The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Compliance Is Not Security

During my career in CIP compliance I have heard the phrase “compliance is not security” many times and in many contexts. If it’s used as a simple statement of fact then I agree with it. Compliance and security are two different, but complementary, domains of effort.

However, when “compliance is not security” is used to imply that compliance has no value or is a waste of resources, then I strongly disagree. The phrase has been used to assert that “we can do it better without standards” or “our compliance violation had no impact on security.” I have never seen a case where these claims were true.

Compliance should be a governance function applied to an entity’s security processes. Without governance, such as internal controls or compliance monitoring processes, you have no assurance that security processes are being consistently applied. As many data breaches show, leaving even a seemingly small security hole can have major consequences.

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.

I’ve also encountered concerns that workshops and other presentations advocate going beyond the minimum requirements of the CIP Standards.

New Presque Isle Light, MI – Photo: L Folkerth

My response to the concern that we are promoting reliability past the level of basic compliance is, “That’s our job.” In fact, reliability is not just our job, it’s our mission and our passion. The ERO Enterprise’s (NERC and the six Regional Entities) primary purpose is maintaining and enhancing the reliability, resilience and security of the Bulk Electric System (BES).

The NERC Reliability Standards establish a level of performance expected for Registered Entities of all sizes and types. This is a level of performance that can be considered a baseline or the lowest acceptable level of performance. They are not intended to keep up with the rapidly changing world of cyber security. As a simple example, CIP-007-6 R5 Part 5.5 requires a minimum password length of eight characters. However, the art and science of password cracking has changed the risk in this area so that recent guidance from the Center for Internet Security suggests a minimum password length of 14 characters.

This means that in any webinar or workshop where password length is discussed, the ERO Enterprise will note that the minimum required password

Continued on page 9

Continued from page 8

length is eight characters but that we recommend using at least 14 characters where feasible.

As an entity responsible for some aspect of the BES, you must constantly adapt to the changing threat environment. For example, the recent shutdown of a major pipeline on the east coast likely resulted from a compromise of one of the pipeline company's billing systems. In response to this occurrence, has your entity reviewed its information systems that are not subject to the CIP Standards?

The CIP Standards are applicable to those systems with real-time (within 15 minutes) impact on the BES. But have you identified all the systems that can cause an operational disruption in a timeframe longer than 15 minutes?

At a generating plant, fuel handling systems seldom have a 15-minute impact on operations. But what if those systems are compromised and as a result are disabled or damaged? How long will the plant stay operational? If these systems suffer physical damage as a result of cyber compromise, how long will it take to repair the systems, and at what cost?

The role of the ERO Enterprise is to enhance reliability, resilience and security. Monitoring compliance with the NERC Reliability Standards is one tool we use to perform that role, but not the only tool. RF has multiple offerings listed on our website to assist you in improving your reliability, resilience, security, and compliance. The various Regions are cooperating on outreach activities and opening outreach such as webinars, workshops and training to all entities across the NERC footprint.

I encourage you to get involved by attending the webinars and workshops of interest to you. You can become actively involved by participating in the RF Critical Infrastructure Protection Committee.Technical Talk with RF is a monthly virtual meeting that brings together experts to discuss various topics of interest, and also provides announcements of other outreach and training events across the ERO.

If you are being audited, take the opportunity to talk to your auditors about what they are seeing and solicit their recommendations and advice as they have the advantage of seeing multiple programs and internal controls. While we have many tools at RF, all the departments share the same mission in helping our entities continuously improve so that you can be both secure **and** compliant.

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, can be reached here.