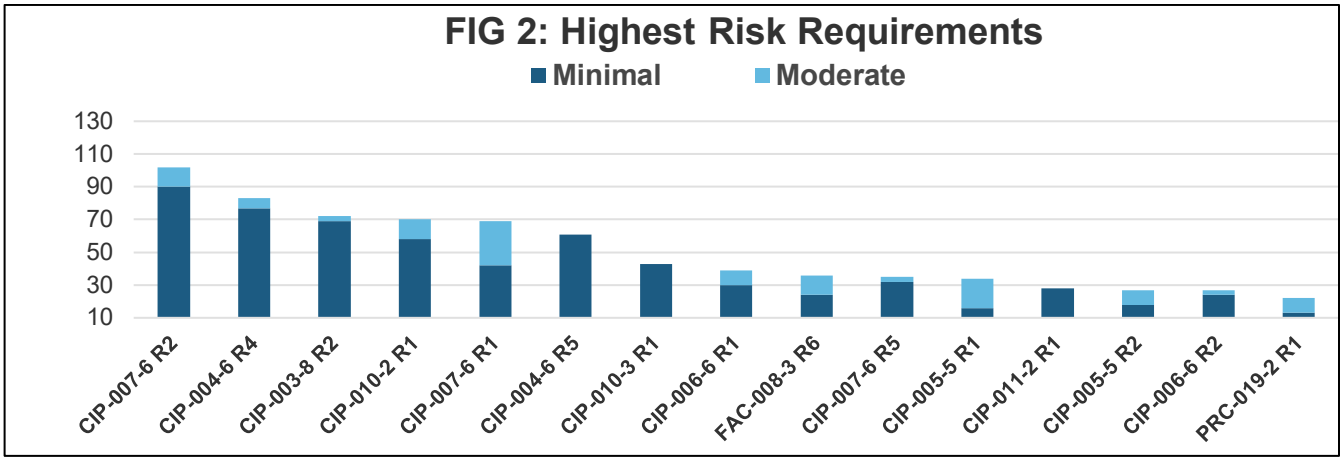
Compliance Severity Index (Figure 1)

MRO staff use the Compliance Severity Index (CSI), shown in Figure 1, to evaluate progress toward a key reliability goal of less severe violations. The CSI represents the total risk that instances of noncompliance bring to the reliability or security of the bulk power system in the MRO region. The CSI is calculated using the risk determination and Discovery Method for each noncompliance. MRO has seen a notable decrease in the risk of issues of noncompliance over the past decade due to an overall improvement in the culture of compliance. Registered entities are self-identifying issues of noncompliance in a timely manner prior to issues presenting a greater risk to reliability.



Highest Risk Issues of Noncompliance (Figure 2)

Figure 2 provides the 15 highest risk requirements, from January 1, 2019 to December 31, 2023, that have a history of issues of noncompliance, based on the CSI. Higher risk violations are associated with cyber and physical security standards, accurate facility ratings, and timely maintenance of protection systems.



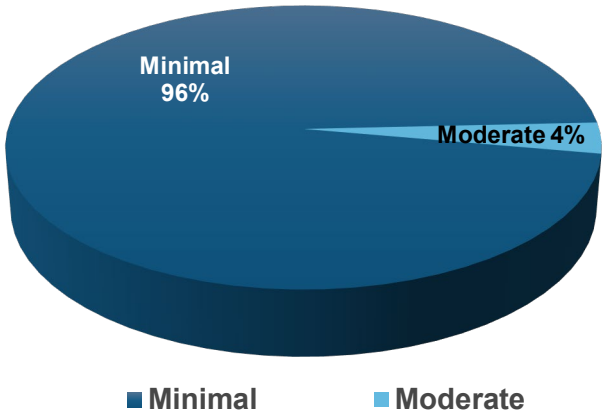
Description of the Top Five Highest Risk Requirements (Figure 2)

- CIP-007-6 R2: Requires a patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. A high-volume monthly requirement in which even the most mature security programs will have occasional noncompliance.
- CIP-004-6 R4: Implement access management programs which authorize access to applicable BES Cyber Systems.
- CIP-003-8 R2: Specify consistent and sustainable security management controls.
- CIP-010-2 R1: Requires current baseline configurations for applicable Cyber Assets.
- CIP-007-6 R1: Intended to minimize the attack surface of BES Cyber Systems through disabling or limiting access to unnecessary network accessible logical ports and services and physical I/O ports.

Risk Determinations for Issues of Noncompliance (Figure 3)

Ninety-six percent of all instances of noncompliance from January 1, 2019 to December 31, 2023, were determined to be minimal risk. There is a correlation between the percentage of issues of noncompliance being minimal risk (Figure 3) and the percentage of self-reported issues of noncompliance. Entities are identifying noncompliance earlier before the issues become more impactful to the reliability and security of the bulk power system.

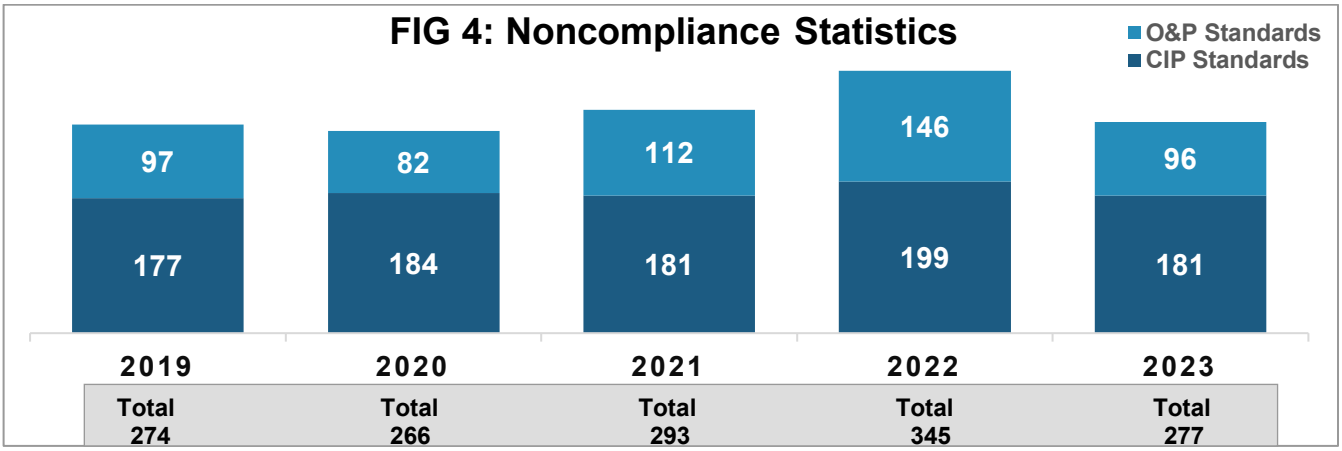
FIG 3: Risk Determinations for Instances of Noncompliance
(January 1, 2019 - December 31, 2023)



Noncompliance Trends and Statistics

Breakdown of Critical Infrastructure Protection (CIP) vs. Non-CIP Possible Issues of Noncompliance (Figure 4)

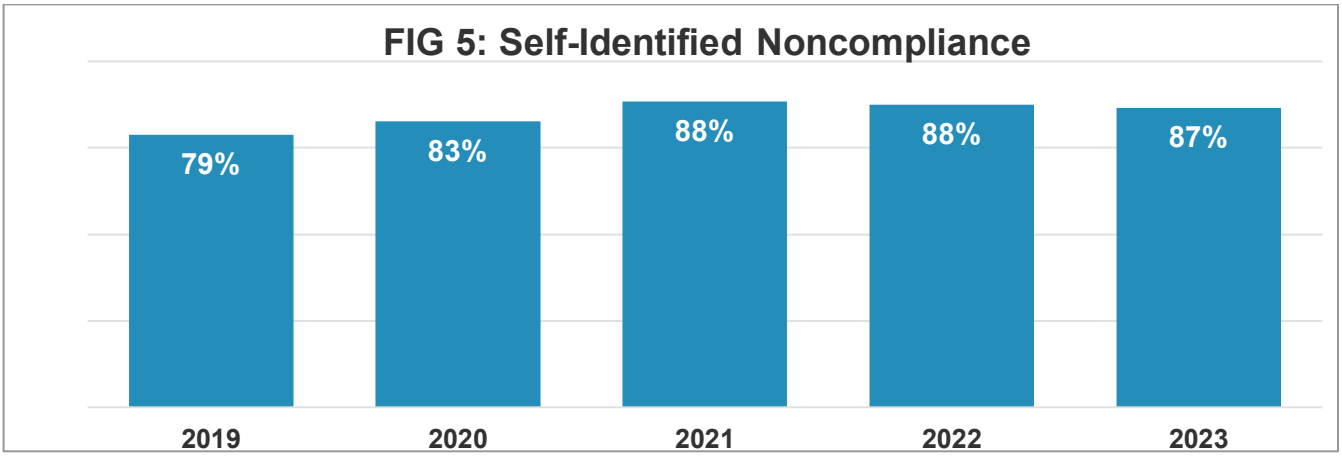
The noncompliance statistics and trends in Figure 4 are discovered and reported to NERC. Each bar represents a year from 2019 through 2023.



Registered Entity Responsibility (Figure 5)

MRO staff analyzes how often registered entities self-identify and accept responsibility for noncompliance. These trends are indicators of the commitment among registered entities in the region to perform self-assessments of their compliance with the reliability standards. The high percentages, reflected in Figure 5 , demonstrate a strong governance and compliance culture of registered entities in the MRO region, as well as registered entities' willingness to accept, and learn from, discovered issues of noncompliance in order to prevent future noncompliance with NERC Reliability Standards.

Figure 5 reflects issues of self-identified noncompliance that MRO issued dispositions from January 1, 2019 to December 31, 2023.



Discovery Method Detail (January 1, 2019 through December 31, 2023) (Figure 6)

In Figure 6, the numbers reflect the discovery method for all noncompliances in the MRO region that were reported to NERC or other applicable Regulatory Authority.

FIG 6: Discovery Method

Discovery Method Detail	2019	2020	2021	2022	2023	Sub Total	(-less) Dismissed	Adjusted Total
Compliance Audit	46	41	18	18	27	150	17	133
Compliance Investigation	0	0	0	0	0	0	0	0
Data Submittal	0	0	0	0	1	1	0	1
Self-Certification	11	6	17	24	9	67	13	54
Self-Log	131	141	155	182	174	783	9	774
Self-Report	86	78	103	121	65	453	17	436
Spot Check	0	0	0	0	1	1	0	1
Totals	**274**	**266**	**293**	**345**	**277**	**1455**	**56**	**1399**

Noncompliance Processing Methods (Figure 7)

MRO staff analyzes trends in the status of noncompliance processing by compiling all available processing methods, the average age of open noncompliances, and the closure percentage of noncompliances for each year. This analysis indicates continued progress towards expedited processing due to the increased use of CEs to dispose of minimal risk noncompliance.

Figure 7 includes issues of noncompliance for entities that were registered in the MRO region during the specified time period.

FIG 7: Noncompliance Processing Methods

(January 1, 2019 - December 31, 2023)

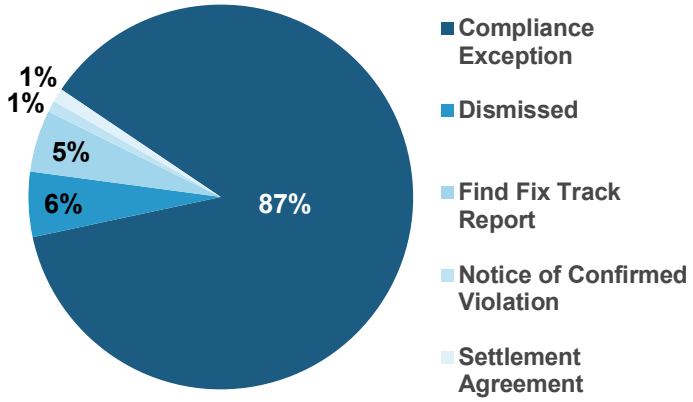
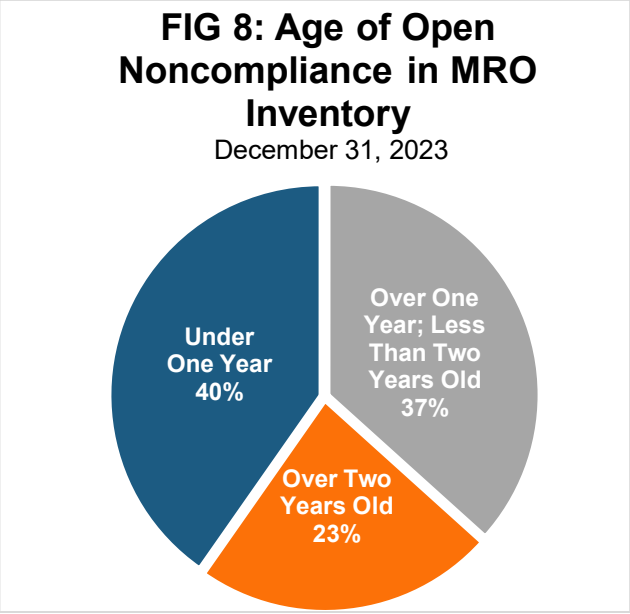


Figure 8 illustrates the aging time for all open instances of noncompliance reported to MRO and applicable government authority.



For questions on this report, please contact MRO's Enforcement Department at: enforcement@mro.net