By Lew Folkerth, Principal Reliability Consultant

CIP-012-1 In-Depth

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.

On January 23, 2020, FERC issued Order 866 approving CIP-012-1, Cyber Security - Communications between Control Centers, as mandatory and enforceable. Let's take a close look at some key concepts in this new Standard. Although CIP-012-1 won't become effective until July 1, 2022, we should start our security and compliance planning now in order to ensure we can properly address the long lead-time actions properly.

In this article I will abbreviate "Real-time Assessment and Real-time monitoring data" as "RTA/RTM data." (Note that this is not a NERC-approved abbreviation.)

Scope and Applicability

CIP-012-1 is unusual within the Cyber Security Reliability Standards in that it doesn't refer to impact ratings or BES Cyber Systems. Instead, CIP-012-1 applies to certain communications between Control Centers.

One way to determine if you need to comply with CIP-012-1, and, if so, which communications need to be protected, is to follow this series of steps:

1. Identify all applicable facilities meeting the definition of Control Center.
    a. List all Control Centers your entity owns or operates.
    b. Remove exempt Control Centers from the list.
2. Identify the types of data to be protected.

Muskegon, MI: S & N Breakwater, S Pier – Photo: L Folkerth

3. List applicable communication paths.
4. Identify communication paths to be protected.
5. Identify entity coordination requirements.

What's Required

You must develop at least one plan (which I'll call a data protection plan) that identifies the type of security protections used and identifies where those protections are applied in your networks. Your plans also must include provisions to coordinate protections with other entities to protect RTA/RTM data. You must then implement those plans on or before the effective date of the Standard.

Your data protection plan must include provisions for identifying the data to be protected. That data must then be protected while being transmitted between Control Centers.

This means your protection plan must also include provisions for protecting RTA/RTM data when transmitted in any form to any applicable Control Center. For example, data replication between a primary Control Center and a backup

Continued on page 10

Continued from page 9

Control Center must be protected if the replicated data includes any of the RTA/RTM data types.

What's Permitted

CIP-012-1 R1 permits you to invoke CIP Exceptional Circumstances. In order to reduce your compliance risk for CIP-012-1, your data protection plan should include provisions for responding to CIP Exceptional Circumstances.

These provisions should include detection, recording and reporting of protection failures. The definition of a CIP Exceptional Circumstance includes "an imminent or existing hardware, software, or equipment failure," so you should be able to handle some failures of data protection as a CIP Exceptional Circumstance without resorting to a Self-Report.

What's Implied

In order to fulfill Requirement R1, you may need to perform some actions that R1 does not explicitly require:

A. Identify the communications paths to be protected. See Scope and Applicability for my suggestions on how to do this. If you will not be protecting all non-voice communications paths to other Control Centers, you must identify the types of information that meet the definition of RTA/RTM data and identify the communications paths to other Control Centers that carry any of this information. I recommend documenting the steps you use to perform this identification in your data protection plan so you can repeat the process as needed.

B. As with any plan, each of your data protection plans required by CIP-012-1 should be reviewed periodically, perhaps annually. While the Standard doesn't require this or specify a review period like other CIP Standards, I strongly recommend that you include review provisions in your plan. The intent of this review is to ensure your physical systems still match your plan and that changes haven't crept in that would make your plan inaccurate.

C. Each data protection plan should also include provisions to handle changes. For example, if the data to be protected changes, additional communication paths might need to be protected. Or you might commission a new Control Center, which must be added to the applicable data protection plans. Also, expect the Certification process for your new Control Center to look closely at the applicable data protection plans.

Conclusion

You will need to perform an applicability evaluation early as you assess your compliance and security posture around efforts to determine the communication paths that will be in scope, so you can begin planning the protections for those communication paths.

I suggest you begin your compliance efforts now; don't wait until the effective date is looming.

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.

An expanded version of this article, "CIP-012-1 In Depth," is available in the RF CIP Knowledge Center. Back issues of The Lighthouse, expanded articles and reference documents are also available.

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.