NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

This is a Compliance Monitoring and Enforcement Program (CMEP) Practice Guide. It is developed exclusively by the ERO Enterprise under its obligations for independence and objectivity. This CMEP Practice Guide is intended for use by ERO Enterprise Staff to support consistency as they perform CMEP activities. This CMEP Practice Guide is posted publicly solely to provide transparency.

ERO Enterprise CMEP Practice Guide

Using the Work of Others
March 14, 2023

Background

To support successful implementation and compliance with the North American Electric Reliability Corporation (NERC) Reliability Standards, the Electric Reliability Organization (ERO) Enterprise[1] adopted the Compliance Guidance Policy.[2] The Compliance Guidance Policy outlines the purpose, development, use, and maintenance of guidance for implementing Reliability Standards. According to the Compliance Guidance Policy, Compliance Guidance includes two types of guidance – (1) Implementation Guidance and (2) Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.[3] This document summarizes some of the requirements in NERC Reliability Standards, but the language of the Reliability Standards is enforceable and supersedes any description in this document.

Purpose

This CMEP Practice Guide provides guidance to CMEP staff[4] when reviewing evidence, provided by registered entities, that is generated "Using the Work of Others." Work of Others can include an assessment of the registered entity's compliance with a Reliability Standard or an independent internal control review may be conducted by: 1) an independent Subject Matter Expert; 2) a government entity (such as the Government Accountability Office or Nuclear Regulatory Commission); 3) a contractor who has been commissioned by the registered entity as an independent third party; or 4) an internal department within the registered entity that is independent of the department performing Reliability Standards operations.

The use of the word "others" in this Practice Guide refers to internal or external parties that perform work for the registered entity. Similarly, "independent" refers to the internal or external party that can objectively carry out its work for the registered entity in an unbiased manner.

Using the Work of Others

A registered entity may seek to rely on the work of others to support a registered entity's demonstration of compliance with a Reliability Standard. This may include internal or external party.

---

[1] The ERO Enterprise consists of NERC and the six Regional Entities.
[2] The ERO Enterprise Compliance Guidance Policy is located on the NERC website at: https://www.nerc.com/pa/comp/guidance/Documents/Compliance%20Guidance%20Policy.pdf
[3] **Implementation Guidance** provides a means for registered entities to develop examples or approaches to illustrate how registered entities could comply with a standard that are vetted by industry and endorsed by the ERO Enterprise. **CMEP Practice Guides** differ from Implementation Guidance in that they address how ERO Enterprise CMEP staff executes compliance monitoring and enforcement activities, rather than examples of how to implement the standard.
[4] CMEP staff encompasses ERO Enterprise, NERC and the six Regional Entities

Government Auditing Standards[5] were used as a framework to develop this practice guide. CMEP staff generally follow the guidelines below when using the work of others to assess a registered entity's compliance with NERC Reliability Standards.

- CMEP staff should determine whether materials or evidence provided by an entity are relevant to the current compliance monitoring activity objectives.
  - The materials or evidence provided to CMEP staff may include an assessment performed by others of the entity's compliance with a Reliability Standard and should be reviewed following the application guidance herein.
- If a registered entity provides CMEP staff with the work of others, CMEP staff should receive and review documentation of others' qualifications, capabilities, and independence and should determine whether the scope, quality, and timing of the work performed can be relied on in the context of the current engagement objectives.
  - When evaluating qualifications, capabilities, and independence, CMEP staff may consider the expertise in the related area, such as certifications, relevant training, background, and work experience.

CMEP staff can use the following application guidance:

- The results of others' work as stipulated in a specific Standard/Requirement could be used as useful sources of information for planning and conducting the compliance monitoring engagement. Relying on the work of others could influence the CMEP staff's selection of objectives, scope, and subjects that warrant further audit work or follow up.
- Internal Audit, Internal Control, and Risk Management functions are an important part of overall governance, accountability, and internal controls. A key role of many internal audit organizations is to provide assurance that internal controls are in place to adequately mitigate risks and achieve program goals and objectives. Given the role of internal audit organizations, CMEP staff may elect to rely on the work of the registered entity's internal auditors in assessing the effectiveness of design or operation of internal controls that are significant to assessment of risk consistent with the audit objectives.
- If others have completed work related to the objectives of the current compliance monitoring engagement, CMEP staff could rely on the work to support findings or conclusions and thereby avoid duplication of effort. In making this determination, CMEP staff could review the most recent reports, plans, or documentation, or perform tests of others' work to modify sampling strategy[6]. The nature and extent of evidence needed will depend on the significance of the others' work to the current objectives and the extent to which CMEP staff will use that work.

[5] Government Auditing Standards are located on the GAO website at: https://www.gao.gov/assets/720/713761.pdf (See Sections 8.80-8.86 "Using the Work of Others").
[6] Additional guideline on sampling can be found within ERO Enterprise Compliance Monitoring and Enforcement Manual (See section "Risk-Based Approach").

- Conclusions of others may be used if:
  - The work product is determined to stand on its own, whereas a reasonably qualified person may re-perform the work and come to the same conclusion, and
  - If it is known or demonstrated others were qualified to make those conclusions and that they were considering NERC Reliability Standards compliance, including internal controls.

Examples

CIP-013: Independent Third-party Assessment of Vendors

A registered entity may rely on an independent third-party assessment of vendors in developing an overall process to procure CIP-013 applicable BES Cyber Systems. In such cases, the registered entity could submit the assessment to CMEP staff to support demonstrating compliance and/or other CMEP activities, such as mitigation of a noncompliance. CMEP staff should review the assessment to determine how the registered entity used the information in their environment to gain reasonable assurance that the selected vendor met the requirements. For example, CMEP staff should consider the following:

- Asking the registered entity to provide artifacts to demonstrate supply chain compliance. In this example, the registered entity could provide the independent third-party assessment report that it used to gain assurance of compliance.
- Validating the assessor's qualifications and cyber security framework used to perform the vendor assessment by personnel with appropriate independence, credentials, and sufficient understanding of cyber security supply chain risk through independent certifications and/or credentials.
- Evaluating the scope, sampling, and results of the third-party assessment.
- Understanding the assessor's scope of review and results, including the sampling methodology.
- Evaluating how the registered entity used the third-party assessment in its Supply Chain risk management plan (CIP-013 R1).[7]
- Requesting and reviewing further evidence, if necessary, to gain reasonable assurance of compliance.

Federal Information Security Modernization Act (FISMA) Audits

Registered entities, typically Federal agencies, that are governed by FISMA Compliance requirements are regularly assessed by others for adequacy and effectiveness of information security policies, procedures, and practices. In such cases, the registered entity could submit the independent assessment to CMEP staff to support demonstrating compliance and/or other CMEP activities. CMEP staff should review the independent assessment to determine how the registered entity used the information in their environment to gain reasonable assurance of compliance with the NERC Reliability Standards by:

[7] NERC Reliability Standard CIP-013-2

- Asking the registered entity to provide the independent FISMA assessment artifacts.
- Evaluating the assessor's qualifications and cyber security framework used to perform the assessment by personnel with appropriate independence, credentials, and sufficient understanding of the areas being assessed.
- Understanding the FISMA scope of review and results, including the sampling methodology.
- Requesting and reviewing, if necessary, additional evidence to gain reasonable assurance of compliance.

Internal Audit, Internal Control, and Risk Management Programs of Registered Entity

A registered entity may rely on the work of others to support internal control development and testing. Registered entities often use internal auditors, or other independent assurance teams, to assess the design, implementation, or effectiveness of internal controls in support of compliance obligations. Similarly, CMEP staff should evaluate specific instances of registered entities relying on the work of others to comply with Standards and Requirements and consider how the registered entity may be using the work of others in its compliance program.

Conclusion

Where registered entities rely on the work of others for their compliance obligations, the ERO Enterprise CMEP staff may rely on this information to determine reasonable assurance to support demonstrating compliance and/or other CMEP activities around compliance. CMEP staff should review the relevant documentation provided by others, in addition to reviewing the qualifications, capabilities, and independence. If necessary, CMEP staff may request further evidence to conduct their own review. CMEP staff may use information gathered to adjust scope or sampling selections during the current engagement, and/or modify future CMEP engagements.

Revision History

Revision #	Revision Date	Revision Details
V1.0	03/14/23	Initial Draft