By Lew Folkerth, Principal Reliability Consultant

Foundations - Part 2

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your entity.

It may also help you and your entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency and sustainability of your CIP compliance programs.

There are times that I also may discuss areas of the Standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

This article continues the discussion of the background needed in order to be a proficient CIP professional. For the purposes of this article, I'll assume you're new to the CIP Standards, but this material should be useful to all CIP professionals, even if only as a review.

Understand the CMEP and the CMEP Processes

The Compliance Monitoring and Enforcement Program (CMEP) is Appendix 4C to the NERC Rules of Procedure. It describes how the Reliability Standards are monitored, assessed and enforced.

There are seven compliance monitoring processes defined in the CMEP. Think of these processes as seven general ways that Standards can be monitored for compliance.

1. Compliance Audit (audit) is probably the best known of the compliance monitoring functions. An audit consists of a formal review of compliance. The scope of an audit (or other CMEP process) consists of the Standards and Requirements under review, as well as the time period considered by the review. Audits may be conducted on-site (at the Registered Entity's site) or off-site (via teleconference). Audits are typically scheduled well in advance, but an unscheduled audit may be initiated with a notice of ten business days.

2. Self-Certifications are sometimes used when a new Standard comes into effect, or for other lower-risk issues. A Registered Entity is required to certify its compliance with a Standard. A self-certification should be treated as a self-audit with a specified scope. In most cases, entities are asked to supply the supporting documentation they used to arrive at their self-assessment.

Frankfort South and North Breakwater, MI – Photo: L Folkerth

3. Spot Check is very similar to a Compliance Audit but usually has a limited scope. Spot Checks are usually conducted off-site.

4. Compliance Investigations are in-depth reviews of a very specific compliance area and can be triggered by a system disturbance, a Complaint, or other indication of non-compliance.

5. Self-Report is a submittal by a Registered Entity that reports a possible instance of non-compliance to CMEP staff. As no compliance program is perfect, Self-Reports are an expected occurrence by entities with robust compliance programs and strong internal controls. Self-Reports are encouraged by mitigating credit being permitted in penalty calculations. Some Registered Entities are granted approval to perform **Self-Logging** for minimal-risk issues instead of submitting a full Self-Report.

6. Periodic Data Submittals are used for some Standards that need frequent but routine monitoring. For

Continued on page 13

Continued from page 12

example, FAC-003-4 is monitored in part by quarterly Data Submittals of vegetation outage reports.

7. Complaint is a report by a third party to NERC or a Regional Entity of possible non-compliance on the part of a Registered Entity. A Complaint may be submitted anonymously.

In my opinion, any CIP professional should be very familiar with the CMEP processes outlined here. I suggest you read and study Appendix 4C.

Understand Compliance Tools

The Reliability Standard Auditor Worksheet (**RSAW**) is the document used to communicate your approach to compliance with a Standard.

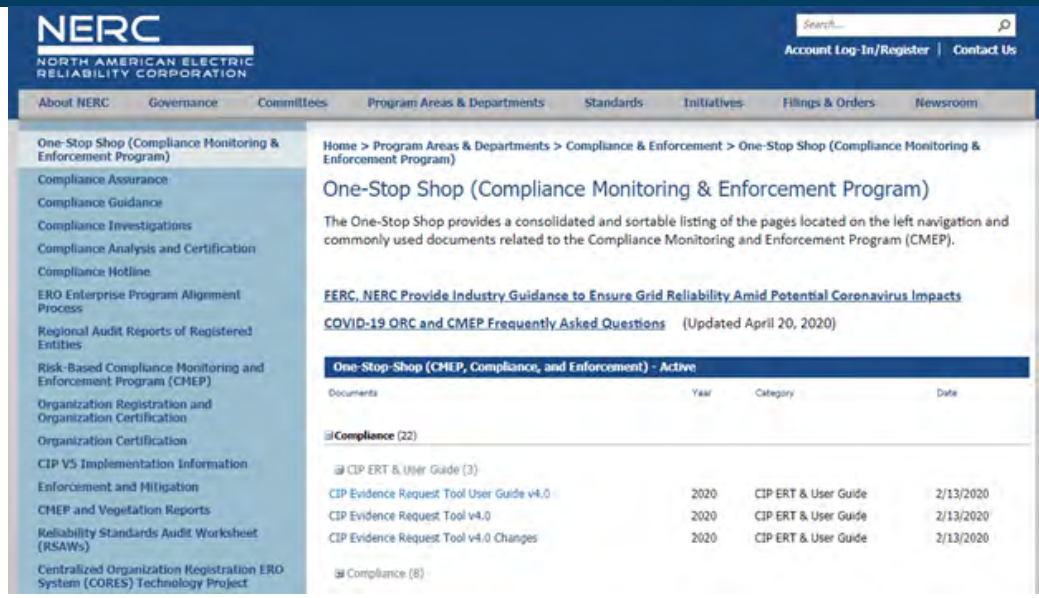
For a CMEP monitoring engagement (audit or spot check) within the RF footprint, you obtain the RSAW for a Standard from the NERC website and fill it out prior to the monitoring engagement. You will supply, in the appropriate sections:a list of subject matter experts responsible for the Standard, a list of evidence being supplied to demonstrate compliance with each Requirement or Part, and a narrative of how you achieve and maintain compliance with the Requirement or Part.

CMEP staff will typically follow the flow in the Compliance Assessment Approach section when evaluating evidence of compliance. This section of the RSAW also can give you valuable insight into how a monitoring engagement will proceed.

The narrative section of the RSAW is the most important part of the submission. It's your chance to convey to the audit team, in your own words, what the Standard means to you and how you approach compliance with the Requirement or Part. My article in the May 2015 RF Newsletter (available here) provides an in-depth look at the CIP RSAWs.

The CIP Evidence Request Tool (**ERT**) complements the RSAW by providing a common structure and format for submitting compliance evidence. You can see at any time what types of evidence will be requested for a monitoring engagement and what form the evidence should take during submission.

The ERT consists of the CIP Evidence Request Tool User Guide and the Evidence Request Tool spreadsheet. The current version of these documents can be obtained on the NERC website by hovering over “Program Areas & Departments” on the top menu and selecting “Compliance & Enforcement” from the pop-up menu. Then select “One-Stop Shop (Compliance Monitoring &



Enforcement Program)” from the left menu. Open the “Compliance” section and then open the “CIP ERT & User Guide” section.

Requests for Assistance

If you are an entity registered within the RF Region and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the RF website here.

Back issues of The Lighthouse, expanded articles and supporting documents are available in the RF CIP Knowledge Center.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

Lew Folkerth, Principal Reliability Consultant, I maybe reached here.