The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Accompanying the July/August 2020 RF Newsletter Article "CIP-012-1 Key Concepts"

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 this new Standard. Although CIP-012-1 won't become effective until mid-2022 in the U.S., we should start our security and compliance planning now in order to ensure we can properly address the long lead-time actions. The sidebar, "CIP-012-1 Applicable Documents," lists the documents referenced in this discussion.

CIP-012-1 Applicable Documents

Standard

Implementation Plan

Technical Rationale

Proposed Implementation Guidance

Glossary of Terms

Reliability Functional Model

FERC Order 866

TOP-003-3

IRO-010-2

Secure ICCP - PNNL

CIP Exceptional Circumstances

Control Systems Communications Encryption Primer

NIST SP800-77 Guide to IPsec VPNs

Applicable Definitions

Before we analyze CIP-012-1, let's explore some of the definitions we'll need.

CONTROL CENTER

From the NERC Glossary of Terms (reformatted):

> "One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of:
>
> 1) a Reliability Coordinator,
> 2) a Balancing Authority,
> 3) a Transmission Operator for transmission Facilities at two or more locations, or
> 4) a Generator Operator for generation Facilities at two or more locations."

Note that this definition does not say an entity must be registered as Reliability Coordinator (RC), Balancing Authority (BA), Transmission Operator (TOP) or Generator Operator (GOP). It says the facility performs the reliability tasks of one of those functions. In order to determine the reliability tasks for a function, we need to look at the Reliability Functional Model (see inset). For example, a facility hosting operating personnel that perform any of the following Generator Operation functions would be considered a Control Center in the context of the Glossary definition:

1. Formulate daily generation plan.
2. Report operating and availability status of units and related equipment, such as automatic voltage regulators.
3. Operate generators to provide Real Power and Reactive Power or Interconnected Operations Service per contracts or arrangements.
4. Monitor the status of generating facilities.
5. Support Interconnection frequency.

Reliability Functional Model

The Reliability Functional Model is a NERC document that provides a framework for the development and applicability of the Reliability Standards. It is developed by a team of stakeholders, is endorsed by the Standards Committee, and is published on the NERC web site.

REAL-TIME ASSESSMENT

From the NERC Glossary of Terms (reformatted):

> "An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to:
>
> - load,
> - generation output levels,
> - known Protection System and Special Protection System status or degradation,
> - Transmission outages,
> - generator outages,
> - Interchange,
> - Facility Ratings, and
> - identified phase angle and equipment limitations.
>
> (Real-time Assessment may be provided through internal systems or through third-party services.)"

REAL-TIME MONITORING

Real-time monitoring is not a defined Glossary term (other than "Real-time" being defined as "Present time as opposed to future time"). In order to determine what is meant by this term, we need to refer to the process used to develop CIP-012-1. FERC Order 866 contains a summary of this information at paragraphs 37-43. In particular, Order 866 states at paragraph 43, "[T]he data protected under Reliability Standard CIP-012-1 is the same data identified under Reliability Standards TOP-003-3 and IRO-010-2."

TOP-003-3 (Operational Reliability Data) requires each TOP and BA to maintain a documented data specification, which will include the data needed to perform Real-time Assessments and Real-time

monitoring, and to communicate that specification to the applicable entities including each BA, TOP, GOP, Transmission Owner (TO) and Generator Owner (GO).

In a similar manner, IRO-010-2 (Reliability Coordinator Data Specification and Collection) requires each RC to maintain and distribute a documented data specification to entities that have data, including Real-time monitoring and Real-time Assessment data, the RC requires.

Both TOP-003-3 (for each BA and TOP) and IRO-010-2 (for each RC) permit the BA, TOP and RC to add applicable inputs to the list specified in the Real-time Assessment definition.

RTA/RTM DATA

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.) In order to determine the data that needs to be protected, you will need to obtain the lists of data that support Real-time Assessments and Real-time monitoring from your BA, TOP and RC. Keep these lists as compliance evidence.

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. Based on the definition discussed above, Control Centers identified by CIP-002-5.1 (BES Cyber System Categorization) that contain BES Cyber Systems must be on this list. Note that from this definition it may be possible to own or operate a Control Center that does not have any BES Cyber Systems identified. For example, a merchant operations center might perform real-time monitoring of a generation fleet but not operate systems that could have a 15-minute impact on those generators. If there is not a 15-minute impact, then your entity would not have identified BES Cyber Assets, and therefore would not have identified BES Cyber Systems, at that Control Center. However, this Control Center must be included in the list generated by this step.

        Output: List of Control Centers owned or operated by your entity

    b. REMOVE EXEMPT CONTROL CENTERS FROM THE LIST. If any Control Center listed in Step 1 falls under the jurisdiction of a nuclear regulatory agency, that Control Center is exempt from CIP-012-1. (See CIP-012-1 Sections 4.2.1 and 4.2.2.) Also, any Control Center that only transmits RTA/RTM data about a co-located generation or Transmission facility is exempt from CIP-012-1. (See CIP-012-1 Section 4.2.3.) The Technical Rationale describes this case in detail. Remove these exempt Control Centers from your list and document the reason for later use as compliance evidence.

If your entity is registered for one of the six applicable functions, but does not own or operate an applicable Control Center, I recommend that you coordinate with your Regional Entity's risk assessment team to ensure your Inherent Risk Assessment (IRA) reflects this fact. If you are registered in the RF footprint, please make sure your responses to the questions related to Control Centers in the Entity Profile Questionnaire are accurate and up-to-date. If you have any questions about how to do this, please send an email to entityprofile@rfirst.org.

Output: List of applicable Control Centers

2. IDENTIFY THE TYPES OF DATA TO BE PROTECTED. Unless you are going to protect all data communication paths to other Control Centers, you will need to know what data you are required to protect. As discussed, you must obtain the data specifications required by TOP-003-3 and IRO-010-2. From those data specifications you will extract the types of data used in Real-time Assessment and Real-time monitoring.

   Output: List of data types (RTA/RTM data) that need to be protected in transit to other applicable Control Centers.

3. LIST APPLICABLE COMMUNICATION PATHS. For each applicable Control Center, make a list of all communication paths into or out of the Control Center. This list is not explicitly required, but will be needed by an audit team. For each communication path on this list, you may exclude (and document the reason for the exclusion):

   a. Paths that carry only oral communications, and
   b. Paths that do not communicate with another Control Center.

   Output: List of data paths to other Control Centers

4. IDENTIFY COMMUNICATION PATHS TO BE PROTECTED. Now that you have the list of data paths between Control Centers, you may choose between two approaches. You can protect all of these links as if they all carry RTA/RTM data and thereby not need to determine what data is carried by each link. Or you can determine which paths are not capable of carrying RTA/RTM data and therefore may be excluded from compliance with CIP-012-1, as these links do not meet the language of R1. Note that any link that carries any of the data types identified as RTA/RTM data will be in scope for CIP-012-1. Even if your entity doesn't perform Real-time Analysis or Real-time monitoring, any communication path that carries any RTA/RTM data must be protected.

   Output: List of communication paths to be protected

5. IDENTIFY ENTITY COORDINATION REQUIREMENTS. From the list of communication paths to be protected, list those paths that are connected to another entity. This is the list of paths that will require inter-entity coordination per Part 1.3.

   Output: List of communication paths requiring inter-entity coordination

Effective Date

In the U.S., CIP-012-1 will become effective on July 1, 2022.

What's Required

CIP-012-1's enforceable language contains only one Requirement:

R1 *The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include:*

- ***1.1.*** *Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;*
- ***1.2.*** *Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and*
- ***1.3.*** *If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.*

You must develop at least one plan (which I'll call a data protection plan) that identifies both the type of security protections used and where those protections are applied in your networks. Your plan must also include provisions to coordinate protections with other entities to protect RTA/RTM data. You must then implement all of your data protection 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, not just to the entity that identified that data. For example, if your TOP identifies certain information as RTA/RTM data, that data must be protected in all Control Center-to-Control Center communications, not just in communications to the TOP.

This means your protection plan must also include provisions for protecting RTA/RTM data when transmitted in any form to any Control Center that is not exempt from CIP-012-1. For example, data replication between a primary Control Center and a backup Control Center must be protected if the replicated data includes any of the RTA/RTM data types.

The data protections applied to each applicable communication path must be in effect at all times. Any failure of these protections may result in an instance of non-compliance, which could result in a Self-Report. For example, a device that provides encryption on a link to another Control Center could fail, forcing you to bypass the encryption while the device is repaired. You would be in a state of non-compliance while this device is out of the data path.

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 (see my article referenced in the sidebar). 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 CIP-012-1 R1, you may need to perform some actions that R1 does not explicitly require:

COMPLIANCE EVIDENCE

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.

PERIODIC REVIEW

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.

CHANGE MANAGEMENT

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.

CHANGES TO THE IDENTIFICATION OF RTA/RTM DATA

There is no provision for phasing-in changes to the scope of CIP-012-1. If your TOP, BA or RC changes the identification of RTA/RTM data such that additional communication paths come into scope for CIP-012-1, you may be in violation if the additional paths are not protected. I suggest you work with your TOP, BA and RC to provide advanced notice of any such changes, so you have time to make modifications to your data protection plan. You may want your data protection plan to include a control to monitor for changes to ensure adjustments are made in a timely manner.

CONTROL CENTER BOUNDARY

The Glossary definition of Control Center does not clearly identify the boundary of a Control Center. Since CIP-012-1 R1 requires you to protect data "while being transmitted between any applicable Control Centers," you will need to define where the boundary of a Control Center lies. For Control Centers containing high or medium impact BES Cyber Systems, this might be the Physical Security

Perimeter (PSP). However, if the Control Center has only low impact BES Cyber Systems or no BES Cyber Systems then you will need to define the boundary in some other way.

I suggest you include a clear and reasonable identification and justification of the boundary of each of your applicable Control Centers in your data protection plan. Ensure that RTA/RTM data is protected before it crosses that boundary.

DATA CENTERS

The Control Center definition also includes associated data centers. Communications between each of your Control Centers and each of your data centers should be included in your data protection plan. If the Control Center and the data center are co-located, this might be as simple as making sure all communications runs are in conduit. But if the Control Center is separated from the data center such that physical protection for the communication paths is impractical, then you will need some form of logical protection for these paths.

Supporting Documents and Guidance

In addition to the Standard and its Implementation Plan that were approved by FERC, the CIP-012-1 Standard Drafting Team (SDT) produced two other documents.

The Technical Rationale discusses the 4.2.3 exemption for Control Centers and provides additional background for the Standard itself.

The SDT also produced an Implementation Guidance document that has not, as of this writing, been approved by the ERO. The Implementation Guidance discusses where and how to apply protections.

Limited Risk-based Approach

CIP-012-1 Requirement R1 states that you must implement plans to "mitigate the risks" posed by impairments to confidentiality and integrity. This implies that CIP-012-1 is a risk-based Standard and should provide you some flexibility in the way you approach protecting the applicable data.

You will need to describe the risk mitigations you have in place. You will also need to demonstrate that the residual risk, which is the risk remaining after mitigating actions have been applied, has been reduced to an acceptable level.

Unaddressed Issues

AVAILABILITY

CIP-012-1 addresses only the confidentiality and integrity of RTA/RTM data. In Order 866, FERC directed NERC to also develop protections for the availability of communications between Control Centers. I suggest you monitor the development of these revisions and participate in the drafting efforts if you are able.

Possible Security Strategies

Protections for communications between Control Centers will fall into two major categories: physical protections and logical protections.

Physical Protections

Physical protection of a communications path between two control centers may be feasible over a short distance but will prove unworkable at longer distances. Physical protection will entail controlling and/or monitoring access to the physical communication medium, such as the copper wire or fiber optic cable. This will require a conduit, access-controlled tunnel or other means. Your data protection plan should identify the means of physical protection employed and should describe how this protection meets the needs of CIP-012-1.

Logical Protections

Logical protection generally means encryption of the RTA/RTM data while in transit between applicable Control Centers. As discussed in the Implementation Guidance, there appears to be two main approaches to protecting RTA/RTM data in transit: application-level protections and network protections.

One common protocol used in communication between Control Centers is the Inter-Control Center Communications Protocol, or ICCP. This is an application layer protocol that, in its original version, passes all data in the clear (unencrypted). There is a version of ICCP, Secure ICCP, which applies application-level encryption to the data. Secure ICCP, if properly implemented, will prevent both unauthorized disclosure and unauthorized modification of the ICCP data stream. However, before you decide to implement Secure ICCP, I recommend that you read the Secure ICCP paper by Pacific Northwest National Laboratory (PNNL) referenced in the Applicable Documents sidebar.

If you choose to implement a network protection scheme, such as a virtual private network (VPN), I suggest you consider applying the protections outside of the Electronic Security Perimeter (ESP), if any, to facilitate traffic monitoring at the ESP.

Whatever method you choose to employ to logically protect RTA/RTM data, your data protection plan will need to consider at least these items: protocol selection, encryption strength and key management. In developing this aspect of your data protection plan, it may be helpful to refer to these publications (links in the sidebar):

- Control Systems Communications Encryption Primer: While somewhat dated, this DHS publication is still a good overview of the logical protections available for control system communication paths.
- NIST SP800-77 Guide to IPsec VPNs: This recent NIST document discusses design choices and implementation concerns for a popular protocol used in VPNs.

TOP-003-3 R5 Part 5.3 and IRO-010-2 R3 Part 3.3 both require “A mutually agreeable security protocol.” If the security protocol in use for these communication paths will mitigate the risk of unauthorized modification and unauthorized disclosure, you should be able to incorporate this existing protection into your data protection plan. Remember to document the identification of the security protection (CIP-012-1 Requirement R1 Part 1.1), where the protection is applied (Part 1.2), and the responsibilities of each party subject to the mutual agreement (Part 1.3).

Q&A

Q: If an RC, TOP or BA is supplying read-only State Estimator results to their members as a FYI (and not part of the member's primary RTA), would this communication path need to be protected under CIP-012? Sometimes an entity might say their alternate RTA (when their SE is down) is to use / look at an RC's SE results (that they get live in their control center). Does that put this communication path in-scope, even though it may be defined as FYI or nice-to-know (not need-to-know)?

A: If the communication path originates in the RC, TOP or BA's Control Center, terminates in your Control Center, and contains any of the information classified as RTA/RTM data, then that path must be protected per CIP-012-1. Whether it is put to use as a primary information source, secondary information source, or just a nice-to-have, that data must be protected.

Q: Do paths between Control Centers by the same company (e.g., primary to backup) fall within scope, or is this just Control Centers to other (not the same entity) Control Centers?

A: Communication paths between Control Centers that contain any portion of the identified RTA/RTM data are in scope for CIP-012-1. Ownership of these Control Centers is immaterial except for CIP-012-1 R1 Part 1.3 coordination requirements. By including a separate Part 1.3 for coordination between entities, the Standard makes it clear that communications between Control Centers owned by the same entity are in scope for CIP-012-1 Parts 1.1 and 1.2.

Conclusion

CIP-012-1 is at present the shortest of the CIP Standards, and it is deceptively simple. It will require substantial time and resources to implement this Standard.

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. In particular, if you are planning to implement Secure ICCP you will need to give your staff enough time so that they can perform their work without impacting safety or reliability.

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.

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

Feedback

Please provide any feedback you may have on these articles. I may be reached at lew.folkerth@rfirst.org.