The Lighthouse

Greetings, and welcome to The Lighthouse! I'm Lew Folkerth, and I've been a CIP auditor since before there were CIP audits. I am now Principal Reliability Consultant in the Entity Development department. I will be authoring this recurring column in which we'll explore various CIP issues, including some as yet unanswered questions. I think you'll find the Lighthouse metaphor apt. I can't steer your ship for you! I can only provide guidance and perhaps a fixed point of reference on the sometimes stormy waters of CIP compliance.

Since the CIP Standards are in transition, our primary focus will be the CIP V5 and CIP V6 Standards, although the current version 3 is not off limits. As this is the first column, I'll address some common questions and concerns regarding these Standards. I hope you will send your questions to me at lew.folkerth@rfirst.org, so they can be discussed in future columns.

CIP V5 and V6 are *Results Based Standards*

Q "A Physical Security Perimeter isn't explicitly required to be defined by CIP-006-5. Will I really need to define one when v5 becomes enforceable?"

A Yes, you will. The CIP V5 and CIP V6 Standards are what NERC calls Results Based Standards. Simply put, the Standard specifies the result, not the means of achieving the result.

As an example, CIP-006-5 R1 Part 1.2 requires the use of at least one method of control for physical access into a Physical Security Perimeter. That's the end result being specified, not the means of getting to the end result.

In order for the end result (use one method of access control) to be achieved, you need to know what access you're controlling.

In this case, a Physical Security Perimeter (PSP) is needed as a frame of reference for the access control. Now we need to look at the Glossary definition (capitalized term, remember?) to find that a PSP is a physical border around some things for which access is controlled.

What is actually required, then? Let's take the requirement language apart and consider it piece by piece. I think you will need to demonstrate:

1) That access into the PSP is controlled ("Utilize at least one physical access control");

2) That access is normally denied ("to allow unescorted physical access");

3) That a PSP has been established around the applicable systems ("into each applicable Physical Security Perimeter");

4) That unauthorized access is detected or prevented ("to only those");

5) That individuals gaining access are identified ("individuals");

6) That individuals gaining access are properly authorized ("who have authorized unescorted physical access"); and

7) That all of this is documented ("documented physical security plans" from the base Requirement).

That's a lot for one sentence, but it's a good example of a results based requirement. We'll visit this concept again in future columns.

CIP V6 Development

As I write this, the first draft of the CIP V6 Standards is posted for comment and initial ballot. V6 consists of several Standards that have been revised from v5, plus the second version of CIP-010 and CIP-011. The convention is to call this collection "version 6."

The CIP V6 Standards are modifications of the CIP V5 Standards to address four issues identified by FERC in Order 791:

1) Remove the "identify, assess, and correct" language;

2) Expand the protections for Low Impact BES Cyber Systems;

3) Add protections for transient devices; and

4) Address protection for communication networks.

Seul Choix Point, MI
(Photo: L. Folkerth)

I strongly recommend you review and comment on these Standards if you have not done so already.

Also posted for comment, but not for ballot, is the first draft of the RSAW for each of the v6 Standards. The NERC website includes links to the draft RSAWs and an email address for comments. If the comment period has closed by the time you read this, send your comments to me and I will get them to the RSAW authors.

Please Submit Questions

If you have questions or topics you would like to see addressed in this column, please send me an email at lew.folkerth@rfirst.org.

October CIP V5 Workshop

RF is conducting a CIP V5 Workshop on October 2-3, 2014, in Cleveland. The agenda is posted here, and the registration page is here. I hope to see you there!

The Lighthouse

By: Lew Folkerth, Principal Reliability Counsultant

Q My company does not have Critical Assets under CIP-002-3, but will probably have medium impact BES Cyber Systems under CIP-002-5.1. How and when should I start working on compliance with CIP?

A The "when" part of your question is easy—start now! CIP version 5 is the second generation of CIP and in many areas is more demanding than the first generation (versions 1, 2, and 3).

In organizing your work, let me suggest that you start with CIP-002-5.1. Identify any high, medium, and low impact BES Cyber Systems. For now, focus your efforts on the high and medium systems. You may want to wait until CIP-003-6 is close to approval to do any significant work on the low impact systems. You'll have an extra year to implement compliance for the low impact systems.

CIP-002-5.1 R1 does not specify an approach for identifying BES Cyber Systems. (See June's column for a discussion of results-based Standards.) Two approaches to identification are being discussed by the industry—top-down and bottom-up.

If you take the top-down approach, your process will look something like this:

1. Determine those assets that could contain high or medium-impact BES Cyber Systems (see Attachment 1 in CIP-002-5.1);
2. Identify the BES Reliability Operating Services (BROS) that apply to a specific asset (see Guidelines and Technical Basis in CIP-002-5.1);
3. Identify the BES Cyber Assets that support the BROS for each asset; and
4. Group the BES Cyber Assets into BES Cyber Systems.

If you take the bottom-up approach, you will:

1. Identify all of your Cyber Assets;
2. Evaluate each Cyber Asset as a possible BES Cyber Asset; and
3. Group BES Cyber Assets into BES Cyber Systems.

Hybrid approaches are possible, and some companies may elect to perform both approaches to ensure nothing is missed.

If you would like more information on identifying BES Cyber Systems, here are some references that may help:

http://www.spp.org/publications/Identifying BES Cyber Systems Webinar Updated 6-16-14.zip; and

http://www.wecc.biz/compmtg/20140514/Lists/Presentations/1/2%20-%20CIP-002 May V5 SLC.pptx

Once you have your high and medium impact BES Cyber Systems identified, I suggest you make a project plan for the remaining CIP Standards based on the estimated time to implement each Standard and Requirement.

You should also allow for time in your project plan to practice your process for some of the more detailed Requirements before going live. For example, I would start working on CIP-010-1 R1 (Configuration Change Management) very early in your implementation. It will take a lot of time to get this one right. Another requirement that may need a lot of lead time is CIP-007-6 R2 (Security Patch Management).

Q What does it mean to "identify" a BES Cyber System?

A The NERC Glossary defines a BES Cyber System as "one or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." You should document each BES Cyber Asset and Cyber Asset that makes up the BES Cyber System. I also suggest documenting the reliability tasks each BES Cyber System performs.

An audit team is going to want to see not only the resulting list of BES Cyber Systems, but also how you determined that list. Document each step of your process and show your work. The process you follow should be repeatable, such that anyone who follows your process will reach the same conclusion.

There are some fine points you may want to consider when identifying BES Cyber Systems. Note that the definition of BES Cyber Asset includes the phrase, "each BES Cyber Asset is included in one or more BES Cyber Systems." This implies that you have flexibility in identifying your BES Cyber Systems. Also, you are not prohibited from including Cyber Assets that are not BES Cyber Assets in a BES Cyber System.

Copper Harbor, MI
(Photo: L. Folkerth)

If there is interest, we may explore this flexibility in a future issue.

Please Submit Questions:

If you have questions or topics you would like to see addressed in this column, please send me an email at lew.folkerth@rfirst.org.

October CIP v5 Workshop

ReliabilityFirst is conducting a CIP v5 Workshop on October 2 – 3, 2014, in Cleveland. Click here to register for the workshop.

I hope to see you there!

The Lighthouse

By: Lew Folkerth, Principal Reliability Counsultant

CIP Version 5 (and beyond) Navigation Aids

I recently had occasion to realize just how hard it is to keep up with the changing seas of CIP v5/v6/vX compliance. In this third issue of The Lighthouse, I'll point out the essentials you need to know if you're a CIP professional.

Version Complexity

As I write this in early September 2014, CIP v5 is approved and will be effective April 1, 2016. However, FERC Order 791 requires several changes before CIP v5 goes into effect, which will change the version numbers on some of the CIP Reliability Standards. At this time, it looks like CIP v6 will address removal of the “identify, assess, and correct” language and will add consideration of communication networks.

The two other changes required by Order 791 are additional protections for low impact BES Cyber Systems and controls for transient Cyber Assets and removable media, and will be added in a later version, currently called Version X (but probably Version 7). The Version X notation is used in case the additional language passes the next ballot. If the language passes, then it will be incorporated in Version 6. If it does not pass, then it will be worked on as Version 7 while the other topics go to final ballot as Version 6. This is being done in order to meet FERC’s one year deadline for filing for the low impact and communication networks issues.

When reading the Reliability Standards, it is important to understand that only the language of the Requirement can be enforced. The other parts of the standard, such as the Background, Rationale, Guidance, Measures, and Technical Basis sections, can inform our understanding of the Requirement, but are not directly enforceable.

Two other documents, the Implementation Plan for Version 5 CIP Cyber Security Standards (IPv5)and Glossary of Terms Used in Reliability Standards (Glossary), are approved by FERC. The Ipv5 governs the effective date and other conditions regarding the transition to the CIP v5 Standards. The Glossary defines certain terms used in the Reliability Standards. Be aware that much of the content of the CIP v5/v6/vX standards resides in the Glossary.

Transition Documents

While the Standards, Glossary, and IP v5 are the FERC-approved documents that govern cyber security compliance, other documents guide our understanding of what the Standards mean, how they will be applied and enforced, and how the transition to the new Standards will be accomplished.

CIP v5 Transition Guidance describes how the shift to CIP v5 will be accomplished. The plan covers relaxation of the CIP v3 Requirements while the move to CIP v5 is underway. It does not lessen the strength of the controls that must be in place, but does let entities shift to the new Requirements without incurring a risk of violation of the CIP v3 standards. See CIP v5 Transition Guidance on page 5 of this Newsletter, for more information.

During 2013 and early 2014, several entities voluntarily participated in a transition study. The results of that study will be published as a series of “Lessons Learned,” which will further guide how the CIP v5 Standards are understood and enforced. Look for these on the NERC web site as they are released. You should pay close attention to these, as NERC and the Regions are committed to abide by them, and they should provide answers to some of the tougher problems presented by CIP v5.

Compliance Documents

On another note, the RAI will affect the way the CIP v5 standards are enforced. NERC and the Regions continue to develop the RAI and will communicate what the RAI is and how it will affect compliance monitoring as that understanding matures.

Au Sable Point, MI
(Photo: L. Folkerth)

Meanwhile, NERC has posted the 2015 ERO CMEP (Implementation Plan) on its web site. While this plan does not cover implementation of the Standards, it does cover the implementation of the compliance monitoring program. The Implementation Plan shows how the RAI will begin to be implemented and guides the Regions in what and how to audit for the year, using a risk-informed process to develop entity specific compliance monitoring scope.

Education

The Regions and NERC will continue to host Workshops, Seminars, Webinars, etc. to clarify various issues surrounding the conversion to CIP v5 and later Standards. ReliabilityFirst will hold a CIP v5 seminar in October in conjunction with the Fall Compliance Workshop. See www.rfirst.org for more information.

Please Submit Questions

If you have questions or topics you would like to see addressed in this column, please send me an email at lew.folkerth@rfirst.org.

The Lighthouse

By: Lew Folkerth, Principal Reliability Counsultant

The Role of the CIP Senior Manager

Q Does the role of the CIP Senior Manager change in CIP v5?

A There are two answers to this question. The first involves the actual language of the Standard. The second involves what is called the "spirit" of the Standard – a concept that goes beyond the language of the Standard and raises an entity's posture when it comes to CIP security and compliance. As we move forward with RAI, we may see an entity's understanding and incorporation of the "spirit" of the Standard assessed and used to help determine the strength of an entity's security posture and the maturity of its compliance program.

The Language of the Standard

In CIP v5, an entity must designate a CIP Senior Manager (CIP-003-5 R3). The CIP Senior Manager has four specific duties:

1. Approve delegations of authority, if any (CIP-003-5 R4);
2. Periodically approve identification of BES Cyber Systems (CIP-002-5 R2);
3. Periodically approve cyber security policies (CIP-003-5 R1, R2); and
4. Approve, as needed, extensions to patch management mitigation plans (CIP-007-5 R2 Part 2.4).

From the perspective of the language of the Standard, not much changes in CIP v5. The entity must designate a CIP Senior Manager and the CIP Senior Manager has a few approval duties. So, why does CIP v5 retain this concept if the CIP Senior Manager has so few enforceable duties? To answer this question, we need to talk about the reason this concept of a single accountable person came to be, and the CIP Senior Manager's implied duties. In other words, we need to talk about the "spirit" of the Standard.

The "Spirit" of the Standard

The designation of a management official to be responsible for an entity's cyber security program has been included in every version of the NERC cyber security standards. The best explanation for this may be the Commission's determination in FERC Order 706, page 381:

> "The Commission adopts its CIP NOPR interpretation that Requirement R2 of CIP-003-1 requires the designation of a single manager who has direct and comprehensive responsibility and accountability for implementation and ongoing compliance with the CIP Reliability Standards. The Commission's intent is to ensure that there is a clear line of authority and that cyber security functions are given the prominence they deserve."

With this background in mind, let's take a close look at the new Glossary definition of CIP Senior Manager, which is applicable to CIP v5 and future versions:

> "A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011."

"A single senior management official" - This wordingpermits an entity to designate just about anyone, but entities should do this carefully. The designation of the CIP Senior Manager may be the most important single decision in an entity's compliance program.

"[O]verall authority and responsibility" - The intent of this phrase is that only one person has accountability for CIP compliance. In effect, any failure of the compliance program is, in some way, a failure of the CIP Senior Manager. This makes clear the requirement for the entity to place the manager high enough in the organization so that every facet of the CIP compliance program is under the manager's authority. This helps to prevent or coordinate compliance "silos", where differing business units have what amounts to separate compliance programs. It also requires that the CIP Senior Manager's authority span all of the business units at an entity.

Crisp Point, MI
(Photo: L. Folkerth)

"[L]eading and managing" - The CIP Senior Manager is expected to be the head of the corporate CIP compliance program. The designated person is expected to be both a leader and a manager, to both inspire others and to be certain that the job is done using the appropriate resources across the entity.

"[I]mplementation of and continuing adherence to the requirements" of the CIP Standards - Implementation gains renewed importance with the impending CIP v5 Standards. How and when will the entity transition to the new Requirements? Which processes will be replaced and what new processes are required? And, for "continuing adherence," how will we implement these Requirements in a sustainable and auditable manner?

CIP Senior Manager Duties Implied by the "Spirit" of the Standard

With the above discussion in mind, we can now suggest additional duties a CIP Senior Manager might perform. Keep in mind that these duties are not enforceable, but they are good business practice based upon entities that, from RF's perspective, have a successful CIP compliance program.

Continued on page 12

Continued from page 11

Cyber Security Policy

The CIP Senior Manager is required to approve the cyber security policy and this approval may not be delegated. This is because the cyber security policy is the core of any CIP compliance program. It is the tool the CIP Senior Manager is given to lay out the strategy used to address the CIP Standards. For example, the part of the policy that addresses CIP-005-5 R2.3 might say, “Multi-factor authentication is required for all Interactive Remote Access sessions.” But this wording simply paraphrases the requirement, which does not communicate a specific management approach to this action.

As an alternative, consider the following: “Interactive Remote Access will be permitted only upon demonstrated business need. Two factor authentication will be used for all remote sessions. Remote sessions which access medium impact systems will use something the user knows (e.g., username/password) and something the user has (e.g., hardware token). Remote sessions which access high impact systems will use something the user knows and something the user is (e.g., fingerprint).”

Rather than paraphrasing the requirement, this shows how the entity views and implements the Requirement.

Also, importantly, an entity cannot create the cyber security policy in a vacuum. While the vision should be established by the CIP Senior Manager, everyone from the CIP Senior Manager to the Subject Matter Expert (SME) doing the actual work should be involved in the policy development, with sign-off by the CIP Senior Manager.

Representative to Executive Management

A successful compliance program requires support from the highest levels of the organization. The CIP Senior Manager should be the representative of the CIP compliance program to the organization's executives and board. The CIP Senior Manager should ensure that these people are informed about cyber security and how the organization is addressing these challenges and risks.

Oversee Internal Controls

As the RAI gains traction, it will be very important to demonstrate that your controls over CIP processes are robust. An internal control should answer these questions:

- Are my compliance processes well designed and will they result in outcomes consistent with my business needs?
- Are my compliance processes being executed correctly and completely?
- Are compliance artifacts (evidence) available to show each time a compliance process is executed?
- If there is a process failure, is the immediate failure corrected?
- If there is a process failure, is the root cause identified and addressed?
- If there is a process failure, is the failure properly recorded and reported and the process adjustments/enhancements made to prevent recurrence?

The CIP Senior Manager should be the force driving the creation and tuning of these internal controls. More information on internal controls can be found on the RAI page of the NERC web site.

Manage External Relationships

The CIP Senior Manager should be the champion of your CIP program not only to the executive ranks, but to external entities as well. A good relationship with the Regions and NERC, especially understanding and participating in the RAI program, will prove very valuable.

Make the Standards Work FOR You

The CIP Senior Manager must ensure that the entity is using its resources in the most efficient and effective way. The best way to accomplish this is to leverage the CIP Standards to improve the entity's security posture. Let me offer an analogy. Think of your cyber security program as a ship you're steering and you've set the best course for the security program. CIP compliance is a tugboat moored to your ship. The tug can be a passive load, slowing down the ship or even actively pulling it off course. Or the tug can be pulling in the same direction the ship is headed, actively helping move the ship in the right direction.

Such is the CIP compliance program. We have seen CIP compliance programs that were a drag on the entity's resources with little contribution to actual cyber security and even programs that were harmful to the cyber security stance, siphoning resources that could be better used elsewhere. And we have seen CIP compliance programs that are integrated into the cyber security program, furthering the ends of the cyber security program and so seamlessly integrated that you can't tell where one stops and the other begins. Which of these alternatives is the best use of company resources?

Feedback

Please let me hear any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached at lew.folkerth@rfirst.org.

The Lighthouse

By: Lew Folkerth, Principal Reliability Counsultant

Non-Prescriptive Standards

Q: How can I comply with a Standard I don't understand? (Full disclosure: This is really a composite question asked many times by many entities about many different areas in the CIP Version 5 (CIP v5) Standards and in certain cases associated with the operations and planning standards.)

A: Drafting a Reliability Standard is a balancing act between using plain, commonly understood language, and precise, overly prescriptive language. The CIP v5 Standard Drafting Team chose to avoid being overly prescriptive, and not all terms used are defined in the Standard itself.

In CIP v5, there are many examples of this. NERC formed the CIP Version 5 Advisory Group (Advisory Group) to identify Frequently Asked Questions (FAQs) (and there are a lot) and Lessons Learned to address the major questions.

However, it is important to understand that even when the Advisory Group issues FAQs or Lessons Learned to clarify an issue, these should be considered as Reference documents per NERC Rules of Procedure Appendix 3A Section 11. As such, they do not modify the Standard and are not themselves enforceable. Rather, these documents serve as guidance and make an effort to share our understanding of the Standards, but, ultimately, the plain language of the Standard is what governs.

Additionally, the CIP v5 Standard Drafting Team, in a departure from the normal standard drafting process, did include rationale, measures, guidelines, and technical basis sections in the Standards to help with understanding them. These inclusions help in many areas, but should also be considered only guidance.

Given the nature of the CIP v5 Standards, how should an entity approach compliance?

Let me suggest a process to follow to help entities apply the Standards to their own unique circumstances:

1. Determine what the Requirement intends to accomplish in the context of the entity, and how the entity will address this intent.
2. Document this determination and the reasoning behind it, incorporating references to the language of the Requirement, any reference documents, such as FAQs or Lessons Learned, any published guidance, and industry best practices.
3. Build and document your processes, procedures, protocols, and internal controls based on the above determinations.
4. Document the implementation of and ongoing adherence to your processes, procedures, protocols, and internal controls including the associated compliance evidence.

Let's work through an example. CIP-010-1 (and -2) R1 Part 1.1 uses the term “software” in two locations, Part 1.1.2 and Part 1.1.3. CIP-010-1 Part 1.1 requires the development of a baseline configuration which must include certain components. For purposes of this article, I will focus on Part 1.1.3, which reads, “Any custom software installed.”

What is software? The Standard doesn't provide a definition, but the dictionary tells us that software is a set of programs, and a program is a set of coded instructions. The dictionary definition does not limit how large or how small a program can be. Anything from the operating system down to a one-line script seems to qualify.

Whitefish Point, MI
(Photo: L. Folkerth)

Here's where we hit the problem. Incorporating every single executable piece of code, including the smallest scripts, into the CIP-010-1 R1 baseline, and subsequently tracking and managing each one, may consume huge amounts of resources with little or no benefit to reliability. Is this really what the Requirement intends to accomplish?

To resolve this, let's implement the four step process above.

Step 1

Determine what the Requirement intends to accomplish in the context of the entity, and how the entity will address this intent.

CIP-010-1 R1 did not spring into being in a vacuum. It was built on well-recognized security practice, and in this case the principle that “You must know what you have before you can protect what you have.” A good reference for us is the DOE/DHS “Electricity Subsector Cybersecurity Capability Maturity Model” (ES-C2M2).

Section 7.2 of the ES-C2M2 covers Asset, Change, and Configuration management. This section talks about defining baselines to ensure similar systems are configured in a similar manner. Changes should be managed to prevent introduction of vulnerabilities

Continued on page 9

The Lighthouse

Continued from page 8

to these systems.

We can work with this. Let's create a statement explaining our understanding of the intent of the Requirement:

CIP-010-2 R1 Part 1.1.3: Custom software is intended to include any programs, libraries, modules, or scripts, that are not identified in Part 1.1.2, that can be used to introduce a vulnerability into an Applicable System.

So, how does this explanation apply in our example? We can say that, for our purposes, "custom software" includes:

- A program or system of programs that affects a reliability function of the BES Cyber System. For example, if an entity develops its own state estimator, such a system would affect the reliability of the BES;
- A program that is intended to run with elevated privileges. Administrative scripts fit this description.
- A program that runs on a scheduled basis.

This is not an exhaustive list. My point here is not to try to define "custom software" as applied to you, but rather, it is to show you what the process of applying the Standard to your entity might look like.

Step 2

Document this determination and the reasoning behind it, incorporating references to the language of the Requirement, any reference documents, such as FAQs or Lessons Learned, any published guidance, and industry best practices.

The documentation should include the reference to the ES-C2M2 as a best practice, and any other reference source used in the determination. The more references that can be cited, the better.

The documentation should also include a discussion of how the reference material applies to you and your specific processes.

Step 3

Build and document your processes, procedures, protocols, and internal controls based on the above determinations.

These processes, procedures, protocols, and internal controls should incorporate the determinations made in Step 1. Implementations of these determinations should be made as if that Standard actually included your determinations. The processes, procedures, protocols, and internal controls should use clear wording.

Internal controls should be designed to answer these questions:

- How do you know your processes have been implemented correctly?
- How do you know a process will be performed every time it is needed?
- How do you know a process will be performed as intended?
- What compliance evidence needs to be preserved for your processes?
- When a deficiency in the performance of a process is detected, is the deficiency documented, is the deficiency's risk assessed, is the deficiency corrected in a manner appropriate to the risk, and is the deficiency corrected in a time frame appropriate to the risk?
- When a deficiency in the performance of a process is detected, is the cause of the deficiency identified, corrected, and documented, and is the risk assessed and documented?
- Are any deficiencies reported to the appropriate Compliance Enforcement Authority (CEA) in the manner established by the CEA?

Step 4

Document the implementation of and ongoing adherence to your processes, procedures, protocols, and internal controls including the associated compliance evidence.

The documentation related to the points above should be kept for Internal Controls Evaluations and for compliance monitoring (i.e., audits, spot checks, etc.). Any automated tool used for this purpose should be able to generate an audit trail.

Summary

Your determinations in Step 1 should be reviewed periodically and you should define this review period in your process documentation. Additional information, such as new FAQs or Lessons Learned, may become available that may support or change the determinations.

Keep in mind that this process is not guaranteed. Much depends on how you implement these steps.

Feedback

Please let me hear any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached at lew.folkerth@rfirst.org.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Compliance Approach for CIP-002-5.1

Q how can I make sure my compliance program is on track, and that I am not spending too many or too few resources on compliance?

A NERC's CEO stated that for CIP Version 5(CIP v5) he wants to prevent the "bow wave" of violations that occurred with CIP version 1. I was in the middle of that "bow wave," first at an entity preparing for CIP compliance, then at RF as a CIP auditor involved in the first round of CIP Spot Checks and CIP Audits. RF fully agrees that preventing this "bow wave" is the desirable outcome and we are working with NERC to prevent that with CIP v5.

This article is the first in a series that will discuss a recommended "Compliance Approach" to some of the CIP requirements. Let me begin this discussion by saying that blindly following the recommendations here will NOT ensure compliance or a desirable audit outcome. You, as the Registered Entity, must apply these approaches to your specific circumstances. No one can tell you how to be compliant. You must chart your own course, perhaps referring to that point of light on the shore to help you find your way.

While I call what follows a "Compliance Approach," you will find my recommendations may go beyond compliance. In general, each "Compliance Approach" will include these topics:

- Discussion of the language of the Requirement or Part;
- Some of the topics your processes and procedures should address;
- Suggested evidence to be collected and retained for demonstrating compliance;
- The "Compliance Approach" itself, which will be adapted from the original Draft 1 RSAW Compliance Assessment Approaches;
- A discussion of best practices regarding compliance;
- Tips for the CIP Senior Manager on how to manage compliance and security appropriate to the Requirement or Part; and
- References to available guidance.

CIP-002-5.1 R1

Discussion of the Language

CIP-002-5.1 R1 requires that you identify the cyber systems that can have a real-time impact on the reliable operation of the BES. Much of R1 is contained in the Glossary definitions. Be sure to read these definitions carefully:

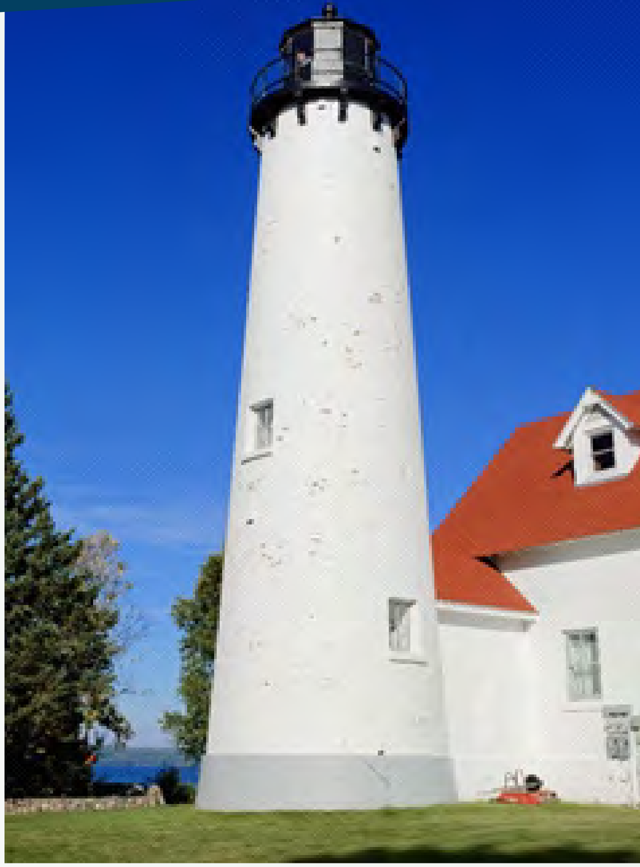
- Cyber Asset
- BES Cyber Asset
- BES Cyber System

I analyzed the language of the Requirement in a presentation for RF's Fall 2014 CIP Compliance Workshop. Here a link to the slide deck.

In working with the language of R1, Attachment 1, and the Glossary, it is important to note that not all terms are defined. In the absence of other guidance (see References below), refer to the process I proposed in my previous column.

Considerations for Processes and Procedures

R1 requires the "implementation of a process," which has specific components. Implementation of the process must result in the identification of each high or medium impact BES Cyber System, and each asset that contains a low impact BES Cyber System. BES Cyber Systems may be located at any of the six classes of asset listed. BES Cyber Systems are identified according to the criteria in Attachment 1.


Iroquois Point, MI
(Photo: L. Folkerth)

There are many supporting documents to assist in developing a process for identifying BES Cyber Systems. I suggest you use these only as source material for your own process, and do not adopt any process blindly. Here are some that I am aware of:

- SPP RE Identifying BES Cyber Systems
- WECC Road Show

Continued on page 9

The Lighthouse

Continued from page 8

A simple Google search (try searching for "CIP-002-5.1 identification assets") will identify many others.

Suggested Evidence

The evidence presented to an audit team should show each step of the process to identify the high and medium impact BES Cyber Systems. Here is a suggested (not all inclusive) list of items that you should be prepared to present:

- The process implemented per R1 that considers each of the asset types listed in R1 (i through vi) to identify and assign an impact rating to BES Cyber Systems.
- A list of all assets for which you are responsible for compliance for this Requirement, per CIP-002-5.1 Section 4, Applicability. This list should include the following information:
  - Identification (name, number, etc.) of the asset.
  - The type of asset (generation resource, substation, etc.).
  - A description of any compliance responsibility shared with another Registered Entity.
  - If the asset was commissioned during the audit period, the date of commissioning.
  - If the asset was de-commissioned during the audit period, the date of de-commissioning.
- A list of all high impact BES Cyber Systems identified, and the asset(s) where the BES Cyber System is located.
- A list of all medium impact BES Cyber Systems identified, and the asset(s) with which the BES Cyber System is associated.
- A list of all assets that contain a low impact BES Cyber System.
- For each high and medium impact BES Cyber System, a list of BES Cyber Assets (and Cyber Assets that are not BES Cyber Assets, if any) that are logically grouped to comprise the BES Cyber System.
- Evidence that the process required by R1 was implemented to determine the list of high and medium impact BES Cyber Systems. In other words, evidence that you followed your own process.
- Evidence that the process required by R1 was implemented to determine the list of assets containing low impact BES Cyber Systems.
- For assets that do not contain a BES Cyber System, evidence that the process required by R1 was implemented and resulted in a determination of no BES Cyber Systems.
- The rationale for the determination of the impact rating of each BES Cyber System. (Usually a reference to the criteria in Attachment 1.)

Compliance Approach

Be able to show that the process implemented per R1 considers each of the asset types listed in R1 (i through vi) to identify and assign an impact rating to BES Cyber Systems. Be able to demonstrate the following:

- The process considers each of the asset types listed in R1 (i through vi).
- The process contains provisions to ensure that all assets of each applicable type are considered.
- The process identifies all high and medium impact BES Cyber Systems at each asset.
- The process assigns the correct impact rating to each identified high and medium impact BES Cyber System at each asset.
- The process identifies all assets that contain a low impact BES Cyber System.

Be able to show that you have implemented the process for each of your assets, and that:

- The high impact BES Cyber Systems used by and located at each asset have been identified.
- The medium impact BES Cyber Systems associated with each asset have been identified.
- The assets that contain a low impact BES Cyber System have been identified.
- As always in demonstrating compliance, show your work! If you didn't document it, you didn't do it.

Best Practices

Be able to demonstrate that your compliance with CIP-002-5.1 is firmly based on the reliability of the

Continued on page 9

Continued from page 9

BES. If you are able to show that each decision in the process to identify BES Cyber Systems is made with reliability as the primary consideration, you will enhance the strength of your process.

Be able to show how you applied each of the criteria in Attachment 1. For example, did you apply Criterion 2.5 at the asset level or at the Facility level? Is the Criterion applied in a way that best supports the reliability of the BES?

Managing Compliance to CIP-002-5.1

As the CIP Senior Manager, you or your delegate will need to approve the identification of high and medium impact BES Cyber Systems, and the identification of assets containing low impact BES Cyber Systems. This approval needs to occur on or before April 1, 2016, and once each "CIP year" (15 months) afterward.

I suggest you do not delegate the first approval, and only delegate the annual approvals if you must.

In order for this approval to mean anything, you should have an understanding of the process your subject matter experts (SMEs) go through to create the identifications. A good way to obtain this understanding is for your SMEs to explain it to you in the same way they would explain it to an audit team. I suggest a meeting with your SMEs where they present the BES Cyber System identification process to you in a manner similar to the way they will present it to an audit team. Here's what such a meeting might look like:

CIP Senior Manager's Homework (prior to the meeting):

- Obtain a copy of CIP-002-5.1
- Obtain a copy of the NERC Glossary
- Read the Glossary definitions of Cyber Asset, BES Cyber Asset, and BES Cyber System
- Read the requirement language of R1 and R2
- Read Attachment 1

Meeting Agenda (about 1 hour):

- SMEs explain the process used to comply with R1. This will include a walkthrough of the process and a general explanation of how it is implemented. The walkthrough should include any assumptions used in the process, including how the criteria in Attachment 1 were interpreted and applied by your SMEs. (10 minutes)
- SMEs explain how the process is applied to each type of asset (e.g., Control Center, substation, generator, etc.). (15 minutes)
- SMEs present the resulting identification of high and medium impact BES Cyber Systems and assets containing low impact BES Cyber Systems. (5 minutes)
- The CIP Senior manager chooses one of each type of asset. The SMEs present the work papers for each of these assets. The CIP Senior manager reviews these work papers for consistency and completeness. (20 minutes)
- The CIP Senior Manager questions any shortcomings or inconsistencies in the presentations. Any questions that cannot be immediately answered become remediation items for the SMEs. (15 minutes)

If you hold such a meeting, it will look very much like an audit team interview. The point of the meeting is to ensure your SMEs' processes and presentations form a consistent story to an audit team. It is important be very critical of inconsistencies or apparent gaps in coverage. If you have questions, an audit team will have questions.

You may want to invite a representative from your company's Internal Audit team to this meeting to provide constructive feedback about the presentation and quality of SME evidence including the process and assessment for identification of BES Cyber Systems.

I strongly suggest that you hold this meeting as early as possible in the compliance process in order to give your SMEs time to remedy any gaps identified.

References

CIP-002-5.1

NERC Glossary

'NERCs "Implementation Study, Lessons Learned, and FAQs" Web Page

Feedback

Please let me hear any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached at lew.folkerth@rfirst.org.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Compliance Approach for CIP-005-5 R1

We continue the series of compliance approaches that began in the previous issue with a discussion of CIP-002-5.1 R1. While I call what follows a "Compliance Approach," you will find my recommendations may go beyond compliance. Blindly following the recommendations here will NOT ensure compliance or a desirable audit outcome. You, as the Registered Entity, must apply these approaches to your specific circumstances. No one can tell you how to be compliant. You must chart your own course, perhaps referring to that point of light on the shore to help you find your way.

CIP-005-5 R1 - *Discussion of the Language*

I won't repeat the language of CIP-005-5 R1 here. The base Requirement and its five Parts are comprised of one sentence each. Each sentence is straightforward with, in my opinion, little or no ambiguity. The ambiguity and ongoing discussion and clarification efforts involve some of the terms defined in the NERC Glossary that are used in this Requirement. These terms, and some of the points under discussion, are:

- BES Cyber System
    - An entity is granted great flexibility in defining its BES Cyber Systems. Where and when is this flexibility useful? What are the pitfalls to consider when exercising this flexibility?
- Cyber Assets
    - What does "programmable electronic device" really mean?
- External Routable Connectivity
    - When is a routable connection "bi-directional" and, more importantly, when is it not?
    - Under what circumstances can a serially connected device be considered to be accessible via bi-directional routable protocol connection?
- Electronic Access Point
    - What are the implications of the access point being defined as an "interface?"

Control Center

- Does the ability to remotely start a generator from the control room of a different generator make that control room a Control Center?

I don't answer those questions in this article. I list them here to inform you that there are ongoing discussions regarding these issues. Please follow the development of the Frequently Asked Questions (FAQs) and Lessons Learned on the NERC web site. If you would like me to address any of these issues in a future article, please see the "Feedback" section below.

This article will deal with Cyber Assets associated with high and medium impact BES Cyber Systems, unless low impact BES Cyber Systems are explicitly mentioned. I will discuss low impact BES Cyber Systems in a future article, probably after FERC acts on CIP Version 6.

Little Sable Point, MI
(Photo: L. Folkerth)

Considerations for Processes and Procedures

There has been considerable confusion over the identification and classification of the Cyber Assets to be protected by the Version 5 (and 6) CIP Standards. Cyber Assets for which the CIP Standards are applicable may fit one or more of these classifications:

- A component of a BES Cyber System;
- An Electronic Access Control or Monitoring System (EACMS);
- A Protected Cyber Asset (PCA);
- A Physical Access Control System (PACS).

Let's first cover these components and determine when and how to identify them.

Step 1: Identify BES Cyber Systems and BES Cyber Assets (per CIP-002-5.1 R1)

The first step in identifying the Cyber Assets to be protected is to identify your BES Cyber Systems as required by CIP-002-5.1 R1. After completing CIP-002-5.1 R1 you will have a list of your BES Cyber Systems and the BES Cyber Assets (and, optionally, Cyber Assets) that comprise the BES Cyber Systems. Also, you will have assigned an impact rating to each BES Cyber System.

Step 2: Identify the Cyber Assets that are required to reside within an Electronic Security Perimeter (ESP)

Those Cyber Assets of high and medium impact BES Cyber Systems that are connected to a network with a routable protocol are required to reside within an ESP. This is separate from the concept of External Routable Connectivity.

Step 3: Identify Electronic Security Perimeter(s) around each of the Cyber Assets identified in Step 2

In this step you will define the "logical border" enclosing each of the Cyber Assets you identified in the previous step. You can have as many ESPs as you choose. Make sure that every Cyber Asset of every high and medium impact BES Cyber System that is

Continued on page 9

The Lighthouse

Continued from page 8

connected to a network with a routable protocol is protected by an ESP.

Step 4: Identify any Protected Cyber Assets (PCA)

Once the ESP is defined, identify any additional Cyber Assets connected to the ESP network that are not part of a BES Cyber System. These Cyber Assets must either be relocated outside of the ESP, or they must be identified as PCA.

In addition, any Cyber Asset of a BES Cyber System that is not part of the highest rated BES Cyber System within the ESP must be designated as a PCA associated with the highest rated BES Cyber System. For example, if an ESP contains both medium and low impact BES Cyber Systems, then the Cyber Assets of the low impact BES Cyber Systems must be identified as PCA associated with a medium impact BES Cyber System.

Step 5: Identify the Electronic Access Point(s) (EAP) for each ESP

If any Cyber Asset within an ESP can be accessed from outside the ESP via a bi-directional routable protocol connection, then you must identify one or more EAPs for this traffic. Note that the EAP is an "interface" of a Cyber Asset. This is a significant change from CIP-005-3. Any Cyber Asset that has an interface designated as an EAP must be identified as an EACMS for use in Step 7.

Step 6: Identify the methods and systems used for Interactive Remote Access

If you are going to permit Interactive Remote Access into your ESPs, you need to identify the Cyber Assets that will be used for this purpose. Any Cyber Asset used as part of an Intermediate System must be identified as an EACMS for use in Step 7.

Step 7: Identify the Electronic Access Control or Monitoring Systems (EACMS) associated with each ESP

Any Cyber Asset that is used for electronic access control or for electronic access monitoring must be identified as an EACMS. This will include firewalls or other network devices that host an EAP, components of Intermediate Systems, authentication systems, intrusion detection systems, or any other system that meets the definition.

Step 8: Identify the Physical Security Perimeter (PSP) surrounding each ESP (per CIP-006-6 R1)

Identifying, at least at a general level, the PSPs lets us identify the Physical Access Control Systems in Step 9. The details of identifying the PSPs must be left for a discussion of CIP-006-6.

Step 9: Identify the Physical Access Control Systems (PACS) for each PSP

Any Cyber Asset that controls, alerts, or logs access to a PSP must be identified as part of a PACS.

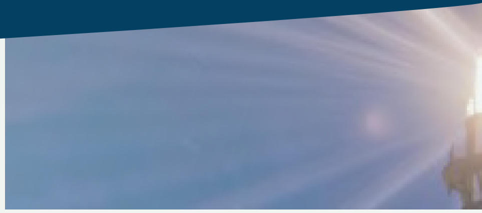
Step 10: Identify the BES Cyber Systems with special attributes

Some Requirements only apply to BES Cyber Systems or associated Cyber Assets with special attributes. The BES Cyber Systems with these attributes must be identified so that the appropriate Requirements are applied.

> *External Routable Connectivity*
>
> These are the Cyber Assets that communicate outside of an ESP with a bi-directional routable protocol. This is not a simple determination, and a Lessons Learned document is being prepared to provide additional clarification.
>
> *Dial-Up Connectivity*
>
> If a BES Cyber System is accessible via a dial-up connection (modem and phone line, or equivalent) this constitutes dial-up connectivity.

Step 11: Identify any medium impact BES Cyber Systems (and associated EAP) at Control Centers

If a medium impact BES Cyber System or an associated PCA is at a Control Center, then it must be identified, as additional Requirements apply.



Suggested Evidence

Your compliance evidence should include the process used to identify your Cyber Assets within the scope of CIP compliance, and any applicable attributes (such as External Routable Connectivity), per the steps above. Note that Steps 1 and 8 could reside in the processes for CIP-002-5.1 R1 and CIP-006-6 R1, respectively.

You should be prepared to show that you followed this process to create your list of in-scope Cyber Assets.

You should also be able to show the outcome of your process. I suggest keeping the outcome in a spreadsheet or database table with one row for each in-scope Cyber Asset. I suggest maintaining the following information, at a minimum, for each row in the table:

- Cyber Asset identifier (this identifier should also be clearly marked on the Cyber Asset to facilitate audit review)
- Type of Cyber Asset (server, workstation, switch, firewall, etc.)
- If part of a BES Cyber System:
  - BES Cyber System identifier
  - Impact rating of BES Cyber System
  - Is the Cyber Asset connected to a network via a routable protocol?
- Asset type (Control Center, Transmission substation, etc.)
- If within an ESP, the ESP identifier
- If within a PSP, the PSP identifier
- Classification of Cyber Asset (BES Cyber Asset, Cyber Asset of a BES Cyber System, EACMS, PACS, PCA)
- Vendor (Dell, Cisco, etc.)
- Model
- Operating System (Windows Server 2008, IOS 15.4, etc.)
- If this is a guest on a virtual system:

Continued on page 10

Continued from page 9

  - The type of virtualization (VMware ESX, etc.)
  - Physical host identifier
- Deployment date, if deployed within the audit period
- Indicators (yes/no) for:
  - Dial-up Connectivity
  - External Routable Connectivity
- If information is for multiple registered entities, indicate the entity responsible for compliance

For each ESP, identify all Electronic Access Points.

For each Electronic Access Point, provide:

- The list of inbound access permissions
- The list of outbound access permissions
- The reason for granting access for each of the inbound and outbound permissions
- Evidence that all other access is denied by default

For each in-scope Cyber Asset with Dial-up Connectivity, provide:

- Evidence that authentication is performed when establishing a connection, or
- A reference to an approved Technical Feasibility Exception (TFE) covering this Part and this Cyber Asset

For each Electronic Access Point for a high impact BES Cyber System or a medium impact BES Cyber System at a Control Center, provide evidence of one or more methods of detecting malicious communications.

Compliance Approach

For all high and medium impact BES Cyber Systems, be able to show that all BES Cyber Assets, and all Cyber Assets that are part of a BES Cyber System, that are connected to a network via a routable protocol, are identified and are protected by an ESP.

The CIP Standards do not explicitly require a list of in-scope Cyber Assets. However, creating and maintaining such a list is an implicit requirement; this list or an equivalent will be requested by the audit teams during the review of CIP-005-5 R1. Also, this list will make your job of identifying and protecting your in-scope assets much easier. If you keep this list and periodically review it, you will be ahead of the curve when you are audited.

Ensure all Electronic Access points have been identified. Ensure that you can provide the inbound and outbound permissions (rule sets), and the reason for each permission. Ensure that you can demonstrate deny by default.

If you permit Dial-up Connectivity, your process must show how it is controlled and authenticated. If your dial-up equipment does not support authentication, be sure you have a TFE in place.

If you do not permit or do not use Dial-up Connectivity, be able to document this.

For BES Cyber Systems at Control Centers, ensure you can provide evidence demonstrating your ability to detect malicious communications in both directions.

Best Practices

Here are some practices not explicitly required by CIP-005-5 R1, but that are highly advisable:

1. Keep the Cyber Asset spreadsheet or database (from Suggested Evidence, above) under version control. In other words, keep a record of all changes, including details of the change and the date of the change.
2. Periodically review the evidence for this requirement to ensure it is correct and current. Document this review, including who performed the review and the date.
3. Periodically perform a discovery process to identify any previously unidentified devices within your ESPs. Document this process, document each time it is performed, and the results of each discovery.
4. Ensure your change management procedures require updating the evidence for this requirement as part of any applicable change.
5. If Part 1.5 is applicable to you, have a method of alerting appropriate personnel on detected malicious communications.

Managing Compliance with CIP-002-5.1 R1

As CIP Senior Manager, you should understand the approach your subject matter experts (SMEs) have taken to identify and document the Electronic Security Perimeters. Here are some questions you might ask your SMEs:

- Is there a comprehensive list of Cyber Assets that are subject to CIP compliance? If not, how are these Cyber Assets being managed?
- Have all Cyber Assets that are subject to CIP compliance been identified? How do we know this?
- Are there processes we follow to keep the Electronic Security Perimeter documentation up to date? Are these processes and the resulting evidence approved by the appropriate manager?
- Each inbound and outbound access permission requires a reason for the permission. Have these reasons been reviewed to ensure that they are actually the reasons the permission is required, as opposed to a statement of the nature of the permission? For example, if an inbound permission permits email to pass to a protected system, does the reason say what the permission is (“email to system xyz”), or does it provide an actual reason (“email to system xyz is required to permit coordination of failover status between primary and backup systems”)?

References

CIP-005-5

NERC Glossary

'NERCs “Implementation Study, Lessons Learned, and FAQs” Web Page

Feedback

Please let me hear any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached at lew.folkerth@rfirst.org.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP v5 RSAW's

I'm going to interrupt the series of CIP v5 compliance approaches to shine some "light" on the newly-published CIP v5 Reliability Standard Auditor Worksheets (RSAWs).

The Role of the RSAW

The RSAW's primary purpose is that of a tool used in support of the compliance monitoring processes, such as audits and spot checks. When used in conjunction with an audit or spot check, the RSAW tool serves two primary purposes:

1. The audited entity fills out the RSAW and transmits it as part of the initial evidence submission. In this phase of the audit, the audited entity uses the RSAW tool to organize compliance evidence and to communicate its compliance approach to the audit team.
2. Once the audit team receives the RSAW from the entity, its uses the RSAW tool to organize, execute, and document the entity's compliance assessment. The evidence reviewed, the approach used to assess compliance, auditor notes, and the audit findings and recommendations are documented in the RSAW tool.

An entity can also use the RSAW to organize its compliance efforts and to prepare for compliance monitoring actions. However, it is important to keep in mind that the RSAW tool is a worksheet and nothing more.

CIP v5 RSAW Development Overview and Strategy

The development of the CIP v5 RSAWs was an unprecedented undertaking. These RSAWs have received far more development effort and review than any other RSAWs developed by the ERO. Development began officially on May 23, 2013. In the course of the next two years, the development team changed, the Standards changed, and the overall concept of the RSAWs changed.

The first draft of the RSAWs reflected the intent, at that time, to make the RSAW the central repository of all guidance regarding a Standard. That philosophy changed in mid-2014 and most of the guidance was moved to separate documents, such as Lessons Learned and Frequently Asked Questions. The remaining drafts received substantial review and tuning, so that the final product is as error-free as possible.

The CIP v5 RSAWs are organized as one RSAW per Standard. Review of Technical Feasibility Exceptions and CIP Exceptional Circumstances are embedded in the applicable Requirements of each RSAW. The Requirements are addressed with one RSAW section per Part, rather than one section per Requirement.

Manistee North Breakwater, Manistee, MI
(Photo: L. Folkerth)

This is primarily due to the different applicability of each Part. The efficiency of this structure will be reviewed after some experience with using these RSAWs.

Organization and Structure

The CIP v5 RSAWs follow the current RSAW Template. A cover page provides information about the Standard and about the audit being performed. Findings and recommended actions are summarized on the second page. The third page contains the list of the Registered Entity's Subject Matter experts (SMEs).

The next sections are repeated for each Requirement or Requirement Part, beginning with a reproduction of the text of the Requirement. With the Requirement text the RSAW may ask one or more questions, although this is not frequently done.

After the Requirement text and questions, the entity is required to provide a compliance narrative. This narrative is the entity's best opportunity to describe, in as much detail as it sees fit, its approach to compliance with the requirement. The narrative should consist of several paragraphs, but in most cases should be less than a page long.

The intent is to give the audit team a brief synopsis of the entity's compliance approach, and to give sufficient detail so that the audit team will understand the entity's evidence without the need for additional questions or interviews. Copying and pasting from the language of the Standard conveys the wrong message to the audit team; rather, the compliance narrative should be carefully crafted to put the entity's best light on its compliance program.

An Evidence Table is available for the entity's use. This is a good place to

Continued on page 12

The Lighthouse

Continued from page 11

summarize the evidence provided, and to reference specific parts of the evidence for the audit team to review.

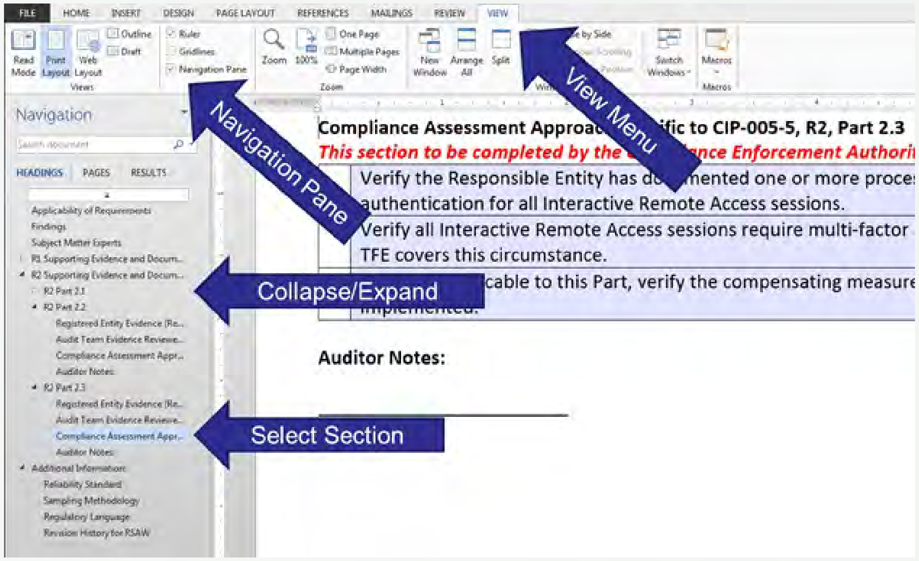
The next sections, Evidence Reviewed, Compliance Assessment Approach, and Auditor Notes, will be completed by the audit team.

Even though intended for the audit team, the Compliance Assessment Approach (CAA) can be very valuable to the entity as well. The CAA section of the RSAW provides the steps the audit team will take to review the entity's evidence and to make its compliance findings.

Minimal guidance is included as "Notes to Auditor." Most of the guidance is related to methods of performing the compliance assessment, and does not attempt to interpret the Standard.

Finally, the Additional Information section brings up the rear of the RSAW. Where the CIP Standards include Attachments, these are included here.

Navigation



Compliance Assessment Approa ific to CIP-005-5, R2, Part 2.3

This section to be completed by the nce Enforcement Authori

Verify the Responsible Entity has do mented one or more proce authentication for all Interactive Remote Access sessions.
Verify all Interactive Remote Access sessions require multi-factor TFE covers this circumstance.
cable to this Part, verify the compensating measure implemented.

Auditor Notes:

Figure 1 shows the navigation feature built in to each RSAW. In Microsoft Word 2013, select the View menu, then check the box next to Navigation Pane. The Navigation Pane will appear, showing an outline of the RSAW. Sections may be collapsed and expanded by clicking the little arrow to the left of each section name. Clicking on any section name will move the document to that section. This provides a rapid and effective way of moving through the RSAW.

Compliance Assessment Approach

As noted above, the CAA provides the framework for the audit review. It is important to understand that the verification steps of the CAA are provided as guidance for the audit teams. The audit teams may skip steps, modify steps, expand steps, or add steps as the audit team deems necessary. It is not intended as a rigid, step by step approach and only serves as guidance for the auditor.

For the CIP v5 Standards, the CAA may approach the audit review in any of several different ways:

Documentation Review

In a documentation review, the entity's evidence is examined to ensure the required documentation exists, and appears to be reasonable and complete. This is the weakest type of audit review used by the CIP v5 RSAWs, and its use is reserved for a few special cases. The CIP-004-6 R3 personnel risk assessments, for example, are extremely sensitive documents. An audit team may determine that it will examine the entity's processes, and the records of the execution of those processes, to determine compliance. If the audit team can obtain reasonable assurance of compliance in this way, the team may not need to examine the results of each personnel risk assessment directly.

Process Evaluation

The CAA for most of the CIP v5 Requirements contains a process evaluation. This consists of ensuring a required process exists and contains the steps or provisions required by the Standard. For example, does the process required by CIP-010-2 R1 Part 1.2 require that the entity authorize and document changes that deviate from the existing baseline configuration, and does the process apply to the systems subject to the Requirement?

Process evaluations are used wherever a process is required, but are not

Continued on page 13

Continued from page 12

For the CIP v5 Standards, the CAA may approach the audit review in any of several different ways: (continuted)

usually the only verification steps in the CAA. The exception to this is where the process is the intended result of the Requirement, such as the CIP-008-5 R1 incident response plan or the CIP-009-6 recovery plan.

Outcome Verification

The most common type of CAA verification step is the outcome verification. In this type of verification, the audit team determines whether the entity has actually performed the work required to secure its systems and comply with the requirement. For example, in order to ensure a CIP-010-2 R1 baseline is complete, the audit team may ask the entity to extract the current baseline information from a sample of Cyber Assets. The audit team will then compare this directly obtained information against the documented baseline and make a determination.

Special Considerations – Proving a Negative

Some concepts in the CIP v5 Standards need special consideration by the audit teams. One of these is proving a negative. In many cases, the entity must demonstrate that it has performed all required work and has not missed or skipped required items. For example, an entity must be able to show that during its performance of CIP-002-5.1 R1, it has not missed identifying any BES Cyber Assets. Some of the techniques that may be used include a process evaluation to ensure the process used in a requirement is sufficient to ensure nothing was missed. Documentation of the implementation of the process could also be reviewed to strengthen the evidence of compliance. The audit team could sample Cyber Assets that were not identified as part of a BES Cyber System and verify that the omission of the Cyber Asset is correct. In certain cases, an attestation may be accepted, although this is normally reserved for demonstrating that there is a null set of evidence. For example, an attestation that no reportable Cyber Security Incidents have occurred in the audit period may be accepted.

Special Considerations – Implied Requirements

In some cases, the audit team will need to review implied requirements – requirements that are not explicitly stated in the Standard's language, but are necessary to complete in order to demonstrate compliance with the language. For example, CIP-002-5.1 does not explicitly require the identification of BES Cyber Assets, but such identification is implied by the fact that BES Cyber Systems are composed of BES Cyber Assets, and each BES Cyber Asset must be included in one or more BES Cyber Systems.

These implied requirements are not usually spelled out in the CAA, but will be considered by the audit teams as part of performing the steps of the CAA.

Tips for Using the RSAWs

Avoid unnecessary redundancy by referencing prior responses where possible; otherwise, copy and paste. For example, if a process applies to an entire Requirement, describe it in one Part and make reference to it elsewhere.

The Compliance Narrative is your best opportunity to tell an audit team how you meet compliance.

Pay attention to any “Notes to Auditor.” They are meant for all users of the RSAWs, not just the auditors.

Use of RSAWs at ReliabilityFirst (RF)

To gain efficiencies in the RF audit practices, RF has integrated all approved RSAWs into the MKInsight Audit Management Suite. This audit tool is used by the RF audit teams when conducting audits, spot checks and other compliance engagements. The teams collect and review all entity evidence and record all auditor determinations in the tool and it is the central repository for RF's compliance monitoring work. Future developments will include the sharing of the “electronic” RSAWs with RF's entities during compliance engagements, further increasing audit efficiency for the entity and RF.

Feedback

Please let me hear any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached at lew.folkerth@rfirst.org.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Issue #9, Reading the CIP v5 Standards – Advanced Topics

In the December 2014 issue of this newsletter, I talked about compliance with "Non-prescriptive Standards." Step 2 of the suggested process touched on using guidance to help determine how to apply a Requirement to your compliance circumstance. In the July Open Compliance Call, I gave a presentation which went deeper into the use of guidance to inform your understanding of the CIP v5 Standards. That presentation and the recording of the call should be posted on the RF web site by the time you read this article.

But before we fall back on guidance in our understanding of the CIP v5 Requirements, we should make sure we need to do so. Many questions can be answered by a strict reading of the enforceable elements of the Standard.

Enforceable Elements of a Reliability Standard

The Standard Processes Manual (NERC Rules of Procedure Appendix 3A), Section 2.5, lists the elements of a Reliability Standard, and states,

> "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes, to establish the relevant scope and technical paradigm, and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority."

In addition to the applicability, Requirements, and effective dates, the Applicable Governmental Authority (FERC in the US) approves Glossary terms and implementation plans.

It is important to make sure we have applied the enforceable elements, including the Glossary terms and implementation plans, before we resort to using the guidance available in the Standard and from many other sources.

Let's look at some examples.

External Routable Connectivity

Question: Can External Routable Connectivity be removed from a Cyber Asset by blocking all access to that Cyber Asset at the Electronic Access Point (EAP)?

Answer: The following discussion uses Figure 1 as an example. "PLC" is the device for which External Routable Connectivity is being removed. "Internal Workstation" has External Routable Connectivity through the EAP on "Electronic Access Control" device to "External Server". The discussion assumes the use of standard TCP/IP and UDP/IP network protocols.

The use of a firewall or other network access control device to attempt to remove External Routable Connectivity from a Cyber Asset presents a serious compliance concern. External Routable Connectivity is defined in the NERC Glossary as,

> "The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection."

Harbor Beach, MI
(Photo: L. Folkerth)

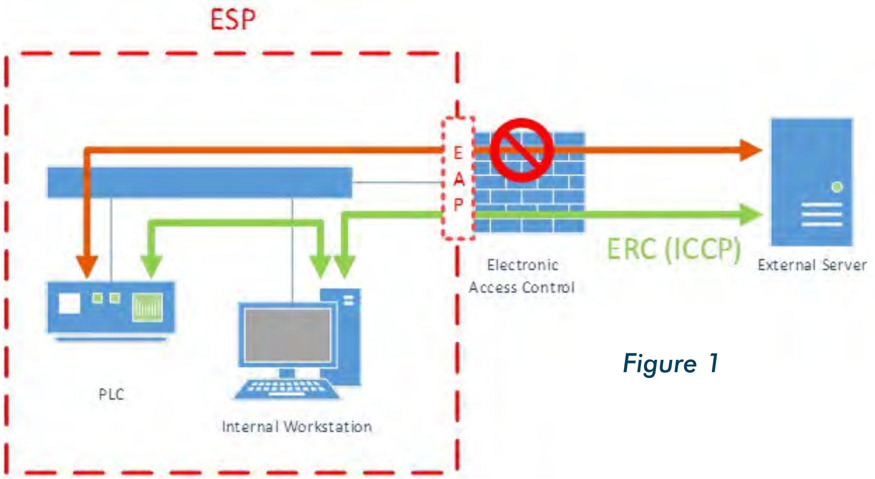


Figure 1

Continued on page 6

Continued from page 5

The use of the phrase "ability to access" in the definition implies that any communication path, whether direct or indirect, from outside the ESP to "PLC" would constitute External Routable Connectivity.

In contrast, CIP-005-5 Section 6, Background, contains a bullet which states,

"Medium Impact BES Cyber Systems with External Routable Connectivity – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity."

Note the phrase "directly accessed" in the bullet. This would seem to modify the wording of the definition of External Routable Connectivity. However, as a Glossary term approved by the Applicable Governmental Authority, the Glossary definition takes precedence.

Our conclusion, then, must be that the ability of any Cyber Asset outside of the ESP to reach "PLC," by any path, will give "PLC" External Routable Connectivity. While it may be theoretically possible to demonstrate that no External Routable Connectivity to "PLC" exists in a very small network, this becomes exponentially more difficult as the size of the network increases. Also note that if this position is taken then every Cyber Asset in the ESP with External Routable Connectivity, such as "Internal Workstation" in our example, becomes an Electronic Access Control and Monitoring System (EACMS), as each of these Cyber Assets controls access to "PLC."

In light of this discussion, the recommended practice is that if any Cyber Asset within an ESP has External Routable Connectivity, then all Cyber Assets within that ESP should be considered to have External Routable Connectivity.

Vulnerability Assessments

Question: My CIP-010-2 R3 vulnerability assessment procedure includes an additional element not required by the Standard. Am I exposing my company to an unnecessary compliance risk if we fall short when performing that element?

Answer: The answer to your question involves two separate topics, the language of the Requirement, and the audit practice of the Regions.

Language of the Requirement

CIP-010-2 R3 requires that an entity implement a documented process (more than one process is allowed) to address each of the Parts of the Requirement. Part 3.1 requires either a paper or active vulnerability assessment at least once every "CIP year" (15 months). Part 3.2 applies to high impact BES Cyber Systems only, and requires an active vulnerability assessment every three years. Part 3.3 requires an active vulnerability assessment before placing an applicable system into production. And Part 3.4 requires documentation and follow-up for the vulnerability assessments in Parts 3.1, 3.2, and 3.3.

This much we already knew from reading the Standard. It is important to note, however, that the term "vulnerability assessment" is not a term defined in the NERC Glossary. The meaning of the term is addressed in the "Guidelines and Technical Basis" of the Standard. From the discussion above, we know that this section is not directly enforceable, but instead informs our understanding of the enforceable elements of the Standard. Entities are "strongly encouraged" to adopt the vulnerability assessment elements listed in this section: network discovery; network port and service identification; vulnerability review/scanning; and wireless review/scanning.

What if an entity does not adopt one or more of these elements of a vulnerability assessment? In that case, the audit teams will probably review the vulnerability assessment procedure to determine if alternative controls are in place that mitigate the risk of not performing one of the suggested actions. If no alternatives are in place the audit teams are likely to write a Recommendation or Area of Concern regarding this shortcoming.

If your vulnerability assessment procedure has all of the suggested elements plus an additional element that you have added, the worst that should happen if you do not perform that added element is that a Recommendation or Area of Concern is issued.

Audit Practice of the Regions

The other part of your answer is that the Regions generally try to refrain from punishing "above and beyond" actions. An "above and beyond" action is an action that the entity requires of itself that goes beyond the actions required by the Standard. Under a very technical reading of the Standard this could be construed to be a violation, as you are required to implement the procedures you write.

But in actual practice, the Regions try to encourage such "above and beyond" actions, and the usual practice if there is a failure in performing such actions is a Recommendation, rather than a violation.

Feedback

Please let me hear any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached at lew.folkerth@rfirst.org.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion and to be helpful to you as you transition and refine your CIP compliance programs toward Version 5 compliance. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed some light on the sometimes stormy waters of CIP compliance.

Q: Is "Zero Tolerance" really gone? If so, how will that affect my compliance program?

A: One of the criticisms of "Zero Tolerance" was that the ERO and entity compliance programs spent too many resources on actions that did not have a significant impact on reliability. Reliability Assurance (formerly the Reliability Assurance Initiative) addresses that concern by permitting Registered Entities to take a flexible approach to achieving compliance with a Reliability Standard.

The price of that flexibility is that each entity must be able to document that the objective of the Standard is met. As CIP Version 5 is primarily results-oriented, it fits well into this approach. Let's take a closer look at the types of flexibility permitted by CIP Version 5.

Transition from CIP V3 to CIP V5

In recognition of the complexity of transitioning from CIP Version 3 to CIP Version 5, NERC published CIP V5 Transition Guidance and its companion document, V3-V5 Compatibility Tables.

In CIP V5 Transition Guidance, NERC states its recognition of the need for flexibility in the compliance approach during transition, and that it will "allow Responsible Entities to transition to the CIP V5 Standards, in whole or in part, during the Transition Period." CIP V5 Transition Guidance references V3-V5 Compatibility Tables in order to map CIP Version 3 Requirements to CIP Version 5 Requirements. Together, these documents provide great flexibility to an entity during the transition to CIP V5.

Let's explore an example.

An entity is implementing a security appliance that will detect known or suspected malicious communications in order to satisfy CIP-005-5 R1 Part 1.5. The entity plans to install this security appliance within an ESP before April 1, 2016, to gain experience with operating the security appliance and to be in full compliance on the compliance date. The security appliance cannot meet the password complexity required by CIP-007-3 R5.3.2 and cannot run anti-malware in order to meet CIP-007-3 R4.

The entity has the flexibility to declare the new security appliance a non-critical Cyber Asset within an ESP under CIP V3, and follow the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities. This requires the new security appliance to be "Compliant upon Commissioning" with CIP V3. Version 3 TFEs will be required for this security appliance for both CIP-007-3 R4 and CIP-007-3 R5.3.2.

The entity may alternatively declare that the new security appliance will be commissioned under the CIP V5 Standards as an EACMS associated with a BES Cyber System (see CIP V5 Transition Guidance, Section 4). During the transition, the entity will decide for each applicable CIP Requirement in V3-V5 Compatibility Tables whether the security appliance will follow the V3 or the V5 Requirement.

Tawas Point, MI
(Photo: L. Folkerth)

The entity could decide (and document) that the new security appliance will follow the CIP-007-3 R3 patch management process until the entity converts that process to CIP-007-6 R2's patch management requirements.

The entity could also decide (and document) that the security appliance will follow the password requirements in CIP-007-6 R5 and the anti-malware requirements in CIP-007-6 R3. In this case, CIP-007-6 R5 Part 5.5 permits a password complexity of "the maximum complexity supported by the Cyber Asset." CIP-007-6 R3 permits the security appliance to participate in anti-malware that protects an entire BES Cyber System. In neither case is a TFE required (or even permitted).

Continued on page 7

Continued from page 6

An audit team will review the protections applied to the security appliance to ensure that all required protections were applied, but will permit the flexibility of choosing either the V3 or V5 protections during the transition.

Compliance with CIP V5

Since CIP v5 Requirements are mostly results-based, an entity is allowed flexibility as to how its program achieves the result. Audit teams are being trained to recognize this flexibility, and to return "No Finding" if an entity is meeting the objective of the Requirement.

During an audit, the audit teams will keep in mind the three priorities of the electric industry:

1. Safety
2. Reliability
3. Compliance

In other words, an entity is not expected to sacrifice safety or reliability for compliance, but instead is expected to make all three priorities work together, overriding compliance only as needed and with compensating controls to mitigate any resulting risk.

Let's examine some of the ways flexibility can be applied in CIP v5:

CIP Exceptional Circumstances

The provision in CIP v5 for CIP Exceptional Circumstances is a major area of flexibility. While not a carte blanche, the CIP Exceptional Circumstances provision permits an entity to respond to emergencies, temporarily bypassing compliance if necessary, in order to deal with a safety or reliability issue.

> For example, if a Cyber Asset of a high impact BES Cyber System must be replaced with a Cyber Asset that does not match the original Cyber Asset's baseline, and that replacement must occur quickly due to reliability concerns, then the active vulnerability assessment required by CIP-010-2 R3 Part 3.3 may be skipped by invoking CIP Exceptional Circumstances.

The circumstances requiring the invocation of CIP Exceptional Circumstances should be documented, as well as how the policy regarding CIP Exceptional Circumstances was followed.

Results-oriented Requirement

A Requirement may specify a result, but not specify how to obtain the result. An example of this is CIP-007-6 R3 Part 3.2. In mitigating malicious code, the entity determines when and how the mitigation will occur. The entity's approach to this mitigation may vary widely depending on the individual circumstances. Malicious code detected in a Control Center might be expected to be quickly eliminated.

However, if the malicious code is found on an essential component of a generating plant's distributed control system (DCS), the plant may need a scheduled outage in order for the malware to be removed.

During the wait for the outage, other types of mitigation should be implemented and documented. This could include isolating the affected component to prevent it from communicating with the malware's command and control servers.

Flexibility is Explicitly Permitted

A Requirement may explicitly permit flexibility in the approach to compliance. CIP-007-6 R4 Part 4.2 requires that an entity generate alerts for security events "that the Responsible Entity determines necessitates an alert."

Two required types of alerts are listed in the Requirement, and eight possible additional types are identified in the Guidelines and Technical Basis, but the entity is allowed great freedom in choosing which security events will generate alerts.

The price of this flexibility is that each entity must be prepared to convince an audit team that its approach provides robust controls to mitigate the risk of a security event to reliability.

Unintended Consequences

Some aspects of the wording of a Requirement may cause unintended consequences to reliability. For example, CIP-007-6 R5 Part 5.4 requires each default password to be changed on all Cyber Assets in scope for CIP V5 at the high and medium impact levels if the Cyber Asset has the capability to change the default password.

This may not cause issues in a Control Center that uses only standard servers and workstations. In a generating plant or substation setting, however, depending on the circumstances, this Requirement may present a serious threat to the reliable operation of the asset.

Field devices in these locations generally have a much longer service life than their counterparts in Control Centers, and on older systems vendor support may be weak or non-existent.

A plant DCS central server may have a default password for a remote device, such as a

Continued on page 8

Continued from page 7

programmable logic controller (PLC), hardcoded into its applications. The PLC may be capable of changing its password, and therefore, is required to meet CIP-007-6 R5 Part 5.4. But, changing the password would break the relationship with the central server.

In this example, complying with the strict language of the Requirement will have a serious negative impact on reliability. If such a situation occurs, the entity will be expected to verify that it cannot meet strict compliance without sacrificing reliability, and document this verification. The entity should then determine an alternate method of achieving the reliability objective. In the case of the DCS, additional physical and network protections might be implemented to mitigate the risk of a default password being used by an unauthorized person.

When situations like this occur, it will be important to inform your Region staff of the issue and engage them in your mitigation efforts. ReliabilityFirst's Assist Visit program is designed for this and other types of issues.

During an audit, be proactive with the audit team about the issue, how the risk it poses was addressed, and the status of any long-term efforts to remediate the issue. Be sure to have adequate documentation of the compensating controls implemented and their ongoing maintenance. The entity's objective will be to convince the audit team that even though strict compliance was not achieved, the resulting risk to reliability was and continues to be mitigated.

Making Use of Flexibility

To summarize, here is a checklist to use when taking advantage of the flexibility built into the CIP V5 Standards and into today's audit processes:

1. Ensure the reliability objective of the Requirement is met. If there is any doubt about what this objective is, engage your Region staff.
2. Document the implementation and ongoing maintenance of the controls used to implement compliance. Explain any use of the flexibility options listed above, and how those options were exercised to improve reliability.
3. If an alternate means of compliance was implemented, document the circumstances of the issue. Document the implementation and ongoing maintenance of any mitigating measures.
4. Be proactive in communicating any issues to your Region. If in doubt, engage your Region staff as early as possible.
5. Document, document, document!

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion and to be helpful to you as you transition and refine your CIP compliance programs toward Version 5 compliance. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed some light on the sometimes stormy waters of CIP compliance.

Q: What are the implied requirements in CIP Version 5? How can I be expected to comply with a requirement that isn't openly stated?

A: Implied requirements are a consequence of writing CIP Version 5 as results-based Standards. In a results-based Standard, the desired end result is specified, with the method of achieving the result left unspecified. This provides great flexibility in how the result is achieved, but one effect is that some actions that are actually required are not explicitly stated in the Standard.

Note: When referring to a generic requirement, such as a requirement to document a process, the word "requirement" will not be capitalized. If I am referring to a Requirement of a Reliability Standard, the word "Requirement" will be capitalized.

At the ReliabilityFirst CIP V5 Workshop in October, I was asked to create a list of implied requirements. In this column I'll offer you some guidance on how to identify and categorize implied requirements, but I won't attempt to provide a complete list. A list of the implied requirements I can identify today would be far too long for this column. And as my understanding of CIP Version 5 matures, I find that I can identify more implied requirements. My opinion is that we may never be able to achieve a complete list of implied requirements; the more we mature in our understanding of CIP Version 5, the more implied requirements we will find.

Types of Requirements

Implied requirements are affected by the type of Reliability Standard Requirement they are associated with. In general, CIP Version 5 Requirements consist of three types:

1. Periodic Requirements - Requirements that must be performed at certain intervals.

   Example: CIP-004-6 R2 Part 2.3 requires cyber security training to be completed at least every 15 calendar months.

2. Event-Driven Requirements – Requirements that are triggered by a specific event or occurrence.

   Example: CIP-004-6 R2 Part 2.2 requires cyber security training before access is granted. The triggering event would be the request for access.

White River Light Station, MI
(Photo: L. Folkerth)

3. Ongoing Requirements – Requirements that must be continuously maintained .

   Example: CIP-005-5 R1 Part 1.1 requires that all high or medium impact BES Cyber Systems be protected by a defined Electronic Security Perimeter Electronic Security Perimeter. The ESP must be maintained in place at all times.

Some Requirements have characteristics of more than one type. For example, CIP-003-6 R3 requires that a CIP Senior Manager be designated (ongoing requirement), and that any change be documented within 30 days (event-driven requirement).

Sources of Implied Requirements

1. Implications of Requirement Language

   Implied requirements come from different sources. Some come from implications or understandings of the language crafted by the Standard Drafting Team. A prime example is the use of the phrase, "shall implement one or more documented processes." This language occurs many places in the Standards, and in many forms, including implementation of a process, plan, or program. These are usually associated with an Ongoing Requirement. The understanding of this phrase, when used in an Ongoing Requirement, is that the process, plan, or program must not only be implemented once when it is put into place, but its implementation must be maintained on a continuing basis. Take the case of CIP-005-5 R1 Part 1.1. It would make no sense to say

Continued on page 9

Continued from page 8

that an ESP must be defined once when compliance for the Part is put into place, and then ignored. The Requirement must be read that the process to implement a defined ESP must also be maintained on an ongoing basis. This leads to a general implied requirement:

An Ongoing Requirement that includes a requirement to implement a process, plan, or program also includes the obligation to maintain the process, plan, or program on an ongoing basis.

2. Results-Based Specification

   Another source of implied requirements is the results-based specification of a Requirement. To illustrate this, CIP-002-5.1 R1 Parts 1.1 and 1.2 require that high and medium impact BES Cyber Systems are identified, but R1 is silent as to how to identify the BES Cyber Systems. The definition of a BES Cyber System makes it clear that BES Cyber Systems are composed of "one or more BES Cyber Assets." It is therefore not possible to identify a BES Cyber System without identifying its component BES Cyber Assets. We can state this generally as:

   In a Requirement that is results-based, the method of achieving the result must be documented, such that all aspects of the Requirement language, including any applicable Glossary terms, are satisfied.

3. Applicable Systems

   Requirements may be implied by the Applicable Systems language of a Requirement. For example, many Requirements include Electronic Access Control and Monitoring Systems (EACMS) as an Applicable System. Yet nowhere in CIP Version 5 is there an explicit Requirement to identify and list an entity's EACMS. Failure to do so, however, will mean that you cannot demonstrate to an audit team that you have protected all of your EACMS as required by CIP Version 5.

   As most Requirements must be applied to individual Cyber Assets, each Cyber Asset within CIP scope must be identified and assigned to one or more Applicable Systems.

4. Lack of a Definition

   A lack of a definition or other statement of expectations in the Requirement language also creates implied requirements. CIP-010-2 R3 Part 3.1 requires an entity to perform a cyber vulnerability assessment, but the language of the Requirement does not specify what that means. We need to rely on approved guidance in the Guidelines and Technical Basis of the Standard, and on our understanding of good security practice.

   In the case where a Requirement does not include a specific definition or specification of its outcome, approved guidance will inform our understanding of the required outcome.

Failure to Comply with an Implied Requirement

Implied requirements are actions that are needed to support compliance with the language of a Requirement of a Reliability Standard, but are not explicitly stated in the language of the Requirement. If an implied requirement is violated, an audit team will return a finding for the Requirement that is supported by the implied requirement. Since an implied requirement may support multiple Requirements, a violation of the implied requirement may result in multiple audit findings. An example of this would be the failure to identify and protect an EACMS associated with a high impact BES Cyber System. Failure to identify and protect each EACMS could potentially result in an audit finding in 64 Parts of 18 different Requirements.

A List of Implied Requirements

As I said above, I'm not confident that a complete list of implied requirements can be created. And if a "complete" list is created, it will need to be a living document, changing in response to our changing understanding of CIP Version 5. Also, any list of implied requirements will need to be reviewed by the Enterprise ERO, which includes NERC and all eight Regions, and published as a guidance document in accordance with NERC's recently adopted guidance policy.

Feedback

Please share any feedback you may have on these articles.

Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Collecting and Presenting Evidence

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion and to be helpful to you as you transition and refine your CIP compliance programs toward Version 5 compliance. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed some light on the sometimes stormy waters of CIP compliance.

Q: What evidence of compliance will be needed for CIP Version 5? Will ReliabilityFirst require CIP Version 5 evidence to be submitted in a specific format?

A: Generally Accepted Government Auditing Standards (GAGAS) require audit teams to "obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions." (GAGAS 6.56.) In order to assist with evidence collection and formatting, NERC has published the CIP Version 5 Evidence Request (the "Evidence Request") and its associated User Guide. The documents are available on NERC.com in Initiatives, CIP V5 Transition Program. [Note: The current document posted is a Zip file. If you previously downloaded the separate spreadsheet and User Guide, please discard them and download the Zip file.]

The Evidence Request is a logical continuation of the CIP Version 5 RSAW development process. The RSAW development team and the industry representatives we worked with saw a need for additional information to assist entities in preparing for an audit.

The intent in publishing the Evidence Request is to provide information as to what evidence will be needed to demonstrate compliance with the CIP Version 5 Standards. The document does not, and cannot, alter the meaning of the Standards. Rather, it provides a framework for collecting and preserving the evidence that an audit team is likely to ask for and needs to validate and verify compliance.

On first examination, the Evidence Request spreadsheet appears overly detailed and complex, but this is by design. The Evidence Request is intended to be useful and assist an entity as if they were engaged in the most complete and detailed audit the development team could envision. Actual audits may use a subset of the material in the Evidence Request based on audit risk and scope. Also, because the Version 5 Standards are much more complex then the Version 3 Standards, the Evidence Request includes more detail. The Evidence Request development team simplified and consolidated the individual request items as much as possible in accordance with the language of each Requirement.

The Evidence Request is a spreadsheet organized by color-coded tabs. Each tab and each column within each tab is discussed in the User Guide. The User Guide also provides an overview of the evidence request and submittal process.

Intended Uses

The Evidence Request has several intended uses. It is likely that additional uses will be discovered as Registered Entities have a chance to get familiar with it and apply it to their own compliance programs. Here are some of the intended uses of the Evidence Request:

1. The Evidence Request is a guide to the evidence that is likely to be requested by an audit team. The Evidence Request is intended to be a common format used in audits across all eight Regions, although this use has not yet been finalized.

An example of this usage is when a compliance group needs to know what evidence will be necessary to demonstrate compliance with a particular Requirement. Use the "Level 1" tab to determine what process documents the audit team will need, and also any detail tabs the audit team will need as populations for sampling. The "Level 2" tab will indicate what detailed information will be requested of the sampled items.

Old Mackinac Point, MI
(Photo: L. Folkerth)

2. The Evidence Request provides a framework for organizing CIP Version 5 evidence. The "Level 1," "Level 2," and "Level 3" tabs provide a list of evidence that could be used to demonstrate compliance with each Requirement. The Request ID associated with each item of evidence may help to organize your evidence as you accumulate it. The Evidence Request development team is committed to keeping the Request IDs as consistent as possible across future versions of the Evidence Request. If a Request ID must be changed in a future version, the version history of the document will reflect this.

3. The Evidence Request identifies an information structure that may be requested by the audit teams to build populations of items to be used for sampling. The green detail tabs in the spreadsheet ("BES Assets," "CA," etc.) can be used to gather this information. Having this information structure in advance will permit you to automate the generation of information to populate these tabs, which could greatly reduce the time and effort required to respond to an audit team's initial evidence request. Some entities I have spoken to have even stated an intention to use these tabs directly to keep this information as their primary compliance evidence.

4. The Evidence Request identifies detailed information that may be requested by the audit team. The Evidence Request "Level 2" and "Level 3" tabs provide the list of detailed information an audit team may need for a

Continued on page 6

Continued from page 5

sample of items from the populations provided in the green detail tabs. The Evidence Request also identifies the sampling and types of samples that may be used by an audit team. The “Sample Set 2” and “Sample Set 3” tabs list the samples that will be needed, and include references to the source populations.

5. The Evidence Request provides an overview of the information flows for the evidence request and sampling processes used by the ERO audit teams. This may provide an entity with a better understanding of the audit process.

As you can see from the possible uses above, the Evidence Request provides an entity with the structure and evidence lists that may be used by the Compliance Enforcement Authority's audit teams. Having this information, in addition to other published audit information such as the Compliance Auditor’s Handbook, could enable an entity to duplicate the audit processes in sufficient detail to perform its own compliance audit.

This could make upcoming CIP compliance audits an “open book” test, where an entity is able to practice responding to audit requests until its audit responses require minimal effort and accumulation of audit-quality evidence is simply part of day-to-day operations. Coupled with robust internal controls to ensure that compliance processes run reliably, future Internal Controls Evaluations could then conclude that an entity's reliability risk is low enough to greatly reduce the need for external auditing.

What the Evidence Request Is Not

Having discussed what the Evidence Request is, let's also discuss what it is not.

First, the Evidence Request is not intended to be prescriptive. If you have an alternate method of demonstrating compliance that conflicts with an item in the Evidence Request, simply document that difference as a variance from the evidence requested. Your audit team should be willing to work with you on any variances. Also, please let the Evidence Request development team know that you are doing something differently, and perhaps we can accommodate your method in a future version.

Second, the Evidence Request is not carved in stone. The development team will continue working to fine-tune the Evidence Request as errors or weaknesses are discovered or better ways of demonstrating compliance come to light.

Helpful Hints

The Request ID, Standard, and Requirement columns are set up for Excel filtering. This will make it easier to work on a specific Standard or Requirement.

Each of the detail tabs is formatted with 3000 data rows. If you need more rows in a tab, copy the last row and extend the index as far as needed. This will retain the desired formatting. If you need fewer rows, feel free to delete any unneeded rows. When building the detail tabs, please keep the formatting provided and keep the indexes sequential.

Column H in the “CA” tab is a calculated value. If it creates a problem during data import, it may be deleted and re-inserted. Please remember to restore the original formula.

If you need to bring data from an external source into the Evidence Request spreadsheet, common formats such as CSV may be used. For example, to import CSV into a tab, the Data -> Get External Data -> From Text facility in Excel may be used to import data. If you do this, be careful to either preserve or restore the formatting, such as the drop-down lists. If you plan to use this facility during an audit, I suggest you practice so you are comfortable with the interaction of your data with the Evidence Request spreadsheet.

Future Enhancements

As we move forward into 2016, the Evidence Request development team will be working to enhance the Evidence Request and its supporting documents. One of the planned enhancements is to provide some guidance for incorporating risk considerations into the evidence and samples. Lower risk entities should require less evidence and smaller sample sets to provide reasonable assurance of audit results. This should be reflected in the Evidence Request.

Another planned enhancement is the development of a relational database to be used by the audit teams when processing the detailed evidence and when selecting samples. One of the criticisms of the detail tabs is that they are overly normalized for a spreadsheet. This design is intentional and will support creation of a normalized database for use by the auditors.

It is the intent of the development team to publish the specification for this database when it is ready. This may permit entities to export from their existing compliance systems directly to a format usable by the back-end database, bypassing the need to fill in the detail tabs on the spreadsheet.

Comments Encouraged

Comments on the Evidence Request are encouraged. Please email any comments to NERC’s Transition Program at TransitionProgram@nerc.net.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Grand Haven South Pierhead Entrance Light, MI
(Photo: L. Folkerth)

Protecting Against Malware – Passive and Active Defense

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion and to be helpful to you as you transition and refine your CIP compliance programs toward Version 5 compliance. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed some light on the sometimes stormy waters of CIP compliance.

Q: CIP-007-6 R3, Malicious Code Prevention, does not allow for a Technical Feasibility Exception (TFE) in the case where a Cyber Asset can't run an anti-virus program. How do we demonstrate compliance for this Requirement?

A: CIP-007-6 R3 Part 3.1 is a good example of the dual-edged nature of the flexibility built into the new CIP standards. You are given the bare-bones requirement to "Deploy method(s) to deter, detect, or prevent malicious code." This Requirement applies to all Cyber Assets in CIP scope at the high or medium impact level, with no TFE permitted.

> Good architecture and passive defense practices build a defensible ICS; active defense processes establish a defended ICS environment. Countering flexible and persistent human adversaries requires properly trained and equipped human defenders. (Lee, Assante, & Conway, 2016)

I'll admit that when I first read this, I thought it was a poorly-written requirement. But as my understanding of Version 5 and how it is intended to be implemented and enforced has matured, I begin to see that it may be one of the best-written requirements. How is that possible?

CIP Version 5 Standards were written to be results-based and non-prescriptive. CIP-007-6 R3 Part 3.1 meets that goal. It specifies the intended result, but does not say how to achieve it. This then puts the responsibility on each entity that implements this Requirement to first, achieve the result desired, and second, to be able to demonstrate to an audit team that the intended result has been achieved. And to do this without any exceptions.

Let's explore a possible approach to both of these items. Keep in mind that this is just one possible approach. You can adapt these ideas to your own circumstances. Also note that I have incorporated ideas from multiple sources, including actual approaches by some of the RF entities.

Implementation Strategy

Let's start with an implementation strategy, which could be documented in the cyber security policy or an anti-malware program. The items in the strategy will include:

1. Where feasible, all in-scope Cyber Assets are required to have some form of protection from malicious code;
2. All in-scope Cyber Assets are required to have some form of detection for malicious code; and
3. Where applicable, in-scope Cyber Assets will implement practices to deter the entry or propagation of malicious code.

This covers the three core elements of the Requirement: deter, detect, and protect. In the implementation of this strategy, we'll also leverage state of the art defensive techniques.

A good summary of what is considered state of the art can be obtained from the SANS/E-ISAC analysis of the Ukrainian cyber attack. In the Recommendations section, the authors discuss the use of architecture, passive defense, and active defense to protect critical systems.

Figure 1 below lists some possible defensive measures, which was taken from the Ukrainian attack paper and other sources. We will apply this list to each of our in-scope Cyber Assets in an example below.

Figure 1 - Catalog of Available Defensive Measures

Defensive Measure	Type	Deter	Detect	Protect
Network segmentation	Architecture	X		X
Logging	Architecture		X	
Data capture capability	Architecture		X	
Tested tools and technologies	Architecture		X	X
Patching	Architecture			X
Secure remote access	Architecture			X
Event monitoring system	Architecture		X	
Application whitelisting	Passive Defense			X
Host-based anti-virus	Passive Defense		X	X
Network anti-virus	Passive Defense		X	
Intrusion detection system	Passive Defense		X	
Intrusion prevention system	Passive Defense		X	X
Log monitoring & correlation	Passive Defense		X	
System hardening	Passive Defense	X		
Secure software development	Passive Defense	X		
Supply chain management	Passive Defense	X		
Active defense capability	Active Defense		X	
YARA rules (ICS-CERT)	Active Defense		X	
Periodic forensic memory analysis	Active Defense		X	
Periodic disk forensic analysis	Active Defense		X	

Continued on page 10

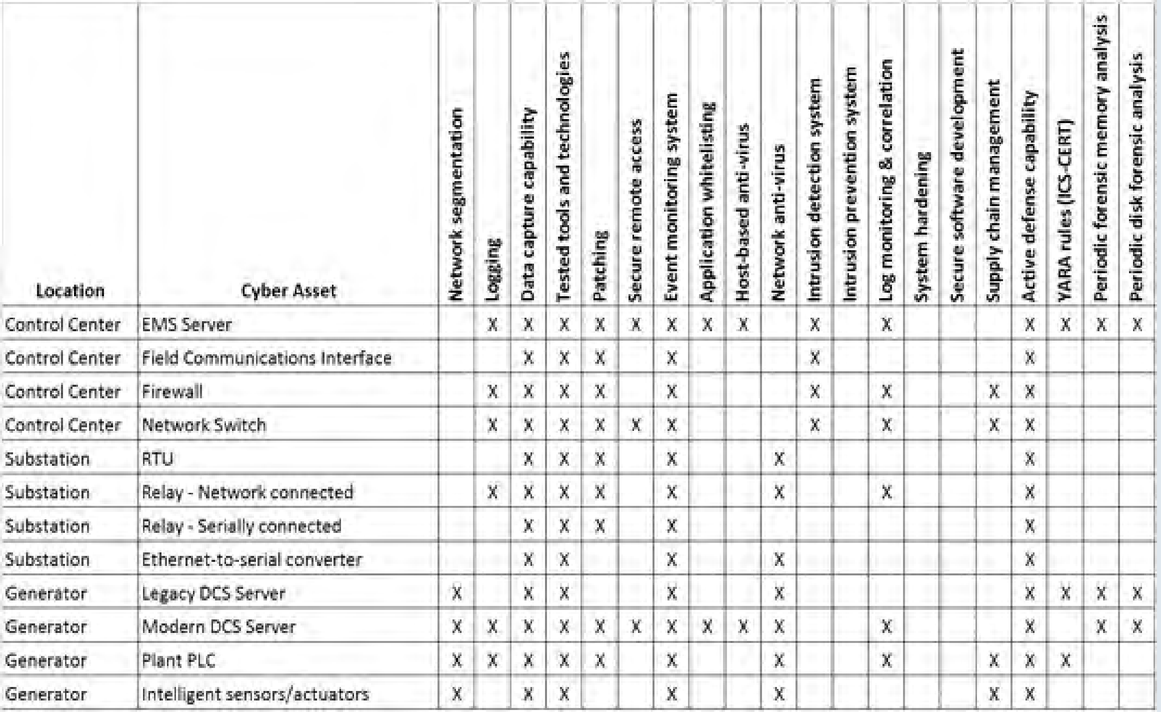
The Lighthouse

Continued from page 9

If we apply these defensive measures they should give us enough tools to provide protection or detection for all devices, without disrupting the operation of field devices.

Our next step is to take these defensive measures and apply them as appropriate to each in-scope Cyber Asset. Let's map out our application of defensive measures like this:

Figure 2 - Application of Defensive Measures



Location	Cyber Asset	Network segmentation	Logging	Data capture capability	Tested tools and technologies	Patching	Secure remote access	Event monitoring system	Application whitelisting	Host-based anti-virus	Network anti-virus	Intrusion detection system	Intrusion prevention system	Log monitoring & correlation	System hardening	Secure software development	Supply chain management	Active defense capability	YARA rules (ICS-CERT)	Periodic forensic memory analysis	Periodic disk forensic analysis
Control Center	EMS Server		X	X	X	X	X	X	X	X		X		X				X	X	X	X
Control Center	Field Communications Interface			X	X	X		X				X						X			
Control Center	Firewall		X	X	X	X		X				X		X			X	X			
Control Center	Network Switch		X	X	X	X	X	X				X		X			X	X			
Substation	RTU			X	X	X		X			X							X			
Substation	Relay - Network connected		X	X	X	X		X			X			X				X			
Substation	Relay - Serially connected			X	X	X		X										X			
Substation	Ethernet-to-serial converter			X	X			X			X							X			
Generator	Legacy DCS Server	X		X	X			X			X							X	X	X	X
Generator	Modern DCS Server	X	X	X	X	X	X	X	X	X	X			X				X		X	X
Generator	Plant PLC	X	X	X	X	X		X			X			X			X	X	X		
Generator	Intelligent sensors/actuators	X		X	X			X			X						X	X			

This shows some of the defensive measures that have been applied to each protected Cyber Asset. You can do this for each class of device, as I have, or you can do this for each device in scope, whichever works for you.

Demonstrating Compliance

Once you have them mapped, as above, to show how the systems are protected, the question remains, how do we show an audit team that we are complying with the Standard? I can't think of a better place to start than Figure 2, above.

This figure not only shows that we are applying at least one defensive measure to each in-scope Cyber Asset, but that we are applying defense in depth across all of these Cyber Assets. This is a great way to give an audit team, or a CIP Senior Manager, a high-level overview of how you are protecting your systems.

During an audit, expect the audit team to choose a sample of Cyber Assets. Be prepared to show the protections applied to each sampled Cyber Asset, as indicated by an "X" in Figure 2. You should be able to produce evidence of the implementation of each of these defensive measures, and show your work!

You should also be aware of the current threat environment, and be prepared to explain how you are equipped to detect and deal with changing threats to your systems.

References:

Lee, R.M., Assante, M.J., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukranian Power Grid*. Washington, DC: E-ISAC. Retrieved the document here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Final Check for CIP Version 5 Compliance

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion and to be helpful to you as you transition and refine your CIP compliance programs toward Version 5 compliance. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed some light on the sometimes stormy waters of CIP compliance.

As we approach the implementation and enforcement date for CIP version 5 compliance, it's a good time for a final check of your compliance program. If something important was overlooked, there is still time to fix it before July 1, 2016. Here are some suggestions for reviewing the fine points of CIP version 5 compliance, so that you're not caught by avoidable errors.

Ensure you have a documented program, policy, plan, or process for every Requirement that needs one.

Most CIP version 5 Requirements contain a base requirement that calls for one or more documented processes, policies, plans, or programs. All but two of these base requirements have an implementation date of July 1, 2016.

The result is that, except for CIP-002-5.1 R2, CIP-003-6 R2, R3, and optionally R4, and CIP-010-2 R4, you must have a documented program, policy, plan or process in place for each Requirement by July 1, 2016. This is necessary even if some of a Requirement's Parts need not be implemented until a later date. For example, CIP-010-2 R3's documented process must be in place on July 1, 2016, even though Parts 3.1 and 3.2 only require initial performance at a later date.

Ensure your documented programs, policies, plans, and processes meet the minimum needs of the Requirement they address.

When reviewing your compliance evidence, one of the first things an audit team will do is verify that all actions required by each Requirement and Part are addressed by your programs, policies, plans or processes. Make sure these documents actually address each of the required items. For example, ensure your information protection program shows how you identify BES Cyber System Information (BCSI), per CIP-011-2 R1 Part 1.1. If your CIP version 3 program has been repurposed for CIP version 5, it is possible to overlook the need to explicitly state how you identify BCSI.

Ensure you have evidence of the implementation of each documented program, plan, or process.

Except for the incident response plan and the recovery plan, every documented program, plan, or process is required to be implemented. The incident response plan and the recovery plan should be implemented as necessary and tested or exercised as required. One way to show that you have implemented a document is through its revision history. If your CIP version 5 document replaces the CIP version 3 document, and the revision history shows this, then that is evidence you can present to an audit team that the CIP version 5 document has been implemented.

As soon as a program, plan, or process is implemented, you should begin collecting evidence of that implementation. An audit team will want to see that your program, plan, or process is in place, and is being used consistently.

Ensure you have reviewed, and your CIP Senior Manager has approved, the lists required by CIP-002-5.1 R1.

The initial performance date for CIP-002-5.1 R2 is

Muskegon South Pierhead Light, MI
(Photo: L. Folkerth)

Low Impact Entities

For entities that have only low impact BES Cyber Systems, the following should be completed before July 1, 2016:

1. Ensure you have a documented process that has been implemented to identify all assets that contain a low impact BES Cyber System;
2. Ensure that generation disaggregation, if any, is complete;
3. Ensure that the list of assets that contain a low impact BES Cyber System has been reviewed and has been approved by your CIP Senior Manager or delegate;
4. Ensure you have documented the identification of your CIP Senior Manager; and
5. Ensure you have implemented your documented delegation process if your CIP Senior Manager has delegated authority.

Continued on page 10

Continued from page 9

July 1, 2016. You must be able to show that you have reviewed the lists of high and medium impact BES Cyber Systems, and the list of assets containing a low impact BES Cyber System, before this date. The CIP Senior Manager or delegate must also have approved these lists.

If you are making use of generator disaggregation, ensure that the disaggregation is complete by July 1, 2016.

Many entities with large generators are taking advantage of the provision in CIP-002-5.1 Attachment 1 Criterion 2.1 to reduce the impact rating of many or all of the generator's BES Cyber Systems to low impact by “disaggregating,” or ensuring that a BES Cyber Asset does not impact more than 1500 MW. Many unforeseen factors can affect the completion of this kind of project, including failure to obtain a plant outage when needed. If your disaggregation is at risk of not being complete by July 1, 2016, you should immediately reach out to RF’s enforcement group.

Ensure your cyber security policies meet the criteria established in the Standard.

CIP-003-6 Section 6, Background, provides additional information about what constitutes a policy:

“The term policy refers to one or a collection of written documents that are used to communicate the Responsible Entities' management goals, objectives and expectations for how the Responsible Entity will protect its BES Cyber Systems. The use of policies also establishes an overall governance foundation for creating a culture of security and compliance with laws, regulations, and standards.”

Your cyber security policies should be written so that they communicate your management's goals, objectives, and expectations. They should also establish a governance foundation for the remaining Standards. For example, a governance foundation could establish oversight of the achievement of the goals, objectives, and expectations? If your present policies fall short of this you will want to revise them, and obtain your CIP Senior Manager's approval of them, before July 1, 2016.

Ensure your CIP training program, including the content of your training materials, meets the specifications of CIP-004-6 R2.

Even though your personnel do not need to finish their “annual” training per CIP-004-6 R2 Part 2.3 until July 1, 2017, the CIP-004-6 program must be in place by July 1, 2016. Your compliance evidence must show that the CIP-004-6 program has been implemented, that the CIP-004-6 training content is in use, and that training based on this content is being tracked.

Ensure your personnel risk assessment (PRA) program meets the specifications of CIP-004-6 R3.

The needs of the PRA program have changed somewhat from CIP version 3. Make sure that your PRA program addresses the changes, such as the revised criminal history check and the process to evaluate the results. Also make sure that any PRAs conducted after July 1, 2016, are performed under this new program and evidence of the use of the CIP-004-6 program is being tracked.

Ensure cabling within an Electronic Security Perimeter (ESP), but outside of a Physical Security Perimeter (PSP), is protected.

CIP-006-6 R1 Part 1.10 requires that physical communication components such as cables, patch panels, etc. that are within an ESP but not within a PSP be protected as specified in the language of Part 1.10. If the ESP involved is just coming into scope under CIP version 5, then you have until April 1, 2017, to protect these components. However, if the Cyber Assets using these components were in scope under CIP version 3, then you must protect them by July 1, 2016, per the language of Part 1.10.

Ensure physical ports are protected.

CIP-007-6 R1 Part 1.2 requires protection of physical ports. Physical ports on Cyber Assets that are members of a BES Cyber System must be protected by July 1, 2016. For example, an EMS server is a BES Cyber Asset and has been grouped into a BES Cyber System. This EMS server must have its physical ports protected by July 1, 2016. A network printer that is classified as a Protected Cyber Asset would need to have its physical ports protected by April 1, 2017.

Ensure all in-scope Cyber Assets are at current patch levels, or that a mitigation plan is in place for each patch not installed.

Your CIP-007-6 R2 patch management program is required to keep your in-scope Cyber Assets at current patch levels, or to mitigate the vulnerabilities addressed by patches that have not been installed. When the July 1, 2016, implementation date arrives, audit teams will expect to see that all Cyber Assets at the high or medium impact levels are patched. For each security patch not applied, a mitigation plan must be in place that mitigates the vulnerabilities addressed by that security patch.

Ensure your information protection program has been updated to comply with CIP version 5.

The information protection program, required by CIP-011-2 R1, has changed from CIP version 3. Where CIP-003-3 R4 required you to “identify, classify and protect information associated with Critical Cyber Assets,” CIP-011-2 R1 requires you to

Continued on page 11

The Lighthouse

Continued from page 10

identify and protect BES Cyber System Information. Make sure you adapted your information protection program to the new Requirement, and that it covers all information included in the NERC Glossary definition of BES Cyber System Information.

Ensure your information protection program identifies designated storage locations for BES Cyber System Information.

While CIP-011-2 does not explicitly require designation of storage locations for BES Cyber System Information, CIP-004-6 R4 Part 4.1 requires a process to authorize access to such locations. To minimize your compliance risk in this area, you should designate such storage locations and include them in your access control program.

Ensure you retain evidence of logging for at least three years.

CIP-006-6 R1 Part 1.9, CIP-006-6 R2 Part 2.3, and CIP-007-6 R4 Part 4.3 all require retention of logs for 90 days. However, in Section C, "Compliance," of each Standard you are required to retain evidence of compliance for each Requirement for three years. These provisions are not in conflict. Section C requires retaining "data or evidence to show compliance" for three years. This means that you need to retain evidence that logs have been kept; you do not need to retain the logs themselves for three years. One method that may be used is tracking daily statistics of the logs, such as number of records stored per day.

Ensure you are retaining sufficient and appropriate evidence.

Audit teams are required to obtain sufficient, appropriate evidence in order to support their findings and conclusions. Sufficient evidence is the measure of the quantity of audit evidence required to form an opinion. Appropriateness is the measure of the quality of audit evidence. Appropriate evidence is evidence that is relevant, valid, and reliable. Relevant audit evidence pertains to the Standard and requirement that is being audited. Valid evidence actually represents what it is supposed to represent. Reliable audit evidence provides consistency of results when the evidence is tested.

More evidence is not necessarily better. A small amount of high quality evidence is better than a large amount of poor quality evidence. You can improve the quality of your evidence by making sure that all compliance documents include:

1. The company name or logo;
2. A document number and/or title;
3. An effective date;
4. Pages numbers to show completeness;
5. Clear reviews and/or approvals as needed; and
6. Detailed version history.

You should compare your compliance evidence to the CIP Version 5 Evidence Request to make sure you can supply an audit team with the evidence it will need in order to draw its conclusions. For example, Request ID CIP-004-R2-L2-01 asks for evidence that training was provided prior to access being granted and for evidence of the training content provided to the individual. Make sure the system you're using to track the training can provide this information without expending excessive effort.

Ensure your reliability, security and compliance programs are meeting both the letter and the intent of the Standard.

Compliance by itself does not contribute to the reliability of the BES. A digital relay does not care that there is a process in place to protect it from unauthorized access. The relay only cares that it is commanded to open a circuit breaker.

Compliance does contribute to security and reliability when it is one component of a comprehensive program that manages and secures the assets that are essential to the operation of the BES. In implementing a compliance program, it is important that we not only obey the letter of the Standard, but that we achieve the intent of the Standard as well. This means going beyond compliance if that is necessary to keep the BES reliable and secure.

Ensure that you are continuously improving your compliance and security processes.

The realm of cybersecurity continues to evolve, and we must evolve with it. We should work towards higher levels of maturity in all aspects of compliance and security.

Requests for Assistance

If you are an entity registered with RF and need assistance, please submit an Assist Visit Request via the RF web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Software Vulnerability Management

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion and to be helpful to you as you strive for continuous improvement in your CIP compliance programs. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed some light on the sometimes stormy waters of CIP compliance.

I recently had a discussion with the security and compliance staff from one of ReliabilityFirst's entities regarding patch management. We discussed the requirements for patch management in CIP-007-6 R2, and how those requirements fit into the overall protection strategy at this entity. We discovered that patch management is part of the larger concern of software vulnerability management, and that it may be better for entities to implement a software vulnerability management process rather than only a patch management process.

Software Vulnerability Lifecycle

In this article we will discuss software vulnerabilities, flaws in software that may be exploited to produce consequences not intended by the software developer. There are other types of vulnerabilities, such as weak passwords, that are outside the scope of this discussion.

A vulnerability in software may exist for a long period of time and only becomes significant to a user of the software when that vulnerability is discovered. Discovery of vulnerabilities may occur at any time in the lifecycle of the software, and may be affected by advancements in tools and techniques used in discovering vulnerabilities. Software that has previously been considered to be secure may become vulnerable as the threat environment changes.

From our perspective in CIP compliance, a software vulnerability begins when the vulnerable software is installed on an in-scope system (i.e., a Cyber Asset that is associated with any system identified in the Applicable Systems section of CIP-007-6 R2). We become aware of the vulnerability when the vulnerability is discovered and announced. It remains a vulnerability of concern to us until the vulnerable software is either removed from all in-scope systems or modified (e.g., patch or upgrade) on all in-scope systems.

There are three different cases we will examine in mitigating an identified software vulnerability:

1. A patch has been released which addresses the identified vulnerability, and the patch can be applied to all in-scope instances of the vulnerable software within the time constraints of CIP-007-6 R2 Part 2.3.
2. A patch has been released which addresses the identified vulnerability, but that patch cannot be applied to all in-scope instances of the vulnerable software within the time constraints of CIP-007-6 R2 Part 2.3.
3. A vulnerability is announced for which no patch is available.

Livingstone Memorial Light,
Belle Isle, MI
(Photo: L. Folkerth)

Vulnerability Removed by Patching

Figure 1 shows a simplified diagram of the lifecycle of a software vulnerability that can be fixed by applying a patch. The vulnerability is created when software is written or modified. Its vulnerabilities become an issue, and applicable to us, when the software is installed on an in-scope system.

Software vulnerabilities are discovered in many ways: by security researchers, software vendors, malicious actors, etc. As end-users we usually learn about a vulnerability when a patch for it is released, but we may learn about it through other means such as ICS-CERT.

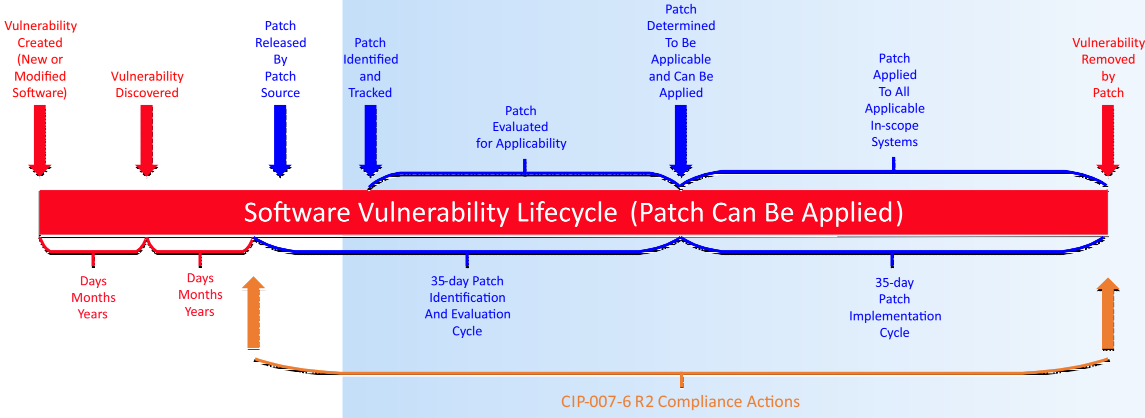

Vulnerability Created (New or Modified Software)
Vulnerability Discovered
Patch Released By Patch Source
Patch Identified and Tracked
Patch Evaluated for Applicability
Patch Determined To Be Applicable and Can Be Applied
Patch Applied To All Applicable In-scope Systems
Vulnerability Removed by Patch
Software Vulnerability Lifecycle (Patch Can Be Applied)
Days Months Years
Days Months Years
35-day Patch Identification And Evaluation Cycle
35-day Patch Implementation Cycle
CIP-007-6 R2 Compliance Actions

Figure 1

Continued on page 8

The Lighthouse

Continued from page 7

To safeguard against these vulnerabilities, CIP-007-6 R2 Part 2.1 requires us to identify a patch source for applicable Cyber Assets. As the definition of Cyber Asset includes the software in the device, we will pull the list of software to be patched from the CIP-010-2 R1 baseline. Each item of software will need a patch source to be identified, if one exists. If there is no patch source, we should document the steps we took to make that determination in case an audit team requests such evidence.

Every 35 days we are required to identify security patches released from a patch source and evaluate those patches for applicability. If the patch addresses a vulnerability that is present on an in-scope system, then that patch is an applicable patch. If the patch is applicable, your documentation should include that fact and the date this determination was made.

For patches that are determined to be not applicable, you should be able to support this determination. This support may range from the results of automated processes to documentation of manual review of the patch.

If a patch is applicable, then that patch must either be applied to remove that vulnerability or that vulnerability must be mitigated by other means. You should also test the patch outside the production environment, if possible, during this time period to ensure the patch can be applied without harming its target systems.

Once evaluation of the patch is complete, it must be applied to all applicable Cyber Assets within 35 days. Actions beginning with the patch release and concluding with application of the patch are subject to compliance review by an audit team. You should document the actions taken so you can clearly show an audit team the steps taken to remediate the vulnerability.

Vulnerability Mitigated Until a Patch Can Be Applied, or In Lieu of Patching

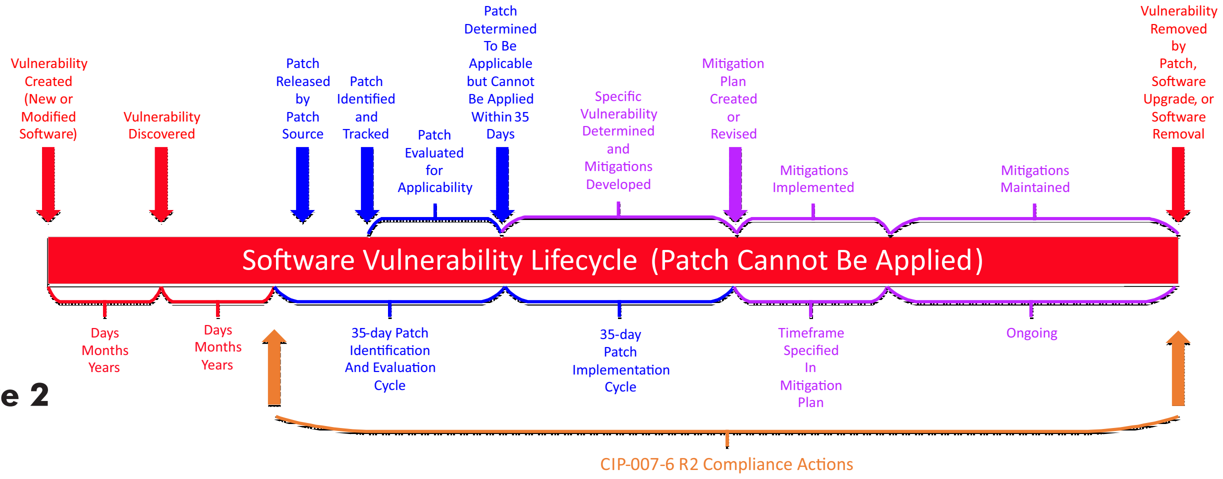

Vulnerability Created (New or Modified Software)
Vulnerability Discovered
Patch Released by Patch Source
Patch Identified and Tracked
Patch Evaluated for Applicability
Patch Determined To Be Applicable but Cannot Be Applied Within 35 Days
Specific Vulnerability Determined and Mitigations Developed
Mitigation Plan Created or Revised
Mitigations Implemented
Mitigations Maintained
Vulnerability Removed by Patch, Software Upgrade, or Software Removal
Software Vulnerability Lifecycle (Patch Cannot Be Applied)
Days Months Years
Days Months Years
35-day Patch Identification And Evaluation Cycle
35-day Patch Implementation Cycle
Timeframe Specified In Mitigation Plan
Ongoing
CIP-007-6 R2 Compliance Actions

Figure 2

Figure 2 shows the case where a patch is available, but will not be applied within 35 days of its evaluation. In this case, CIP-007-6 R2 Part 2.3 requires that, within 35 days of the patch evaluation, a dated mitigation plan be created or that an existing mitigation plan be modified to address the newly identified vulnerability.

The new or revised mitigation plan must contain actions to mitigate the specific vulnerability addressed by the patch, and should explain why the patch was not applied. The mitigation plan must also include a timeframe to complete the mitigating actions.

Once the mitigating actions are complete, these mitigating steps must be maintained and remain in effect until the vulnerability is removed from all in-scope systems or the in scope systems are upgraded or replaced. In all cases the vulnerability must be addressed. Options for vulnerability removal can include:

- applying a patch that fixes the vulnerability,
- upgrading the software to a version that does not have the vulnerability,
- or removing the software from the in-scope system.

Disabling or otherwise rendering the vulnerable software inaccessible is a mitigating action because it does not remove the vulnerability from the affected Cyber Asset. Actions beginning with the patch release and concluding with removal of the vulnerability are subject to compliance review by an audit team.

You should document the actions taken throughout the process, and document the ongoing maintenance of the mitigating actions.

Continued on page 9

The Lighthouse

Continued from page 8

Vulnerability with No Patch Available

In some cases, a vulnerability may be announced without a patch being released to address the vulnerability. This case is not covered by CIP-007-6 R2, but rather by CIP-010-2 R3, Vulnerability Assessments. However, CIP-010-2 R3 only requires a vulnerability assessment to be performed every 15 months. This is far too long to permit a serious vulnerability to exist without mitigation, so I recommend that you integrate a vulnerability mitigation process into your patch management process. This can be done by incorporating vulnerability discovery into your patch evaluation process. If a vulnerability is discovered that does not have a patch available, perform mitigating actions as if a patch was available and could not be installed. Figure 3 shows the vulnerability lifecycle for this case.

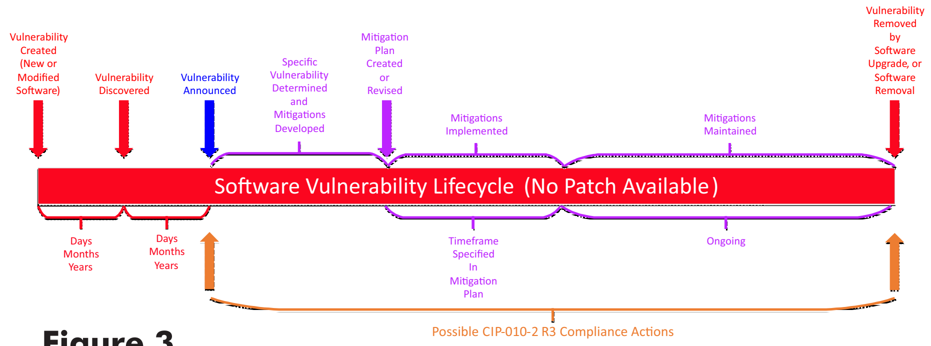

Vulnerability Created (New or Modified Software)
Vulnerability Discovered
Vulnerability Announced
Specific Vulnerability Determined and Mitigations Developed
Mitigation Plan Created or Revised
Mitigations Implemented
Mitigations Maintained
Vulnerability Removed by Software Upgrade, or Software Removal
Software Vulnerability Lifecycle (No Patch Available)
Days Months Years
Days Months Years
Timeframe Specified In Mitigation Plan
Ongoing
Possible CIP-010-2 R3 Compliance Actions

Figure 3

If you do this, be sure to note in your documentation of the vulnerability discovery and mitigation actions that these actions are not subject to CIP-007-6 R2 time constraints. Retain this documentation for use in demonstrating compliance with CIP-010-2 R3.

Possible Elements of a Mitigation Plan

In the case where a vulnerability must be mitigated, the mitigating actions must address the specific vulnerability and should either prevent the vulnerability from being exploited or detect and alert on an attempted or successful exploit of the vulnerability. Generic mitigating actions are unlikely to be acceptable to an audit team. For example, a mitigation plan that says that a firewall and a network intrusion detection system are in use, and that those defenses are sufficient mitigation for the vulnerability, is likely to be unacceptable at audit. Instead, if you show that your firewall blocks a specific port affected by the vulnerability from all except trusted systems, and that your intrusion detection is configured to detect and alert on attempts to exercise the vulnerability, then I expect it would be acceptable to an audit team.

Elements you might use in a mitigation plan include, but are not limited to, one or more of these items:

- Network firewall configuration to block known exploits of the vulnerability;
- Intrusion detection system configuration to detect and alert on known exploits of the vulnerability;
- Network isolation of the affected Cyber Asset;
- Disabling of the vulnerable software;
- Host-based firewalls to block known exploits of the vulnerability;
- Application whitelisting; and
- Removal of the vulnerable software.

Application whitelisting, as applied to real-time control systems, is an emerging technology that holds the promise of being able to mitigate exploits of vulnerabilities before they are even discovered. The most common use of a vulnerability is to exploit it to permit the installation of malicious code. Application whitelisting would then prevent that code from running, thus mitigating the threat of the malicious code. As entities subject to CIP compliance gain experience in this area, I will report on the impact of this technology on the security and reliability of the real-time systems, and on the impact on CIP compliance.

Removal of the vulnerable software is equivalent to applying a patch. (This is known as system hardening and is also a topic that may be addressed in a future issue of The Lighthouse.) Removal of the vulnerable software must be documented as part of the change management of CIP-010-2 R1, and removal of the software makes any associated vulnerabilities not applicable. This is why it is important to only install software that is necessary for normal or emergency operations.

Requests for Assistance

If you are an entity registered with ReliabilityFirst and need assistance, please submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

Entities with Only Low Impact Systems – The Next Steps

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion and to be helpful to you as you strive for continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs. I may also at times discuss areas of the standards that others may be struggling with. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed some light on the sometimes stormy waters of CIP compliance.

With the identification of assets containing low impact BES Cyber Systems completed as of July 1, 2016, let's turn our attention to the remainder of the compliance Requirements for these assets. The next significant compliance date is April 1, 2017. What is needed by April 1, and what steps should we be taking, or already have taken, for the remainder of these Requirements? I'll start at the beginning, and list the steps that I think are needed for compliance for low impact BES Cyber Systems.

Step 1 – Identify assets containing low impact BES Cyber Systems

Yes, this should have been done by July 1, 2016, but I'll cover it again. If you are registered as a Generator Owner (GO) or Transmission Owner (TO) you will almost certainly have at least one asset (a generator or a substation, respectively) that contains a low impact BES Cyber System. Remember that any programmable electronic device (such as a digital relay, a programmable logic controller, or a human-machine interface) that can have an impact on a Bulk Electric System asset within 15 minutes is a BES Cyber Asset.

Each BES Cyber Asset must be part of a BES Cyber System. It does not matter that this device is sitting in a locked cabinet with no connectivity; if it can have a 15-minute impact then it is part of a BES Cyber System.

CIP-002-5.1 R1 Part 1.3 requires that you have a list of all assets that contain a low impact BES Cyber System. This list must have been reviewed and also approved by your CIP Senior Manager, or a documented delegate, on or before July 1, 2016. If you don't have this list I highly recommend that you submit a self-report using WebCDMS.

Step 2 – Identify your CIP Senior Manager

This step also should have been done by July 1, 2016. See this column in the October, 2014, issue for more information here.

Step 3 – Establish your cyber security policies

According to CIP-003-6, a policy is used to communicate your management goals, objectives, and expectations for how you will protect your BES Cyber Systems. The policy should also establish an overall governance foundation that creates a culture of security and compliance. Simply parroting the language of the Standard is not good enough. These policies must reflect how you will approach the tasks of securing your assets and complying with the Standards.

Your policies for your low impact BES Cyber Systems must be approved by the CIP Senior Manager on or before April 1, 2017.

Step 4 – Develop your cyber security plan

CIP-003-6 R2 calls for you to document and implement a cyber security plan by April 1, 2017. This plan must contain all four parts: cyber security awareness, physical security controls, electronic access controls, and Cyber Security Incident response. Be aware that the plan in place on April 1, 2017, must address in some way ALL four parts, even though the physical and electronic controls do not need to be implemented until September 1, 2018. I'll discuss the individual parts of this plan in more detail in Steps 5 through 8.

Point Betsie Lighthouse, Frankfort, MI
(Photo: L. Folkerth)

Step 5 – Implement the plan for cyber security awareness

Effective April 1, 2017, CIP-003-6 R2 Attachment 1 Section 1 requires that you reinforce cyber security practices with your personnel at least once every 15 calendar months. Two of the most common methods of delivering the security reinforcement are by email to all applicable personnel or by signs or posters at the Cyber Asset locations. For example, an entity might purchase posters addressing security awareness and post them at the primary entrances to its protected assets. This gets progressively more difficult as the number of assets increases. Entities with large numbers of assets generally opt for reinforcement by email, targeting the personnel with access to the protected assets.

As a good practice, I recommend performing this security reinforcement much more often than once every 15 months. SANS, as part of its Securing the Human initiative, publishes a monthly security awareness newsletter called "Ouch!" This newsletter is free and may be distributed within your organization for free. Unless you have your awareness program already established, I suggest you consider using "Ouch!" as a

Continued on page 9

Continued from page

resource to enhance your program. The newsletter can be found here.

Step 6 – Develop, test, and maintain an incident response plan

CIP-003-6 R2 Attachment 1 Section 4 also becomes effective April 1, 2017. Section 4 calls for you to develop a Cyber Security Incident response plan, test it periodically, and maintain it as necessary.

An incident response plan is not a substitute for expertise, but a way to guide the response team and to make sure no steps are skipped, and that the appropriate policies are followed when examining and restoring your systems. The time to decide policy-level matters regarding an incident is when you build the incident response plan, not when you're in the middle of an incident. For example, if your cyber security policy says that you will preserve evidence of an incident for possible prosecution, then the appropriate forensic evidence collection and chain-of-custody steps must be included in the incident response plan, and the appropriate response team members must be trained in these protocols.

An excellent resource for building your incident response plan is NIST's Computer Security Incident Handling Guide, SP 800-61, available here. In addition to the steps laid out in this Guide, you will need to add processes for determining whether an incident is a Reportable Cyber Security Incident, and the steps for reporting it to the appropriate agencies, which must include the E-ISAC.

You might also consider coordinating incident response with your state's fusion center. These centers facilitate information sharing between various law enforcement agencies, intelligence agencies, and private industry.

CIP-003-6 R2 Attachment 1 Section 4.5 requires testing your incident response plan every three years. I strongly suggest you exercise your incident response capabilities on a much more frequent basis. I recommend quarterly exercises, varying the exercises in different ways. For example, you should vary the participants in an exercise, simulating the case where a major team member is unavailable. Vary the target of the incident, the type of incident, etc.

The idea is to practice so that your incident response team is comfortable and confident working together, and each team member understands the skill levels of other team members and the overall resiliency of the plan is confirmed.

I recommend building a general checklist, perhaps one or two pages long, of the common response steps in the incident response plan. When the plan is activated, whether as a test or for real, this checklist is filled out by the team leader. The checklist becomes a record that the plan was implemented, and can serve as evidence for audits. The completed checklists prevent two common adverse audit findings by showing that a test of incident response was performed, and that the incident response plan was actually used to respond to the incident. See Table 3-5 in NIST's Computer Security Incident Handling Guide for a starting point in developing this checklist.

Step 7 – Implement the plan for physical security controls

While the September 1, 2018, effective date for CIP-003-6 R2 Attachment 1 Section 2 seems like a long time away, it is actually not much time at all in the physical security realm. You should know what changes are needed to implement your physical security controls, how long the changes will take, and where the budget dollars are coming from.

Step 8 – Implement the plan for electronic security controls

The provisions for the electronic security controls in CIP-003-6 R2 Attachment 1 Section 3 also have an effective date of September 1, 2018. You should have a good idea at this point of how you're going to approach implementing these controls. However, be aware that this language is under revision and the present language will probably be changed by the Standards Drafting Team revising the CIP Standards. I strongly recommend that you monitor and participate in the development of the revisions for these Standards. The project page is located here.

Additional Resources

An additional information resource, NERC recently held advisory sessions regarding implementing the controls for assets containing low impact BES Cyber Systems. The recording and slide deck are available here.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance, remember RF has the Assist Visit program. All you need to do, to request help, is submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

In-depth Considerations for Electronic Access Points

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive for continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs.

There are times that I may also discuss areas of the Standards that other entities may be struggling with and attempt to share 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.

Electronic Access Points

The first three versions of CIP-005 required identification and documentation of each Electronic Security Perimeter (ESP) and all access points to the ESPs. The term “access point,” while not explicitly defined, was understood to be a Cyber Asset that controlled access into an ESP. That changed on July 1, 2016, when CIP-005-5 became effective.

CIP-005-5 includes a new term, “Electronic Access Point (EAP),” which is defined in the NERC Glossary as, “A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.” This term, EAP, is extremely important to the remainder of our discussion here, so let's read the definition carefully.

The EAP is not a Cyber Asset as we understood it to be in CIP V3, but it is an interface, such as a network interface card, on a Cyber Asset. In addition, we see that the interface is the line of demarcation between the ESP and the rest of the world. Cyber Assets “inside” the interface are within the ESP, those that are “outside” the interface are not. To see why we should be concerned about this, let's look at a few examples.

Figure 1 shows a simple ESP protected by a firewall. The “inside,” or ESP-facing, interface is designated as the EAP. CIP-005-5 R1 Part 1.3 is applicable to EAPs for high and medium impact BES Cyber Systems, and states, “Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”

In other words, the interface must have inbound and outbound rules, and each rule must be documented with the reason it is needed.

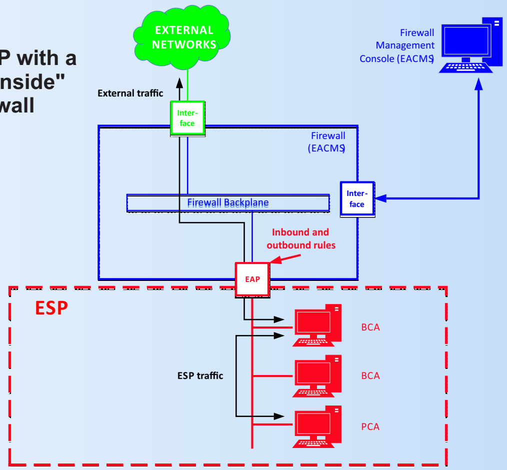
Figure 1 also shows that in this configuration the firewall is outside the ESP, and is therefore treated as an Electronic Access Control and Monitoring System (EACMS).

The firewall management console is shown as being outside the ESP as well, but must also be treated as an EACMS since the rules are stored and managed on this device.

So far there should be no surprises for anyone who has been keeping up to date by studying the CIP V5 Standards. But now it gets trickier. Let’s see what happens if we change the location of the EAP from the inside firewall interface to the outside firewall interface. Figure 2 illustrates this.

Holland, MI (Photo: L. Folkerth)

Figure1 - Simple ESP with a Single EAP as the "Inside" Interface of the Firewall



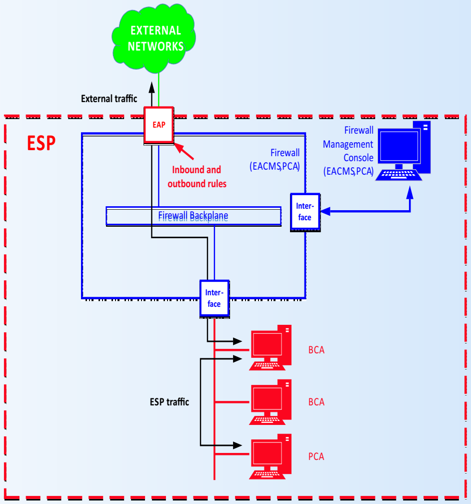


Figure 2 - Firewall Configured with the EAP on the “Outside” Interface

Continued on page 7

Continued from page 6

Note that the firewall is now inside the ESP, and therefore meets the definition of both an EACMS and a Protected Cyber Asset (PCA). Adding the PCA designation means complying with the Interactive Remote Access requirements of CIP-005-5 R2 and the physical port protections of CIP-007-6 R1 Part 1.2.

If the firewall management console is to be directly connected to the firewall, the console must also be within the ESP. If the console is outside the ESP, it must connect through the firewall or some other means of electronic access control, and must be considered as Interactive Remote Access.

Why would anyone implement a network like Figure 2? You probably wouldn't want the added complexity for most purposes, but it lays the groundwork for Figure 3.

Figure 3 - Firewall with Two "Outside" EAPs

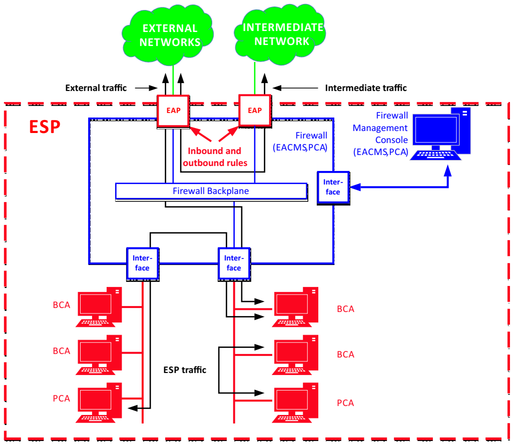


Figure 3 shows a firewall with EAPs identified at two external interfaces, "external" and "intermediate."

This keeps the firewall within the ESP as in Figure 2, but adds an extra consideration. Traffic between the two external interfaces is flowing within the ESP via the firewall backplane.

This means that inbound and outbound rules must be in place to control such traffic. This also holds true if there is one physical external interface using virtual networking to separate the external network from the intermediate network.

The switching and traffic flow still uses the firewall's backplane and is therefore within the ESP.

The final case we'll consider is Figure 4, where we'll use multiple "internal" interfaces to create zones of trust within the ESP.

Figure 4 - Firewall with Two EAPs Defined on "Inside" Interfaces

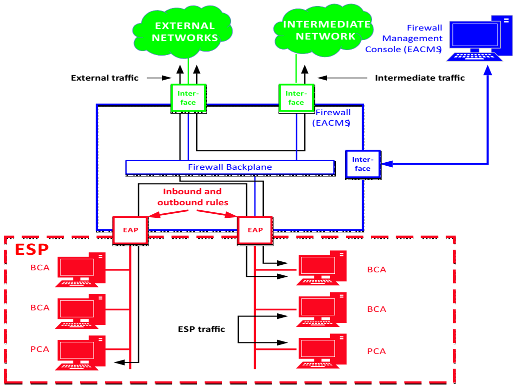


Figure 4 shows an ESP with two zones of trust. This might consist of the field communications network including the SCADA front end processors as one trust zone, and the SCADA servers and consoles as another trust zone. (See the next issue of this Newsletter for more about trust zones and virtual networks.)

Figure 4 makes it clear that traffic from one trust zone leaves the ESP, traverses the firewall backplane, and re-enters the ESP in the second trust zone. Per CIP-005-5 R1 Part 1.2, rules must be in place to control this access.

Expect any audit team encountering this configuration to closely examine the rules, and the reasons for the rules, associated with each EAP.

Requests for Assistance

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

All you need to do is submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

Transient Cyber Assets and Removable Media

North Breakwater Light, Ludington, MI (Photo: L. Folkerth)

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive for continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs.

There are times that I may also discuss areas of the standards that other entities may be struggling with and attempt to share 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.

Q If I have a CIP audit scheduled in 2017, will I be audited on the new requirement for Transient Cyber Assets and Removable Media? If so, what can I expect the auditors to ask?

A If a ReliabilityFirst audit team is leading your audit, and the audit occurs after April 1, 2017, then CIP-010-2 R4 will probably be in scope. For details, see NERC's 2017 ERO Enterprise CMEP Implementation Plan, Version 2.2, December 2016, page 46.

Achieve the Objective

Like other CIP v5 Requirements, you will need to provide the audit team with sound processes and sufficient, appropriate evidence of compliance. Unlike other CIPv5 Requirements, you will need to provide something more.

Many of the subsections of CIP-010-2 R4 Attachment 1 require you to "achieve the objective" of that subsection. In order to demonstrate how you have achieved each objective, you will need to provide the audit team with an explanation of how your processes meet that objective.

This explanation could take many forms. Some possibilities include a description in the RSAW Compliance Narrative, a section in a process (or policy), or a separate document describing achievement of the objective.

Let's look at one of the Sections in Attachment 1 that includes this language. Section 1.3 requires you to "achieve the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset." It also says you may use one or a combination of methods such as security patching, execution from read-only media, system hardening, or "Other method(s) to mitigate software vulnerabilities."

By including "other methods" in the list of options to comply with this Section, Section 1.3 is telling you to do anything you feel needs to be done to protect the Transient Cyber Asset from the risk of unpatched software.

This is the epitome of a non-prescriptive, results-based Standard, and gives you a free hand in the methods you use to comply with the Standard.

However, with this freedom comes added responsibility. Your evidence of compliance will need the following elements in some form in order to document that you have achieved the objective of mitigating the risk of vulnerabilities posed by unpatched software on the Transient Cyber Asset:

- A documented plan to protect the Transient Cyber Asset (per the R4 base Requirement);

Continued on page 10

The Lighthouse

Continued from page 9

- The plan must include the methods you employ to protect the Transient Cyber Asset from the risk introduced by unpatched software;
- The plan (or other documentation) must show how methods documented in the plan achieve the objective; and
- Evidence that these methods are applied consistently and reliably for each applicable Transient Cyber Asset.

Another aspect to consider is that if a BES Cyber System or a Protected Cyber Asset is compromised, and if one element of the compromise was a vulnerability posed by unpatched software on a Transient Cyber Asset, then that might be considered a violation of CIP-010-2 R4 Attachment 1 Section 1.3.

The reasoning would be that you have failed to “achieve the objective” as required by the Standard. We’ll need to see how this plays out if the circumstance ever occurs.

This example focused on on Transient Cyber Assets, but similar considerations apply to Removable Media.

Per Transient Cyber Asset Capability

Some Sections of Attachment 1 include the provision “per Transient Cyber Asset capability.” The CIP-010-2 Guidelines and Technical Basis states that this phrase is to eliminate the need for Technical Feasibility Exceptions for cases where the Transient Cyber Asset cannot perform a certain function, such as native anti-virus protection.

This language, however, does not relieve you of the requirement to achieve the objective of each Section in which it occurs. Let's use Section 1.3 again as an example. Suppose you have a Transient Cyber Asset that is at end-of-life and cannot be patched, that cannot use a live operating system from read-only media, and cannot be hardened.

There may still be mitigations that can be applied. In this example, you might restrict physical access to the Transient Cyber Asset, restrict its network connectivity to only trusted networks, and periodically perform a manual review to look for unauthorized programs or services running on the device.

Whatever protections for the Transient Cyber Asset you choose to use, you must be sure to document the reason “conventional” protections cannot be applied, and also document the protections you do implement. Again, you will need to be prepared to explain to an audit team how you “achieve the objective” of each Section and share the appropriate examples of evidence that illustrate its outcome.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. All you need to do is submit an Assist Visit Request via the RF web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Virtual Systems and Zones of Authority

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive for continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs. There are times that I may also discuss areas of the Standards that other entities may be struggling with and attempt to share 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.

Q Does the present version of the CIP Standards permit the use of virtualization? If so, what types of virtualization are permitted and how should I approach CIP compliance?

A while the present CIP Standards do not explicitly permit use of virtualization, neither do they explicitly prohibit its use. There are three general types of virtual systems: virtual machines, virtual networks and virtual storage. Each type has its own advantages and its own operational, security and compliance risks. The topic of virtualization is, in fact, so complex that a thorough discussion isn't possible within this article. What I will discuss here is what I think is one major source of misunderstanding regarding this topic. I will also introduce the concept of a “zone of authority,” explain what it means and explain how it affects the topic of virtualization.

When Responsible Entity personnel and Compliance Enforcement Authority (CEA) personnel discuss compliance with the NERC CIP Standards, each group brings to the discussion a different viewpoint.

Responsible Entity personnel see their entire network as a whole, with the parts of that network subject to CIP compliance as part of a larger security picture. They can see the protections afforded to all systems, and can see how the protections applied to non-CIP assets increase the security of CIP assets as well.

CEA personnel, on the other hand, only have CIP assets within their purview. They cannot consider non-CIP assets as adding to the entity's security posture, as those assets are not under the CEA's regulatory authority. Non-CIP assets are not subject to audit by the CEA and may change at any time with no notification to the CEA.

This difference in viewpoint can lead to conflicting views of virtual systems such as virtual networks. Responsible Entity personnel see the protections applied to the non-CIP networks that might share, for example, a physical switch with CIP networks. They see the multiple layers of protection and the controls surrounding the security of these non-CIP networks.

CEA personnel, on the other hand, do not have the authority to review the security level of non-CIP assets or networks. The CEA personnel must therefore assume that any non-CIP assets or networks could be compromised and used in attacks on the in-scope CIP assets and networks. The resulting differences in the perception of risk can be a source of misunderstanding between Responsible Entity personnel and CEA personnel.

I call this difference in perspective “mixed zones of authority.” The Responsible Entity's zone of authority is all of its owned assets, both CIP and non-CIP. The CEA's zone of authority is limited to assets that are in scope for CIP.

For this reason, and others that I don't have the space to go into here, I strongly recommend that Responsible Entities refrain from implementing Cyber Assets or networks that mix CIP in-scope and out-of-scope assets, network traffic, or data. The reason for not mixing in-scope and out-of-scope is not, as is commonly discussed, that “untrusted” configurations are implemented.

Grand Traverse Lighthouse, Northport, MI (Photo: L. Folkerth)

The biggest issue, in my view, is that without being able to view all aspects of the systems used for BES reliability, there is no way for the CEA to ensure that weak or high-risk configurations are not implemented.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. All you need to do is submit an Assist Visit Request here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Grand Island East Channel Light, Munising, MI – Photo: L Folkerth

Vulnerability Assessments

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive for continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs.

There are times that I may also discuss areas of the standards that other entities may be struggling with and attempt to share 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.

Q CIP version 3 told the industry what it needed to do in order to perform a vulnerability assessment, but CIP version 5 gives only general direction. Can this language actually be enforced? If so, what must the industry do to avoid violating that language?

A CIP version 3 was indeed quite specific in laying out the minimum requirements for a cyber vulnerability assessment. The Systems Security Management - Cyber Vulnerability Assessment Standard (CIP-007-3 R8) applied to all Cyber Assets within an Electronic Security Perimeter (ESP), and implicitly removed any other elements from compliance review by explicitly requiring four elements in the vulnerability assessment. Similarly, the Electronic Security Perimeter - Cyber Vulnerability Assessment Standard (CIP-005-3 R4) applied to all access points to an ESP, and contained five required elements. These two Requirements were very prescriptive and left little room for flexibility.

Risk-based Requirements

Most of the Requirements in CIP version 5 are written as Risk-based Requirements (See NERC Rules of Procedure, Appendix 3A, Section 2.4). The remainder are written as Capability-Based Requirements (e.g., incident response).

The prescriptive Requirements CIP-005-3 R4 and CIP-007-3 R8, Cyber Vulnerability Assessment, were replaced in CIP version 5 by the Risk-based Requirement Vulnerability Assessments Standard (CIP-010-2 R3). Because CIP-010-2 R3 is a Risk-based Requirement it requires you to reduce a risk posed to the BES. This risk is stated in Section A.3, Purpose, as "compromise that could lead to misoperation or instability in the Bulk Electric System (BES)."

Effective Processes

CIP-010-2 R3 leaves many of the terms used in the Requirement undefined, and the Standard grants wide flexibility in how an entity may comply with the Requirement. With this flexibility, however, comes responsibility. As a Responsible Entity, you must be able to show how your processes that address these Requirements are effective in reducing risk.

Why do I say "effective?" That's because the ERO Enterprise (NERC and the eight Regional Entities) is becoming more risk focused. A process that is not effective presents an elevated risk to the BES. Also, from a business perspective, does it make sense to expend resources on a process that isn't effective?

What does an effective process look like? An effective process will achieve the security purpose of the Requirement, will produce sufficient and appropriate evidence of compliance, and will be sustainable for long-term operations.

An effective process will very likely also include internal controls designed to keep the process effective and consistent by identifying, assessing and correcting issues.

Discussion of CIP-010-2 R3

Let's examine the four Parts of CIP-010-2 R3 individually.

Part 3.1

Part 3.1 requires a vulnerability assessment at least every "CIP year," or once every 15 calendar months. Be sure to include every Cyber Asset that is in scope for CIP at the high or medium impact level. Also note that the deadline for the initial performance of this Requirement is coming up very soon on July 1, 2017.

For guidance in how to achieve the security purpose of a vulnerability assessment, the Guidelines and Technical Basis refers to NIST SP800-115, "Technical Guide to Information Security Testing and Assessment."

Continued on page 10

Continued from page 9

I also recommend NIST SP800-30, “Guide for Conducting Risk Assessments,” where you will find some useful definitions, as well as much discussion of how to assess and manage risk in the cyber environment.

In developing your vulnerability assessment processes, I strongly recommend monitoring or discovering vulnerabilities much more frequently than the required annual timeframe, possibly something more like a weekly or monthly review augmented with a full annual assessment.

Microsoft Releases Patch for End-of-life Systems

In an unprecedented response to the “WannaCry” malware campaign, Microsoft released patches for Windows Vista, Windows XP, and Windows Server 2003 on May 13, 2017. Entities with any of these systems in scope for Systems Security Management - Security Patch Management Standard CIP-007-6 R2 should take note and ensure that patch sources are properly identified and that this patch is entered into the patch management process.

A good example of why this is needed is the recent “WannaCry” ransomware outbreak (see sidebar). This is a malware campaign that exploited a vulnerability that was made public only a few weeks before the outbreak. As an industry, we need to be moving toward a continuous vulnerability management program. I hope to have more on this topic in a future article.

Part 3.2

Part 3.2 requires an “active” vulnerability assessment at least every three years. NIST SP800-115 provides more information on “active” assessments. Note that the initial performance date for this Requirement is July 1, 2018.

Part 3.3

For high impact BES Cyber Systems, Part 3.3 requires an “active” assessment for all new systems prior to being placed in production. Note that this Requirement is in place now, and has been in force since July 1, 2016.

Part 3.4

Part 3.4 requires you to document the results of the assessments, develop an action plan to address any identified vulnerabilities, and track the execution status of the action plan. In my opinion, a mature vulnerability assessment process will produce a concise report targeted to the CIP Senior Manager. This report will not include hundreds of pages of raw vulnerability scanner output (although that type of evidence should be available in case it is needed), but will contain information that can be understood by someone not deeply technical. My suggested format for such a report would look something like this:

- Scope of the assessment
- Description of the techniques used (manual review of vulnerability sources, automated tools, etc.)
- Brief description of vulnerabilities identified
- The approach that will be used to address the vulnerabilities identified
- A timeline for completion
- Future actions needed
- Lessons learned

If the report is more than two or three pages long, you may want to begin with an executive summary.

Enforceability

I would like to see the industry as a whole show its maturity in the cyber security area by going well beyond the minimum Requirement language to implement what's needed to keep our systems secure in this ever more challenging environment.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Mission Point, MI – Photo: L Folkerth

Compliance Guidance

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive for continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs. There are times that I may also discuss areas of the standards that other entities may be struggling with and attempt to share 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.

Q I'm having trouble understanding a CIP Requirement. Where can I go for guidance on what a Requirement means or how to implement it?

A The nature of compliance guidance available to you is changing. In this column, I will discuss compliance guidance and show you when and how to use it. I will also give you pointers for reducing your dependency on compliance guidance.

What is compliance guidance?

Compliance guidance is any document that assists the ERO Enterprise (NERC and the Regional Entities) and industry in reaching a common understanding on how compliance with a NERC Reliability Standard (Standard) can be achieved and demonstrated. NERC's Compliance Guidance Policy, enacted in November of 2015, directs a major shift in the way compliance guidance documents are developed, reviewed, approved, and published. The Compliance Guidance Policy identifies two types of compliance guidance, Implementation Guidance and CMEP Practice Guides (see sidebar).

Under the Compliance Guidance Policy, any new compliance guidance and all existing compliance guidance will be incorporated into either Implementation Guidance or CMEP Practice Guides. Examples of this ongoing effort are numerous. First, most of the CIP Version 5 Frequently Asked Questions and Lessons Learned have been incorporated into Implementation Guidance. Second, the Compliance Application Reports have been removed from the NERC web site and if they return, they will probably return as Implementation Guidance. Third, and finally, there was some informal discussion at this June's NERC CIPC meeting that some of the sections within the NERC Standards, such as Guidelines and Technical Basis, could be moved to independent documents and published as Implementation Guidance.

> **Compliance Guidance Policy**
>
> **Implementation Guidance:** Examples or approaches to illustrate how Registered Entities could comply with a Reliability Standard.
>
> **CMEP Practice Guides:** Address how Compliance Monitoring and Enforcement Program (CMEP) staff execute compliance monitoring and enforcement activities.

As new compliance guidance is created, or as existing guidance documents are revised, expect to see them appear in the new framework as Implementation Guidance or CMEP Practice Guides.

Reducing Dependence on Compliance Guidance

While compliance guidance can be useful, using guidance as the primary basis for high-value decisions may not be wise. The following points are, in my opinion, reasons to minimize reliance on compliance guidance:

- Implementation Guidance and CMEP Practice Guides are subject to change based on actions outside of ballot body or Applicable Governmental Authority approval.
- While compliance guidance may assist us in understanding what a Standard means, it cannot change the plain language of the Standard.
- A formal Interpretation may cause some compliance guidance to become obsolete.
- Compliance guidance does not go through the same development and approval process as a Standard.

In light of these limitations, I offer the following suggestions for ensuring compliance with the Reliability Standards and for reducing your dependence on compliance guidance:

A. Read the Standard Carefully

It is commonly understood that the NERC Reliability Standards are mandatory and enforceable. But what does not appear to be widely understood is that only certain parts of a Standard are approved by an Applicable Governmental Authority (FERC in the U.S.) as mandatory and enforceable. Those parts are listed in the Standard Processes Manual (NERC Rules of Procedure Appendix 3A) at the end of Section 2.5:

> "The only mandatory and enforceable components of a Reliability Standard are the:
>
> (1) applicability,
> (2) Requirements, and the
> (3) effective dates.
>
> The additional components are included in the Reliability Standard for informational purposes, to establish the relevant scope and technical paradigm, and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority." [reformatted from original]

The "Glossary of Terms Used in NERC Reliability Standards" (NERC Glossary) contains terms and

Continued on page 13

The Lighthouse

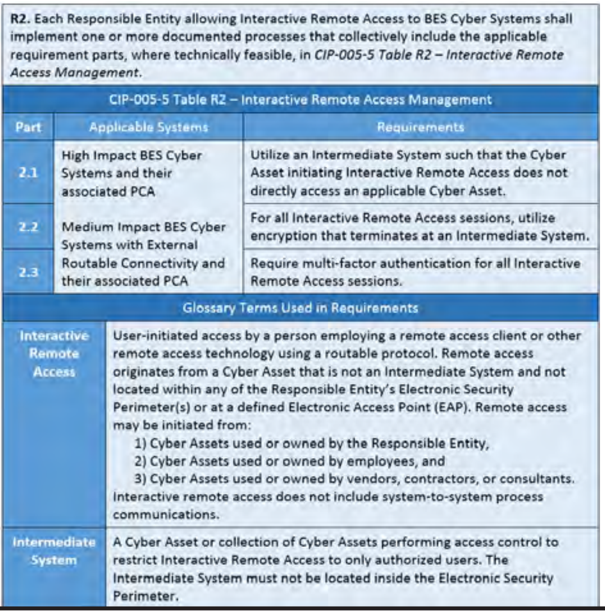
Continued from page 12

definitions that are also approved by an Applicable Governmental Authority (see Standard Processes Manual Section 5.2). Whenever these terms appear in a Standard, they are capitalized. For example, if a Standard uses the term "Facility" it is referring to the NERC Glossary definition. If it uses "facility," then the common meaning of the term applies.

The text of the Reliability Standard includes the Applicability and Requirements. Effective dates may be included in the Standard, but are more frequently specified in a separate implementation plan document that is approved by an Applicable Governmental Authority along with the Standard.

A Reliability Standard may also include formal Interpretations (note the capital "I") that, when approved by an Applicable Governmental Authority, become a mandatory and enforceable part of the Standard. Interpretations are a clarification of what the Standard means, and has always meant. That is why there is never an implementation plan for an Interpretation. The Interpretation becomes effective when approved by an Applicable Governmental Authority and clarifies what the Standard has meant since the Standard became effective. The development of Interpretations is governed by the Standard Processes Manual, Section 7.

Figure 1 - The Enforceable Parts of CIP-005-5 R2



R2. Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in *CIP-005-5 Table R2 – Interactive Remote Access Management*.

CIP-005-5 Table R2 – Interactive Remote Access Management		
Part	**Applicable Systems**	**Requirements**
2.1	High Impact BES Cyber Systems and their associated PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
2.2		For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.
2.3		Require multi-factor authentication for all Interactive Remote Access sessions.

Glossary Terms Used in Requirements	
Interactive Remote Access	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

When I am reading a Standard or Requirement, I focus on the enforceable language. I refer to compliance guidance only when the plain language of a Requirement is insufficient to explain the full meaning of the Requirement. When studying a Requirement, I sometimes condense the Requirement into a document containing only the enforceable language. Figure 1 gives an example of this approach for CIP-005-5 R2, Interactive Remote Access Management. Note that I include terms from the NERC Glossary that, when read along with the Standard, will help me understand the Requirement. I also include the text of any applicable Interpretations. If you adopt this technique, be careful not to change the language of the Standard. You can modify the formatting, but the language of the Standard must remain intact.

B. Make Sure You Understand the Meaning of Key Terms

In reading a Standard, it is very important that you understand the meaning of each term used in any of the enforceable language. There are many resources available for this. NERC documents that contain definitions include:

NERC Glossary: Terms used in a Reliability Standard that appear in the NERC Glossary are capitalized; read the definition of each term just as carefully as you read the language of the Standard. These terms are part of the mandatory and enforceable language of the Standard.

NERC Rules of Procedure Appendix 2: This document contains the definitions of many terms, some of which may be applicable to a Standard.

Verbs Used in Reliability Standards: This list appears in Attachment A of the Drafting Team Reference Manual, and is a list of verbs used in the Standards and their definitions.

Other, less official, sources of definitions include:

Merriam-Webster's Collegiate Dictionary, 11th Edition: This is, unofficially, the preferred dictionary of the ERO.

Other Dictionaries: In the cases where Merriam-Webster is unhelpful, other dictionaries may be used. I suggest referring to a paper dictionary, not an online dictionary. One that I use frequently is the American Heritage Dictionary of the English Language, 5th Edition. For example, the term "vendor" in the definition of Interactive Remote Access (see Figure 1) is not a defined term in any of the NERC sources. Merriam-Webster's definition isn't helpful. The American Heritage definition, "2. One who provides products or services to a business for a fee," works well in this context.

If a term is used in another Standard, examine the meaning of the term in that Standard. Be careful that you consider the context of the use of the term in each Standard.

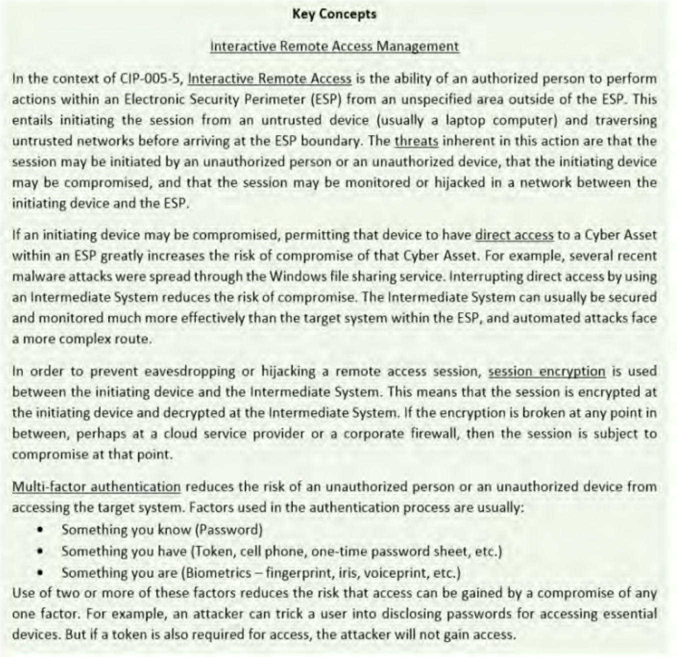
C. Make Sure You Understand the Key Concepts of the Standard

The Standards do not exist in a vacuum. The language of each Requirement assumes some knowledge of the general subject area covered by the Requirement. I think of this underlying subject matter as "key concepts." When I'm providing outreach or training on a Requirement, I find that identifying the key concepts helps me organize my thinking about the Requirement. I also communicate the key concepts if my audience is not fully conversant with them. This provides a common foundation on which to build understanding of the Requirement. For example, if I am providing training on CIP-005-5 R2, Interactive Remote Access Management, I use the key concepts shown in Figure 2. Keep in mind that these "key concepts" are something I have made up,

Continued on page 14

Continued from page 13

Figure 2 - Key Concepts



Key Concepts

Interactive Remote Access Management

In the context of CIP-005-5, Interactive Remote Access is the ability of an authorized person to perform actions within an Electronic Security Perimeter (ESP) from an unspecified area outside of the ESP. This entails initiating the session from an untrusted device (usually a laptop computer) and traversing untrusted networks before arriving at the ESP boundary. The threats inherent in this action are that the session may be initiated by an unauthorized person or an unauthorized device, that the initiating device may be compromised, and that the session may be monitored or hijacked in a network between the initiating device and the ESP.

If an initiating device may be compromised, permitting that device to have direct access to a Cyber Asset within an ESP greatly increases the risk of compromise of that Cyber Asset. For example, several recent malware attacks were spread through the Windows file sharing service. Interrupting direct access by using an Intermediate System reduces the risk of compromise. The Intermediate System can usually be secured and monitored much more effectively than the target system within the ESP, and automated attacks face a more complex route.

In order to prevent eavesdropping or hijacking a remote access session, session encryption is used between the initiating device and the Intermediate System. This means that the session is encrypted at the initiating device and decrypted at the Intermediate System. If the encryption is broken at any point in between, perhaps at a cloud service provider or a corporate firewall, then the session is subject to compromise at that point.

Multi-factor authentication reduces the risk of an unauthorized person or an unauthorized device from accessing the target system. Factors used in the authentication process are usually:

- Something you know (Password)
- Something you have (Token, cell phone, one-time password sheet, etc.)
- Something you are (Biometrics – fingerprint, iris, voiceprint, etc.)

Use of two or more of these factors reduces the risk that access can be gained by a compromise of any one factor. For example, an attacker can trick a user into disclosing passwords for accessing essential devices. But if a token is also required for access, the attacker will not gain access.

and that they are not vetted or part of any official document.

D. Prioritize Your Use of Compliance Guidance

I generally refer to compliance guidance in the following order:

1. Guidance contained in the Standard, such as Purpose, Background, Rationale, or Guidelines and Technical Basis.
2. Approved Implementation Guidance or CMEP Practice Guides. I will include the active Compliance Application Notices in this review until they are superseded.
3. The Reliability Standard Auditor Worksheet (RSAW) for that Standard. The RSAW is the auditor's tool that is the basis for audit activities. In some cases the way the RSAW is worded may shed light on the meaning of a Requirement.
4. Compliance documents from the RF web site. For example, the RF version of the CIP Version 5 Evidence Request is located in the CIP Document Library.
5. "Compliance Tools and Auditor Resources" on the NERC web site.
6. "ERO Enterprise Compliance Auditor Manual" on the NERC web site.
7. The FERC order approving the Standard. Referring back to the order provides significant guidance as to how a governmental authority read the language. The order also outlines the Standard's intended purpose.
8. The development record of the Standard. This is filed with FERC as part of NERC's petition for approval. The drafting team's consideration of comments can sometimes be useful in determining the intended meaning of the Standard.
9. NERC and Regional Entity newsletters, webinars, conference presentations, white papers, etc. These typically receive a review at the NERC or the Regional Entity level before they are published.

E. RF Assist Visits and Other Outreach Activities

RF developed and maintains an "Assist Visit" program. This program is available to all entities registered with RF. Assist Visits are a form of targeted training, and provide a useful way to discuss topics of interest with staff from multiple RF departments. They may be as simple as a short conference call or webinar, or they may involve an on-site visit by RF staff. See "Requests for Assistance" below.

RF also holds Compliance Workshops twice a year. Details are always posted on the RF web site.

F. Be Critical of New or Revised Standards

One of the best ways to reduce your need to rely on compliance guidance is to ensure that the Standards are written to be clear and unambiguous. Registered Entities can take several steps to help out in this area. Whenever a new or revised Standard is posted for comment or ballot, be sure to use the techniques described above to make sure the enforceable parts of the Standard are clear and understandable, that you will be able to implement the Standard, and that upon implementation you will be able to produce evidence of compliance that will demonstrate clearly to an audit team that you have complied with the Standard. After performing this review, if you identify issues, be sure to highlight those issues by submitting a comment on the Standard.

Another option is to volunteer your services on a Standard Drafting Team. Also, if you are a member of a trade association, make sure your association's vote reflects your views.

Conclusion

I encourage you to read the Compliance Guidance Policy I referenced above. This will give you a picture of where compliance guidance is heading and will help you to know any of the limits associated with future guidance. I also encourage you to try the techniques above the next time you have a question about a Standard. Please let me know how they work for you.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. All you need to do is submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Frankfort North Pier, MI – Photo: L Folkerth

Defense Against the Dark Auditor

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive for continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs.

There are times that I may also discuss areas of the standards that other entities may be struggling with and attempt to share 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.

Q I just heard a phrase I don't understand, "Defense against the dark auditor." What is a "dark auditor" and how do I defend against one?

A Since my first exposure to the phrase "Defense against the dark auditor," when I chuckled at the play on words and the Harry Potter reference, I have heard it several times in different contexts.

I believe the concept of the "Dark Auditor" is a myth, founded in misunderstanding of the Standards and the audit process. In this article I will explain where I think this term came from. I will also propose some practices you can put in place to make sure you stay out of the clutches of such a mythological beast.

What is "Defense against the dark auditor?"

In general, "Defense against the dark auditor" appears to mean measures taken to avoid findings of possible non-compliance (PNC), in other words an adverse audit finding. But the phrase also includes the implication that the audit teams are going beyond a reasonable meaning of the Standard, digging to find non-compliance, or engaging in some other behavior to try to find a PNC where no reasonable finding exists.

The Meaning of a Standard

Auditors must sometimes take a stance on the intent and meaning of a Standard that is different from the way a Registered Entity (entity) understands and reads the Standard. The auditors are trained to read each Standard in a way that preserves the ability to enforce the Standard consistently for all entities. This can be perceived as an auditor taking an unreasonable stance on the meaning of a Standard.

Audit Processes

A compliance auditor actually performs two audits at once. The first is a performance audit, where the auditor takes a broad look at an entity's controls to determine that implementation of these controls will result in secure and compliant systems. The controls reviewed may include policies, plans, process, procedures, or other documents that an entity uses to maintain security and compliance.

The compliance auditor also performs a compliance audit to assess an entity's compliance with a Standard based on sufficient, appropriate evidence. When sufficient evidence is not provided in the initial submittal, the auditor must request additional evidence. This is known as "stacking" evidence and is used to strengthen weak evidence so that the total evidence package is sufficient to demonstrate compliance.

Sometimes several layers of stacking evidence may be needed. It may certainly appear to an entity under the stress of an audit that the auditor is digging to find non-compliance, but the reality is that the auditor is evaluating additional evidence in order to find compliance.

I recall one audit where the entity's management refused to submit additional evidence because they thought I was trying to find them non-compliant. I had to explain to them that my team did not yet have sufficient evidence of compliance, and that stopping at that point would result in a PNC.

Continued on page 10

The Lighthouse

Continued from page 9

Management relented, and their staff was able to find and submit the appropriate evidence needed for a "No Finding." In many cases an explanation of what the auditor is looking for and description of the material needed helps our entities better understand what the auditor needs to assure compliance.

Auditors may also ask for a live demonstration of a system. This is done to help an entity show and document compliance, especially where available evidence is weak, and is an opportunity given to the entity to demonstrate the effectiveness of its systems and processes.

Live demonstrations are especially effective when automated systems are employed to manage compliance or compliance evidence. An entity may also request that a live demonstration be used to provide evidence, where this is appropriate.

Unfortunately there are times an audit team needs to ask for additional evidence even when a PNC has already been established. This is done to determine the extent of the violation. The entity may perceive this as diving deeper into the evidence than what is necessary. This review of evidence is done in order to establish the duration of the PNC.

This material will be needed at some point by RF's Enforcement Group. It is frequently easier for the audit team to request and review this evidence on-site, than for the Enforcement Group to request it later.

Defensive Strategy

So, how do you reduce the risk of an audit finding in this environment? I propose action in three areas: preparation, organization, and execution.

Preparation

Make sure you take a conservative reading of each Standard. Many CIP Standards use terms that are not defined in the NERC Glossary, and that may be subject to different meanings depending on how you read the Standard.

You must understand the underlying security principles and ensure your compliance program fully implements these principles in a manner consistent with their risk to the BES. If you have any questions about how to read a Standard, you may request assistance from RF (see below).

Organization

To be successful, a compliance organization must have support at the executive level. Without the proper resources, including budget, personnel, and facilities, a robust compliance program will be very difficult to achieve. This support is a two-way street.

Communicate regularly with the executive team in language they can understand. Provide them feedback on how the allocated resources are being deployed, and what results are achieved. They should, as a result, be better informed on how to foster a strong cybersecurity and CIP compliance program.

Execution

The consequences of an error can be extreme. The Equifax breach appears to have resulted from missing one patch to a server. An unneeded open port, a missed patch, inadequate remediation of a single vulnerability, all can result in the compromise of a system.

It is your SMEs' job to ensure these errors do not occur. It is the CIP auditors' job to make sure the SMEs are doing their job.

The use of properly designed internal controls will help ensure errors do not occur, and will help with early detection of any errors that do occur. Internal control reviews are available as part of RF's outreach efforts.

Due Process

Finally, there may be rare cases where you believe that an audit team does take a reading of a Standard that is beyond what the plain language of the Standard will support. If this happens, remember you have the full range of due process offered by the Compliance Monitoring and Enforcement Program.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. All you need to do is submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Maximizing the Benefit of Baseline and Change Management

Manistique East Breakwater Light, MI - Photo: L. Folkerth

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive for continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs. There are times that I may also discuss areas of the standards that other entities may be struggling with and attempt to share ideas to help you overcome 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.

My focus in this article is on baselines. I'll discuss what baselines are, why they're useful for cybersecurity operations, and how to maximize the benefits of baselines.

What is a baseline?

There are two types of security practice known as a "baseline." The first type, as described by NIST SP800-128 in the sidebar, deals with the configuration of a system and is useful for detecting changes made by normal update processes, such as patches or version releases. The second type, as pioneered by Gene Kim and Gene Spafford at Purdue University, monitors individual files in a system for unexpected or unauthorized change and is useful for detecting malicious changes to a system. CIP-010-2 R1 requires a baseline of the type described by NIST SP800-128.

A baseline is not and should never be a static list, but a living document that will change as system changes are made. A baseline by itself is not a complete change control system; it is, rather, a significant component of a change control system.

Why do we need baselines?

Baselines are commonly used for three major purposes:

1. To document a system's configuration. A baseline provides a very detailed picture of a system's configuration. As I discuss below, this picture can include the hardware platform, the virtual environment hypervisor (if any), the operating system or controlling firmware, application software, configuration files and registry entries, ports, and many other items of detail.

2. To establish items subject to change control. Change control is necessary for high reliability systems. Information Technology (IT) practice has shown that uncontrolled changes or insufficient testing of changes contributes significantly to system downtime. A baseline should contain every configuration item that can affect the reliable operation of the device. Then those configuration items can be managed by a change control process.

3. To enable the detection of unauthorized changes. In order to detect when an unauthorized change has been made to the configuration of a system, you need to know the expected configuration of the system. Then, by comparing the expected configuration of the system to the actual configuration of the system, you will find not only that the system was changed but also what was changed.

How do we maximize the benefit of baselines?

The creation and maintenance of a baseline requires a substantial investment of time and money. It is good business sense and good security practice to maximize that investment by using the baseline for multiple purposes. In order to obtain maximum benefit from the creation and maintenance of the baseline, it must include sufficient detail about the system to be useful without becoming too burdensome. Other than the configuration items required by the Standards, you should balance the usefulness of the baseline with the effort required to maintain any configuration items that are beyond the Standard.

Change Authorization and Testing. The baseline is the basis for change authorization and testing required by CIP-010-2 R1. The Standard covers verification of security controls and, for high impact BES Cyber Systems, testing of changes to ensure that security controls are not affected. But baseline change management can be leveraged to cover functional testing to ensure that your real-time systems are not impacted by unexpected effects of a change.

Detection of Unauthorized Changes. The baseline is the basis for detection of unauthorized changes required by CIP-010-2 R2. In the event an unauthorized change is detected, CIP-010-2 also requires an investigation. I think an audit team will want to know that your investigation of an unauthorized change has answered, or attempted to answer, these questions: What is the extent of the unauthorized change? Who made the change? Was the change malicious? What steps were taken to prevent a recurrence of this or a similar issue?

Patch Management. The baseline is required to include the operating system, firmware, and application software. These items should be transferred to the patch management program of CIP-007-6 R2 (Systems Security Management). This ensures that your patch management program does not miss a piece of installed software. It

Continued on page 17

BASELINE

According to National Institute of Standards and Technology (NIST) SP800-128, "A ***Configuration Item*** *(CI) is an identifiable part of a system (e.g., hardware, software, firmware, documentation, or a combination thereof) that is a discrete target of configuration control processes. A* ***Baseline Configuratio****n is a set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes."*

In this article, I use the term "baseline" to mean a "baseline configuration" per the NIST definition.

Continued from page 16

also assists you during a compliance engagement because an audit team will expect to see this link, so it is best to be able to document that your detailed baseline is used in this manner.

Ports and Services. One of the required elements of the baseline is “Any logical network accessible ports” (CIP-010-2 R1 Part 1.1.4). Each listening network port is held open by an underlying service or other program. For example, network port TCP/443 may be held open listening for connections by a web server. Any connection to this port is directed to the web server for action and response. In my opinion, the best way to document the network ports in use is to identify the services (or other programs) that hold open listening ports, and then identify the ports or port ranges that the underlying service can listen on.

SVCHOST.EXE Considerations

Some programs are used as a “shell” to start other programs. Windows includes a program named “svchost.exe” that is used to start other services. Your baseline should include the actual service started by svchost, not just the svchost process.

If you maintain the determination of need (business need) for each service (and the service's ports) in the baseline, your compliance documentation for CIP-007-6 R1 (Ports and Services) becomes a simple extract from the baseline documentation and has the added benefit of being under change management for compliance assurance.

Incident Response Plans and Recovery Plans. An established detailed baseline is an excellent way to document what's “normal” on your systems. This information is critical for incident response teams and recovery teams. In my opinion, having this information at their fingertips will speed and enhance a team's performance in the identification, containment, eradication, and recovery phases of incident response, and in the recovery of Cyber Assets in the event of an emergency. If you don't agree with me, I suggest you run two operational exercises of a Reportable Cyber Security Incident (so you can take credit for testing your incident response plan).

Run the first exercise without giving the team access to the baseline; run the second test a few months later and provide the team with the current baseline. Measure the team's response time and effectiveness in each exercise. If you do this, I would appreciate hearing about your experience.

What configuration items should be included in the baseline?

In my opinion, a detailed baseline should include many configuration items beyond what is minimally required by CIP-010-2 R1. Here are my suggestions for configuration items to include in your baseline; those required by the Standard are marked [Required]:

Hardware. The baseline's hardware configuration items should include not just the computer model and serial number, but any devices that can be changed without changing the core computer. I would certainly include any expansion cards such as network interfaces and graphics adapters. I would also include items such as external or internal hard drives, the type and quantity of system memory installed, any normally connected devices such as printers or scanners, and any other items that are needed for operation of the device.

System Management. Also include in the hardware baseline any system management processors such as “Integrated Lights Out” (ILO) or similar devices. These devices may also need to be on your list of BES Cyber Assets or Protected Cyber Assets.

External Physical Connections. Other than power connections, you should have a record of any external connections in the hardware baseline. Ethernet, serial, fibre channel, USB, and any other external connections should be recorded.

Network Parameters. Include in your baseline any static network parameters that can affect the operation of the system. If you use static IP addresses, for example, those should be kept in the baseline for recovery purposes.

Externally Supplied Software [Required]. I am breaking the software category into two parts, for reasons you will see in the discussion of custom software, below.

Any software supplied from an external source must be included in the baseline (see Lew's Recommended List). This is true no matter how the software is provisioned or stored.

Lew’s Recommended List

This is my list of software that I recommend you keep in your inventory:

- OS
- Hypervisor (if any)
- BIOS Firmware
- Device control software (firmware)
- Applications
- Device drivers
- System management (e.g., ILO) firmware
- Internal device (e.g., network interface) firmware
- External device (e.g., printer) firmware

Custom Software [Required]. This appears to be a catch-all category to ensure that all software is included in the baseline, including software written in-house. Essentially any software, including scripts, that does not fall into the “externally supplied software” category above should be classed as “custom software.”

Ports and Services [Required].

As discussed above, the best way to document the configuration items related to network ports is to document the program or service that is holding open a listening port, and identify the port or range of ports that program or service can hold open.

Firewall Rules.

While firewall rules are not explicitly required to be included in the baseline, those rules do need to be under change control. I strongly recommend that you either keep in-scope firewall rules in the baseline for the firewall, or have a separate formal change management program for those firewall rules.

Continued on page 18

Continued from page 17

Patches and Updates [Required].

The language of the Standard actually says "security patches," but you must know the version of any software you're running. I recommend keeping a record in the baseline of all patches and updates applied, whether they are security patches or not.

Scripts

A question I am asked periodically is, "How big must a script be to be included in the CIP-010-2 baseline?" In the Guidelines and Technical Basis, CIP-010-2 says that custom software "may include scripts developed for local entity functions or other custom software developed for a specific task or function for the entity's use." However, identifying and managing all scripts on a system is a problem because any file can potentially be a script; if a file contains valid instructions for any of the many scripting languages, then that file is a script. This means that the contents of every file on every in-scope system would need to be examined and a determination made as to whether it is a script or not. This appears to me to be unworkable, so I'll propose a way of approaching the problem that I think will be acceptable to the audit teams

Let's remember that the purpose of the baseline is to enable change management and to permit the detection of unauthorized changes. With that in mind, we need to identify the scripts to be placed under change management. This will be independent of the size of a script and will depend wholly on its function. Scripts that will affect the operation of any in-scope system must be included, as well as scripts that could affect safety or reliability. For example, a one-line script that turns SCADA alarms on or off needs to be in the baseline. A thousand-line script that prints a shift schedule probably does not need to be part of the baseline.

Your approach to the identification of scripts should be covered at a high level in the applicable policy. Details of the script identification parameters, how the scripts are identified, how they are documented in the baseline, and how changes are detected should be in your process required by CIP-010-2 R1.

Anti-malware.

The type and version of your anti-malware software should already be included in the baseline as commercial software. You may also want to include in the baseline significant parameters that affect the operation of the anti-malware, such as frequency of scheduled scans and the types of data streams subject to real-time scans. Note that signature files are tracked by a separate process and should not be in the baseline.

Configuration Items Identified by CIP-007-6 R5.

CIP-007-6 R5 (System Access Control) identifies several types of configuration items that you need to track. Instead of keeping these items in a separate list, it may be beneficial to keep them in your baseline so that if any changes occur, they will be authorized and documented. These configuration items include:

- Default accounts
- Generic accounts
- Shared accounts
- Password Complexity & Aging Parameters

Privileged Accounts.

I recommend keeping a list of privileged accounts for each system in the baseline. These should change rarely, and are a significant event when they do change.

Registry Entries or Configuration Files.

In some cases, a Windows registry entry or a Unix/Linux configuration file may have a significant impact on security or reliability. You might use a process similar to the one suggested for scripts, above, to identify applicable registry entries or configuration files for inclusion in the baseline.

Is compliance risk increased by going above and beyond the Standard?

Many of my suggestions above go beyond the requirements of the Standard. RF (and, in my understanding, the ERO as a whole) refrains from punishing an entity when an entity fails in the execution of a process in an area that goes beyond the Standard. For example, if you keep a detailed hardware inventory in your baseline as recommended above and you fail to authorize the replacement of a failed hard drive, your audit team might give you a recommendation to improve your process, but would not issue a finding of possible non-compliance (PNC).

Can automated tools be used to create and maintain the baseline?

For entities with substantial numbers of in-scope systems, automated tools are probably the only way to sustain the baseline processes required by CIP-010-2. Keep in mind that no tool can do everything. All tools that I'm aware of require a significant amount of manual effort to implement, and also to maintain and operate. A solid process and effective internal controls to monitor and check the implementation are necessary even with the aid of automated tools.

For example, many tools rely on the Windows registry to determine the list of installed software. But some applications, such as Oracle, do not place a record of their installation in the registry location that is expected by the configuration management tools. As a result, you may need to manually add Oracle to the baseline, and manually track any Oracle changes that take place.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. All you need to do is submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Patch Management Mitigation Plans

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

Q I have several BES Cyber Assets that cannot be patched. Is it possible to have a patch management mitigation plan in place that does not need to be updated with every patch that is released for these systems?

A CIP-007-6 R2 (Security Patch Management) requires a new or revised patch management mitigation plan for each and every applicable security patch that is not applied within the time window specified. Note that there are two types of mitigation plans that may apply to the CIP Standards (see sidebar, "Two Types of Mitigation Plan"). In this article, I will review how mitigation plans fit into a vulnerability management program and what the expectations are for those mitigation plans. I will also discuss some methods that might be used to make a mitigation plan easier to adapt to new vulnerabilities.

Two Types of Mitigation Plan

The "mitigation plan" (not capitalized) referenced by CIP-007-6 R2 should not be confused with the term "Mitigation Plan" (capitalized) defined in the NERC Rules of Procedure. As used in this article, "mitigation plan" refers to a plan used to mitigate a vulnerability, not a Plan to correct and prevent re-occurrence of a violation.

Vulnerability Management

In a vulnerability management program, a mitigation plan fills the security gap between the identification of a vulnerability and the vulnerability’s removal from an affected system. A vulnerability is removed by modifying the software containing the vulnerability.

For more information about vulnerability management programs, see The Lighthouse in the July/August 2016 issue of the RF Newsletter.

This is usually done by applying a security patch, but may also be accomplished by upgrading to a version of software that does not contain the vulnerability or by removing the vulnerable software from the affected system. In any case, if the vulnerability cannot be removed in a timely manner it must be mitigated by a series of actions contained in a mitigation plan.

CIP-007-6 R2 addresses only those vulnerabilities that enter your vulnerability management program by way of the release of a security patch, but in my opinion you will best serve the needs of reliability by identifying all vulnerabilities that may impact your systems. Whether you implement a full vulnerability management program or stick with a basic patch management program, one of your primary sources for vulnerability identification will be security patches.

Eagle River, MI - Photo: L. Folkerth

CIP-007-6 R2 requires you to evaluate each security patch for applicability and within 35 calendar days of this evaluation apply the patch, create a new mitigation plan, or modify an existing mitigation plan.

Lifecycle of a Patch Management Mitigation Plan

A mitigation plan has several stages in its existence:

Creation – A mitigation plan is created in response to the release of a security patch that can't be applied within 35 days of the evaluation of the patch for applicability. The mitigation plan must include planned actions and a timeline.

Modification – This stage of the mitigation plan is optional. If the mitigating actions required for a newly released patch are similar to those of a previously mitigated patch, you may want to modify an existing mitigation plan rather than start a new one from scratch.

Mitigation Plan Approval – If a mitigation plan is modified, the modifications must be approved by the CIP Senior Manager or specified delegate. It would be prudent, although not required by CIP-007-6, for management to also review, assess, and approve new mitigation plans.

Continued on page 15

The Lighthouse

Continued from page 14

Execution – After a mitigation plan is created, the plan is executed to implement the mitigating actions specified by the plan.

Revision and Approval – If the mitigating actions are not completed by the dates specified in the plan's timeline, a new timeline must be developed and approved by the CIP Senior Manager or a specified delegate. Be aware that multiple extensions or a substantial extension of the timeline may be closely scrutinized by your audit team. You should carefully document the reasons for any timeline changes.

Completion – When all of the mitigation plan's mitigating actions have been performed, the mitigation plan is considered complete.

Maintenance – Once the mitigation plan is complete, ensure that any configuration items or other mitigating actions are not undone by subsequent changes. One way to accomplish this is to periodically monitor any configuration items that were changed by the mitigating actions. Changes to these configuration items need to be reviewed to verify they did not weaken the mitigations.

Termination – Vulnerabilities may be removed from applicable systems by several methods:

- patching the vulnerable software;
- upgrading the software to a version that does not have the vulnerability;
- uninstalling the vulnerable software; or
- decommissioning the Cyber Asset that contains the vulnerable software.

After all vulnerabilities covered by the mitigation plan are removed from all applicable systems, then the mitigation plan may be terminated and maintenance of the plan may cease. Remember to keep all of your documentation of the mitigation plan's implementation as audit evidence.

Expectations of a Patch Management Mitigation Plan

For the purposes of CIP-007-6 R2, I suggest a mitigation plan structure that consists of eight parts:

1. Identification of the vulnerability or vulnerabilities addressed.

   The mitigation plan should begin by listing the vulnerabilities it applies to. This can be accomplished by listing the patch that fixes the vulnerability, or by providing the National Vulnerability Database (NVD) identifier. Be aware that the NVD usually contains a Common Vulnerability Scoring System (CVSS) Severity Score that can be helpful in determining the overall risk presented by a vulnerability. This can be useful when assessing risk, as described in part 3 below.

2. Identification of the systems or types of systems affected.

   At a minimum, you should record the in-scope systems that have this vulnerability. You will want a control in place to ensure that vulnerable systems are not missed. An automated tool can assist here.

   As a part of your list of affected in-scope Cyber Assets it may be useful to keep the patch status of each system and the date patched. This ensures all information about the vulnerability is in the same place.

3. Consideration of the methods that might be used to exploit the vulnerability.

   This is where you begin developing your mitigating actions. Identify the means an attacker might use to take advantage of the vulnerability in your networks. By considering how a vulnerability could be exploited, you will also identify the risks to your systems. Documentation of these risks can be used in other phases of the mitigation plan to help in establishing prioritization, timing, resource allocation, etc.

4. Mitigating actions to prevent the exploits from occurring.

   From your analysis of the possible attack vectors in step 3, develop a list of configuration items to change and other actions you will take to protect your affected systems. Note that these protections need not be the same for each system, but may reflect different levels of risk based on the location of the system, the function of the system, and other factors.

5. Action items to implement.

   Develop action items and document how you will implement the mitigating actions. Each action item should be a discrete task that can be identified and tracked.

6. Target dates for each action item.

   Assign completion targets for each action item or task. These target dates should reflect the risk posed by the vulnerability and the possible exploits. High risk items should receive immediate attention. Lower risk items can be scheduled when resources are

Continued on page 16

Continued from page 15

available. While CIP-007-6 R2 doesn't specify a timeframe for implementation of the mitigation actions, you must be able to demonstrate to an audit team that your implementation dates are prudent. In my opinion, a good guideline to use would be to mitigate high risk vulnerabilities within a couple weeks of discovery, while it might be reasonable to allow very low risk items to go as long as three months. Whatever approach you take, be sure you document your risk-based approach to determining target dates.

7. Monitoring steps.

   You should maintain a list of configuration items that will be monitored to ensure the mitigating actions remain in effect until the vulnerability is removed from all target systems.

8. Conditions upon which the mitigation plan may be terminated.

   You should list the patches that need to be applied in order for the mitigation plan to be terminated. If a software upgrade is expected to remove the vulnerability, list the minimum version of the software that is required. Or, if it will take a complete system replacement to remove the vulnerability, that should be stated. This information will enable you to determine when the mitigation plan may be terminated (see Lifecycle above).

Note that if you employ an automated patch management system, you may be able to extract much of the required information from that system.

Improving the Coverage of an Existing Patch Management Mitigation Plan

The actions I propose above for a mitigation plan involve a substantial amount of work. If you are in the situation where you are not able to patch systems within the 35-day window, then you will need to become very efficient at developing, implementing, and monitoring mitigation plans. This may include patching delays of:

- Several weeks (e.g., the systems are in a transmission substation and you can't touch them during peak load season),
- Several months (e.g., you need a generating plant scheduled outage of several days to be able to patch), or
- Several years (e.g., a previous patch can't be applied because it interferes with the functioning of the system and subsequent patches are cumulative, so you need a "fork-lift" upgrade to fix the vulnerability).

One way of becoming more efficient might be to categorize mitigation plans by the type of vulnerability addressed. For example, your mitigation plans for Microsoft Server Message Block (SMB) vulnerabilities may contain similar actions. If you already have a mitigation plan that addresses SMB vulnerabilities, it might be easier to modify that plan rather than start a new one from scratch. It is possible you may only need to update the applicable patches and reconsider the possible attack vectors.

Keep in mind that even if you don't need to take any additional mitigating actions because the ones you have in place are effective against exploits of the new vulnerability, you still must revise the mitigation plan. The plan needs to reflect the new patches and any new vulnerabilities identified, even if the mitigating actions are the same.

Requests for Assistance

If you are an entity registered within RF 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 rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP Exceptional Circumstances

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

Q What evidence do I need to retain if I invoke CIP Exceptional Circumstances? Can I declare a CIP Exceptional Circumstance for a Requirement that does not contain that provision?

When referencing CIP-003, Security Management Controls, I will provide references to CIP-003-7, even though it is not yet enforceable.

A The provisions for CIP Exceptional Circumstances are an acknowledgement that responding to an emergency takes precedence over compliance. This makes sense when we list the top three priorities I think every electric utility should have:

1. Safety – The ability to keep people safe, whether it's our workers, customers, or someone passing by on the street, must be at the top of our priority list at all times.
2. Reliability – A reliable source of electric power is essential to our way of life. Reliability has both short-term and long-term aspects. In the CIP world, we focus on preventing widespread or long-term outages caused by malicious actors.
3. Compliance – The standards we set for our performance support the reliable operation of the electric grid. Compliance with mandatory and enforceable standards ensures we meet the standards consistently.

Reliability vs. Compliance

Compliance exists to help ensure the reliability of the BES, not as an end in itself. In recognition of this, FERC included this language in Order 706: "… allowing limited exceptions, such as during emergencies, subject to documentation and mitigation." [FERC Order 706 P 431] This was implemented in CIP Version 5 as CIP Exceptional Circumstances.

Big Bay Lighthouse, MI - Photo: L. Folkerth

What is a CIP Exceptional Circumstance?

The definition of CIP Exceptional Circumstance (see sidebar) is one very long sentence. Let's see if we can break it down so it makes a little more sense.

Figure 1 will help in our analysis of the definition. If we cut out all the modifier language, a CIP Exceptional Circumstance is a situation (orange) that involves (green) a condition (yellow). Now we start considering the modifiers. The condition may consist of any of eight listed items (blue).

One or more (yellow) of those items (blue) may occur, or a similar (yellow) condition may exist to trigger the CIP Exceptional Circumstance. Those items (blue) must also have an impact (purple) on safety or BES reliability. The conditions may exist now ([does] involve, green) or be impending (threatens to involve, green).

What isn't a CIP Exceptional Circumstance?

There are some things to note that do not fall into the definition of a CIP Exceptional Circumstance:

- A condition that impacts only compliance. For example, allowing a repair tech unescorted access into a PSP to perform routine HVAC maintenance.
- A situation that arises from lack of planning. For example, leaving insufficient time for completion of an active vulnerability assessment before

CIP Exceptional Circumstance [NERC Glossary]

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

Continued on page 15

The Lighthouse

Continued from page 14

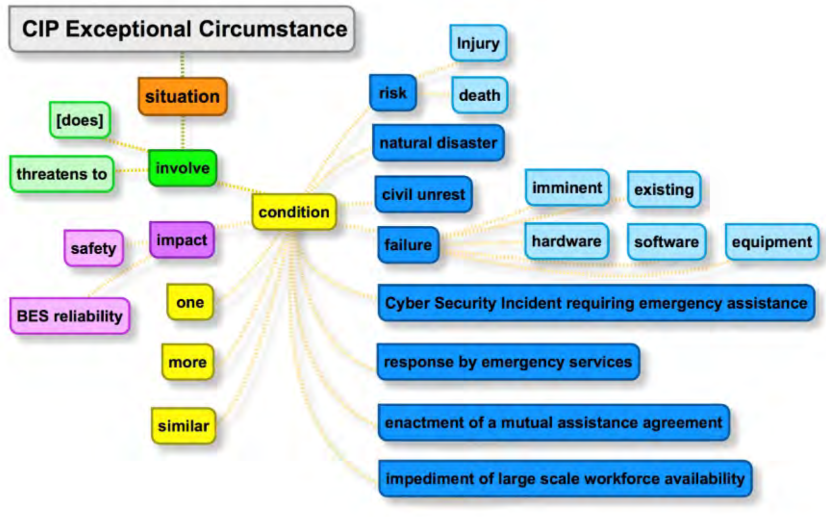

CIP Exceptional Circumstance
situation
[does]
threatens to
involve
condition
safety
impact
BES reliability
one
more
similar
Injury
risk
death
natural disaster
civil unrest
imminent
existing
failure
hardware
software
equipment
Cyber Security Incident requiring emergency assistance
response by emergency services
enactment of a mutual assistance agreement
impediment of large scale workforce availability

Figure 1 CIP Exceptional Circumstance Definition Analysis

placing a new high impact BES Cyber System into production. (CIP-010-2 R3 Part 3.3)

- A situation that arises from lack of resources. For example, security event logs are not retained for 90 days due to insufficient disk space being allocated.

Cyber Security Policy

CIP-003-7, Security Management Controls, Requirement R1 requires your cyber security policy to address declaring and responding to CIP Exceptional Circumstances. Your policy should discuss the goals, objectives, and expectations for the management of CIP Exceptional Circumstances. It should also establish a governance framework for CIP Exceptional Circumstances.

For example, the policy might discuss how your entity views the relationship between safety, reliability, and compliance. In this case the policy could establish a goal of ensuring compliance that does not impact safety or reliability in an emergency by establishing a CIP Exceptional Circumstances plan. The policy might also address how CIP Exceptional Circumstances will be governed: who can declare a CIP Exceptional Circumstance, who is responsible for the CIP Exceptional Circumstances plan, who must approve the closure of a CIP Exceptional Circumstance, and what documentation must be kept.

CIP Exceptional Circumstances Plan

In order to address the possibility of needing a CIP Exceptional Circumstances Plan I strongly recommend that you establish a plan for handling these types of exceptional circumstances. While a plan is not explicitly required by the Standard, there is far too much detail to be discussed that would fit well into a policy. This plan could well be an emergency response plan similar to a Cyber Security Incident response plan (CIP-008-5) or a recovery plan (CIP-009-6), but need to cover an emergency response from a broader perspective.

Although not required by the Standards, you may want to establish a CIP Exceptional Circumstances plan or include provisions for CIP Exceptional circumstances in a more general emergency response plan. In either event, I suggest that your plan address the topics discussed below at a minimum:

Scope

The CIP Standards explicitly permit a CIP Exceptional Circumstance to be invoked in six program areas:

1. Training before access is granted (CIP-004-6 R2 Part 2.2)
2. Access authorization (CIP-004-6 R4 Part 4.1)
   a. Cyber
   b. Physical
   c. BCSI
3. Visitor program (CIP-006-6 R2 Part 2.1, 2.2)
   a. Escorted access
   b. Visitor logging
4. Security event log retention (CIP-007-6 R4 Part 4.3)
5. Active vulnerability assessments prior to production use for high impact (CIP-010-2 R3 Part 3.3)
6. Transient Cyber Assets (CIP-003-7 R2 Att 1 Sec 5, CIP-010-2 R4)

The plan should address how each program area might be affected in an emergency. For example, if a mutual assistance crew must have access to a substation's medium impact BES Cyber Systems, you won't be able to put the crew through your cyber security training before they are given access. Your plan could provide guidance on how to grant this access, how to remove it when no longer needed, how to return to normal operations, and how to document the CIP Exceptional Circumstance.

Out-of-scope Requirements

In the case of Requirements not listed above, I recommend that your plan include provisions for foreseeable extensions into areas not explicitly permitted to be part of a CIP Exceptional Circumstance. For example, the mutual assistance crew from the above example will not have personnel risk assessments performed by your entity. You will need to grant the crew access knowing that this is not strictly permitted by the Standard.

Your plan should also address how you will handle unforeseen circumstances, whether explicitly permitted by the Standard or not.

Continued on page 16

The Lighthouse

Continued from page 15

Lifecycle

Your plan should address all aspects of a CIP Exceptional Circumstance. I suggest you include the entire lifecycle of a CIP Exceptional Circumstance as shown in Figures 2 and 3.

1. **Declaration**
   Your CIP Exceptional Circumstance plan should have a clearly defined method for declaring a CIP Exceptional Circumstance. The declaration may occur before the emergency (see Figure 2), such as in preparation for a hurricane, during the emergency, or after the emergency has ended (Figure 3).

2. **Emergency Response**
   During an emergency, you attend to the emergency. Compliance is a lower priority than an emergency.

3. **Recovery**
   After the emergency has ended, you return to normal (compliant, reliable, secure state) operations.

4. **Assessment and Mitigation**
   After returning to normal operations your work is not done. You have been in violation of the Standards, so cleanup is required. Your plan should require an assessment of possible impacts to your cyber security posture, and you should implement mitigations for any areas that may have been weakened.

   For example, if a mutual assistance crew was granted password access to Cyber Assets belonging to medium impact BES Cyber Systems in a substation, then those passwords should be reset after the emergency is over.

   Be sure you find and mitigate any area that may have gone out of compliance while you are still protected by the CIP Exceptional Circumstance. If you find additional areas of noncompliance after the CIP Exceptional Circumstance is terminated, you may need to self-report such areas.

5. **Termination**
   Once you have recovered to normal operations and mitigated any noncompliance, you should terminate the CIP Exceptional Circumstance.

6. **Documentation**
   The documentation you keep should describe the need for the CIP Exceptional Circumstance, the significant dates associated with it, all actions taken during emergency response, how you recovered to normal operations, and how you assessed and mitigated any possible noncompliance. Save this documentation as evidence.

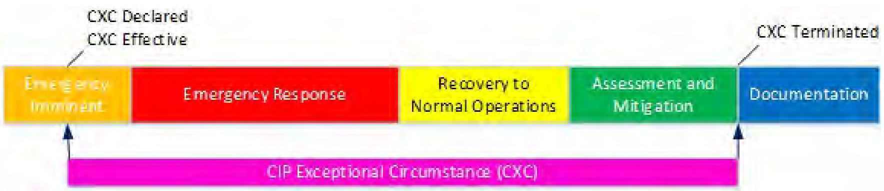

CXC Declared
CXC Effective
CXC Terminated
Emergency Imminent
Emergency Response
Recovery to Normal Operations
Assessment and Mitigation
Documentation
CIP Exceptional Circumstance (CXC)

Figure 2 CIP Exceptional Circumstance Lifecycle Example A

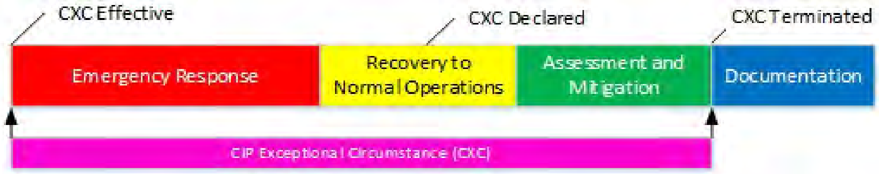

CXC Effective
CXC Declared
CXC Terminated
Emergency Response
Recovery to Normal Operations
Assessment and Mitigation
Documentation
CIP Exceptional Circumstance (CXC)

Figure 3 CIP Exceptional Circumstance Lifecycle Example B

Communications

In addition to any communications your CIP Exceptional Circumstance requires, I recommend informally communicating any declaration of CIP Exceptional Circumstances to the ReliabilityFirst Enforcement group as soon as practicable. In addition, if you have been out of compliance in any program area not explicitly permitted by the CIP Standards during a CIP Exceptional Circumstance, you should submit a self-report of that occurrence. Again, if you have communicated the circumstances surrounding the emergency and your response, RF will be in a better position to assess whether any additional actions are needed.

Requests for Assistance

If you are an entity registered within RF 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 rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Low Impact Update

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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 April 19, 2018, FERC issued Order 843 approving CIP-003-7, Security Management Controls. See the article on pages 11 and 12 of this Newsletter for details. In recognition of this action, I'll explore multiple questions related to low impact BES Cyber Systems.

Physical and Electronic Access Controls Implementation Date

Q With FERC approving CIP-003-7, do I still need to put physical and electronic access controls in place for my low impact BES Cyber Systems by September 1st of this year?

A No. Neither the physical access controls of CIP-003-6 Attachment 1 Section 2 nor the electronic access controls of CIP-003-6 Attachment 1 Section 3 will go into effect. Instead, these controls have been replaced by CIP-003-7 Attachment 1 Sections 2 and 3, with an effective date of January 1, 2020. You have an extra 16 months to put these controls in place. However, I recommend that you do not interrupt or postpone your efforts to bring your assets with low impact BES Cyber Systems into compliance. Instead, use this gift of time to put your controls in place and test them thoroughly. You can test different approaches and see what works (and what doesn't) without a compliance risk. You can also use this time to mature these controls so that they are an integral part of your operations, similar to a pre-job safety briefing.

FERC-ordered Study of Electronic Access Controls

Q Why did FERC order a study to assess the implementation of CIP-003-7?

A Without asking the Commission directly, we can't know for sure. But we can make some inferences based on the public documents available.

Mandan, MI - Photo: L. Folkerth

In its Notice of Proposed Rulemaking (NOPR) for CIP-003-7, FERC expressed concern that CIP-003-7 Attachment 1 Section 3.1 "does not appear to contain clear criteria or objective measures to determine whether the electronic access control strategy chosen by the [R]esponsible [E]ntity would be effective for a given low impact BES Cyber System to permit only necessary inbound and outbound connections" (NOPR, P. 29). In particular, I believe FERC was concerned about the phrase "as determined by the Responsible Entity" (NOPR, P. 24-26) and about a lack of objective measures to assess compliance (NOPR, P. 28-29).

Instead of ordering more stringent language in Section 3, FERC was persuaded to let industry implement the existing language (Order 843, P. 27-30). FERC also established several very clear expectations:

- Responsible Entities are expected to be able to provide a technically sound explanation as to how the electronic access controls meet the security objective.
- NERC and the Regional Entities will have the ability to assess the effectiveness of the electronic access control plan required by CIP-003-7 R2.
- NERC and the Regional Entities will have the ability to assess an entity's adherence to its electronic access control plan.

In order to verify that these expectations are being met, NERC is required to perform the study you asked about. The study will include:

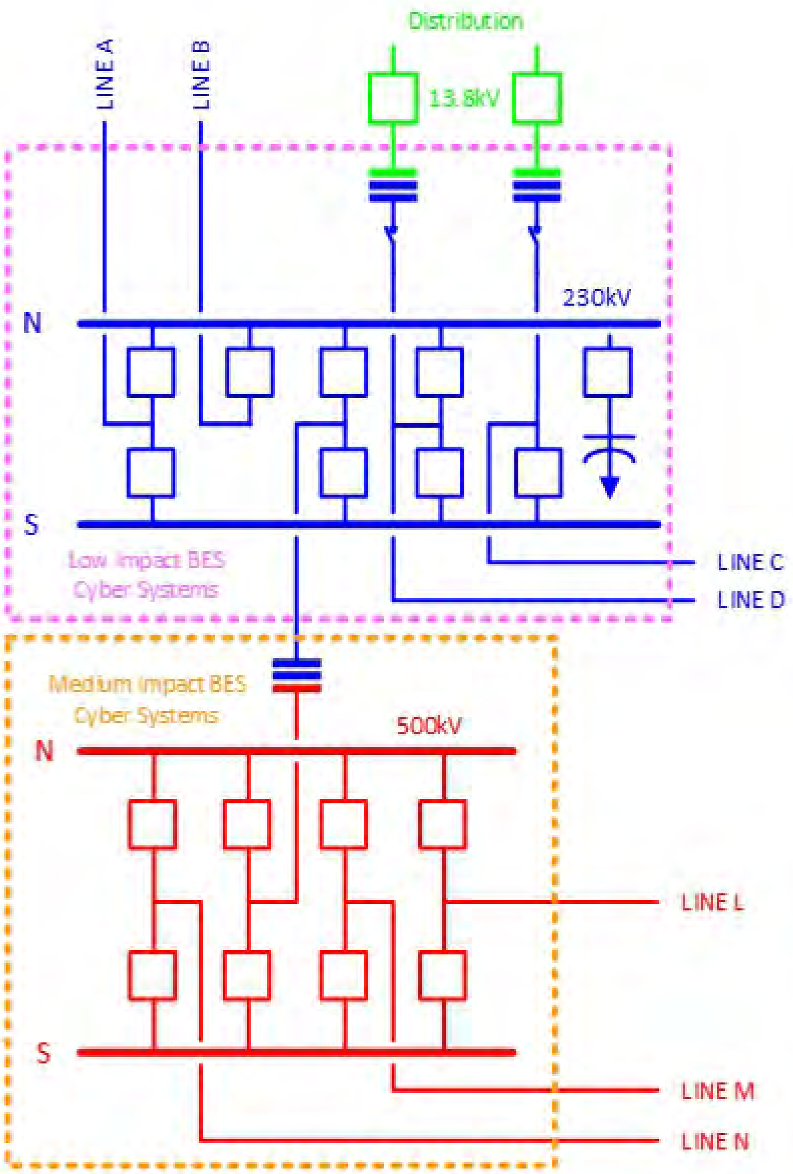
- What electronic access controls entities choose to implement;
- Under what circumstances these controls are implemented;
- The adequacy of these controls; and
- Other relevant information.

When audits of your electronic access controls for low impact BES Cyber Systems

Continued on page 15

Continued from page 14

Figure 1



begin in 2020, you should expect them to be very detailed and thorough. The audit teams will not only be reviewing your compliance with the Standard and its associated controls, they will be gathering information to provide to NERC for its study.

Impact of IRC 2.4 on Low Impact BES Cyber Systems

Q Does the presence of 500kV or above bring an entire substation up to medium impact?

A No, not by itself. According to CIP-002-5.1a Attachment 1 Impact Rating Criterion (IRC) 2.4, BES Cyber Systems associated with substation Facilities operating at 500kV or more will be assigned a medium impact rating. Note the capital "F" of Facilities calls out the Glossary definition, "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)" These Facilities will include any transformer with a high side at 500kV or more, and breakers, reactors, capacitors, etc. operating at 500kV or more.

However, BES Cyber Systems associated with the remaining Facilities within the substation will be evaluated according to IRC 2.5. IRC 2.5 contains two criteria. In order to meet IRC 2.5, a substation must connect at 200kV or higher to three other substations. If this is true, then an aggregate weighted value is calculated based on the number of lines crossing the substation boundary and the voltage level of those lines. If this aggregate weighted value exceeds 3000, then the BES Cyber Systems associated with Facilities at that substation receive a medium impact rating. Otherwise, those BES Cyber Systems receive a low impact rating per IRC 3.2.

For example, the substation in Figure 1 connects to seven other substations by 230kV and 500kV lines. Each line is protected by breakers. There is a capacitor on the 230kV side of the transformer. BES Cyber Systems associated with the 230kV/500kV transformer and the 500kV breakers will have a medium impact rating. Since the substation is connected to three or more other substations at voltages above 200kV, we need to calculate the aggregate weighted value of the substation. We do The aggregate weighted value for this substation does not exceed 3000. Therefore the BES Cyber Systems associated with the 230kV breakers and the 230kV capacitor will be assigned a low impact rating.

Line	Line Voltage	Line Weight Value
A	230kV	700
B	230kV	700
C	230kV	700
D	230kV	700
L	500kV	0
M	500kV	0
N	500kV	0
Distribution	13.8kV	Out of Scope
Aggregate Weighted Value		2800

List of Low Impact BES Cyber Systems

Q Is a list of low impact BES Cyber Systems required?

A Based on the notes attached to CIP-002-5.1a R1 and CIP-003-7 R2, the audit teams cannot require a list of low impact BES Cyber Systems at an asset. If we take a close look at CIP-003-7 Attachment 1 Section 3, however, we see

Continued on page 16

Continued from page 15

that electronic access controls are required for any routable communications that are between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber Systems. If you take the approach that any routable communications crossing the asset boundary may originate or terminate at a low impact BES Cyber System, and control electronic access accordingly, then you will not need to identify individual BES Cyber Systems, but only the assets containing low impact BES Cyber Systems.

At a generator or substation, you have the flexibility within the language of the Standard to say that not all communications are to low impact BES Cyber Systems. In order to take advantage of this flexibility you need to know which Cyber Assets are members of low impact BES Cyber Systems so that you can control electronic access to those Cyber Assets. You must be able to provide sufficient, appropriate evidence that you are protecting communications to low impact BES Cyber Systems. In order to provide this evidence you will need to know, and provide evidence regarding, which Cyber Assets are part of a low impact BES Cyber System and which are not.

One way of thinking of this is to differentiate whether you provide low impact protections at the asset (substation or generator) level or at the BES Cyber System level. If protections are at the BES Cyber System level, then you will need to be able to identify the Cyber Assets being protected. There are several places within CIP-003-7 Attachment 1 that permit compliance at the BES Cyber System level:

- Section 2, Physical security controls, permits an entity to control access to the locations of the low impact BES Cyber Systems at the asset;
- Section 3, Electronic access controls, permits an entity to control electronic access to a low impact BES Cyber System; and
- Section 5, Transient Cyber Asset and Removable Media malicious code risk mitigation, requires mitigation of the threat of the introduction of malicious code to low impact BES Cyber Systems.

In each of these cases, if you treat all Cyber Assets at an asset as low impact BES Cyber Systems, then you will not need to identify individual BES Cyber Systems to your audit team. However, if the Cyber Assets at an asset are treated differently based on whether they are members of a low impact BES Cyber System, then you will need to be able to identify those systems are that are required to be protected.

Initial Test of Incident Response Plan

Q Does the approval of CIP-003-7 alter the required date for the first test of my Cyber Security Incident response plan for low impact BES Cyber Systems?

A No, the first test of your incident response plan was due on April 1, 2017. This is not changed by CIP-003-7.

The CIP-003-5 Implementation Plan (available here) on page 2 states that the initial performance of periodic requirements in CIP-003-5 R2 is the effective date of CIP-003-5 R2, which was April 1, 2017. The CIP-003-6 Implementation Plan (available here), on page 10, incorporates the CIP-003-5 Implementation Plan by reference.

The CIP-003-7 Implementation Plan (available here) states, "The effective dates or phased-in compliance dates within the CIP-003-6 Implementation Plan, remain in effect except that the compliance dates for CIP-003-6, Requirement R2, Attachment 1, Sections 2 and 3 shall be replaced with the effective date of CIP-003-7."

This makes it clear that the compliance dates for Section 4 do not change with CIP-003-7's approval.

If you did not understand this and have yet tested your low impact Cyber Security incident response plan, I strongly recommend that you perform a test as soon as practical. You should also contact the RF Enforcement Group to discuss and work through any potential noncompliance.

I also recommend testing your plan much more frequently than the Standard requires. It is important for even low impact BES Cyber Systems to have a usable and effective Cyber Security Incident response plan, and to have a trained and proficient incident response team to carry out the plan.

Requests for Assistance

If you are an entity registered within RF 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 rfirst.org web site here.

Feedback

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

I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Cybersecurity and CIP for Small Entities

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

Q I'm at a small company and I've been tasked with creating a cybersecurity and CIP compliance program. Where do I start?

A There are a number of resources available to help you on your way. Since you are a small entity, I will assume for this article that you are in the CIP program at the low impact level, although most of my suggestions will be applicable to the high and medium impact levels as well.

I suggest you begin with a basic Information Technology (IT) program and then adapt it to your Operational Technology (OT) environment. As you build your program keep the CIP Standards in mind. I feel it will work best if you build the CIP Standards into your security program, as opposed to building a security program around the CIP Standards. In other words, a good cybersecurity program should go far beyond the minimum requirements of the CIP Standards, while maintaining compliance with all aspects of those Standards.

If you're new to cybersecurity, a good way to start is with a class on the fundamentals. If you need advice on choosing a class, send me an email at the address below.

Books

If your budget or your schedule won't accommodate a class, start with a basic book on IT security. One example of an introductory book I've found useful is "Defensive Security Handbook" (2017, O'Reilly Media Inc., ISBN 978-1-491-96038-7). This walks you through building a cybersecurity program from the ground up, although it does not deal with Industrial Control Systems (ICS).

St. Joseph, MI – Photo: L Folkerth

To build ICS capability into your cybersecurity system, a book like "Hacking Exposed – Industrial Control Systems" (2017, McGraw Hill Education, ISBN 978-1-25-958971-3) is one possible choice. In particular, the first chapter provides an excellent introduction to ICS security. RF will post a list of books and resources you may find useful in the upcoming CIP Knowledge Center on our website.

CIS "Top 20" Controls

As you are working through understanding your environment, a key facet of your cybersecurity program will be a set of security controls. You can start with a set such as the "Basic CIS Controls," available for free at

	CIS Control	CIP Standard
1	Inventory and Control of Hardware Assets	CIP-002-5.1 R1, BES Cyber System Categorization
12	Boundary Defense	CIP-003-7 R2 Att 1 Section 3, Electronic Access Controls
17	Implement a Security Awareness and Training Program	CIP-003-7 R2 Att 1 Section 1, Cyber Security Awareness
19	Incident Response and Management	CIP-003-7 R2 Att 1 Section 4, Cyber Security Incident Response

Continued on page 13

The Lighthouse

Continued from page 12

These controls, also known as the “Top 20,” may be adapted as needed to your OT environment or adopted as a whole for your entire organization. Because the “Top 20” deal with IT environments, you should also read “Implementation Guide for Industrial Control Systems,” available at here in order to adapt the Basic CIS Controls to your control systems environment.

At the low impact level, the CIS controls in Table 1 (on the previous page) have applicability to the CIP Standards.

US-CERT/ICS-CERT

While not required by the CIP Standards at the low impact level, your security program should include vulnerability management. This will enable you to address weaknesses in your security posture before these weaknesses are exploited by malicious actors. The U.S. Cyber Emergency Response Team (US-CERT) tracks and alerts on vulnerabilities in the IT environment while ICS-CERT does the same for control systems.

You can sign up for alerts here and here. ICS-CERT also has a good overview of ICS vulnerabilities here.

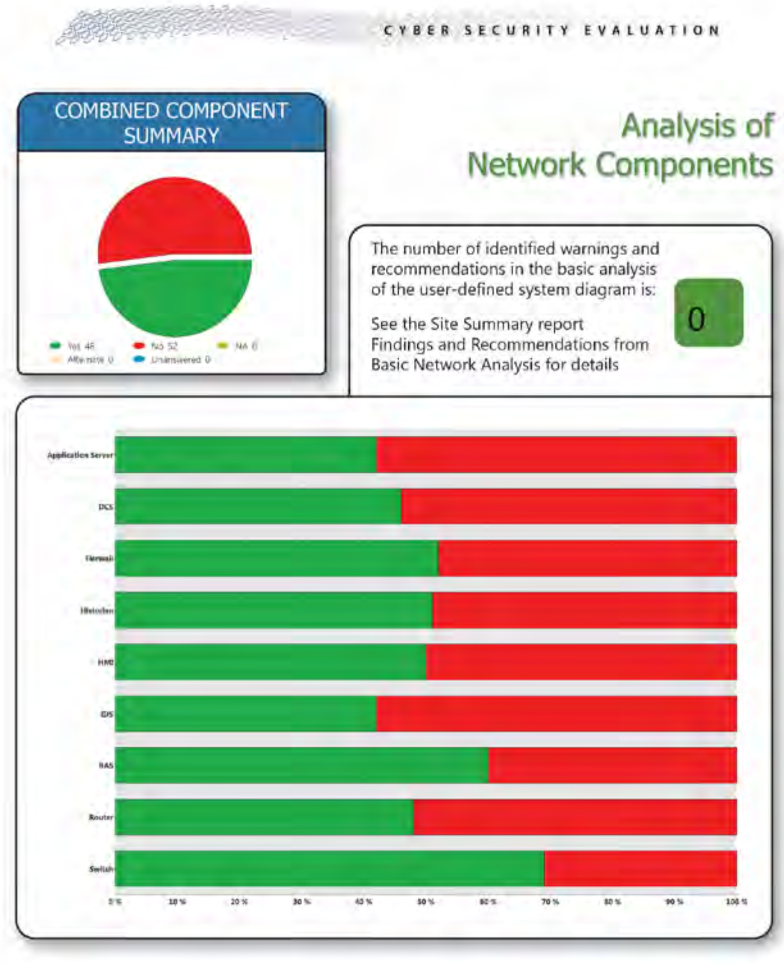
ICS-CERT goes beyond vulnerability alerts in offering free training. The available training ranges from introductory videos to instructor-led classes (also free, except that you must pay your own travel expenses), culminating in an advanced five-day hands-on class. More information on ICS-CERT training is available here.

CSET

As you get deeper into your cybersecurity program, you will want to conduct evaluations of the program. A valuable tool for our industry is the ICS Cyber Security Evaluation Tool (CSET) provided for free by the National Cybersecurity and Communications Integration Center (NCCIC), an organization within DHS. This tool helps you to perform a self-assessment of your control system security posture, and goes into detail about your control system networks and how they are protected. CSET is a Windows application that you will download and install on a local PC.

It includes a network diagramming tool so that you can easily describe your control systems network to the tool. CSET will ask you a series of questions regarding your security practices. The final result is a set of reports that will provide details about the results of the assessment (see Figure 1 for a sample page).

CSET has the ability to take the CIP Standards into account in its assessment. This capability could be used to give you a more accurate picture of your security and compliance posture. CSET does not directly support low impact at this time, but you can select standards for high and medium impact that will address the low impact requirements.



CYBER SECURITY EVALUATION

COMBINED COMPONENT SUMMARY

Analysis of Network Components

The number of identified warnings and recommendations in the basic analysis of the user-defined system diagram is: 0

See the Site Summary report Findings and Recommendations from Basic Network Analysis for details

Figure 1

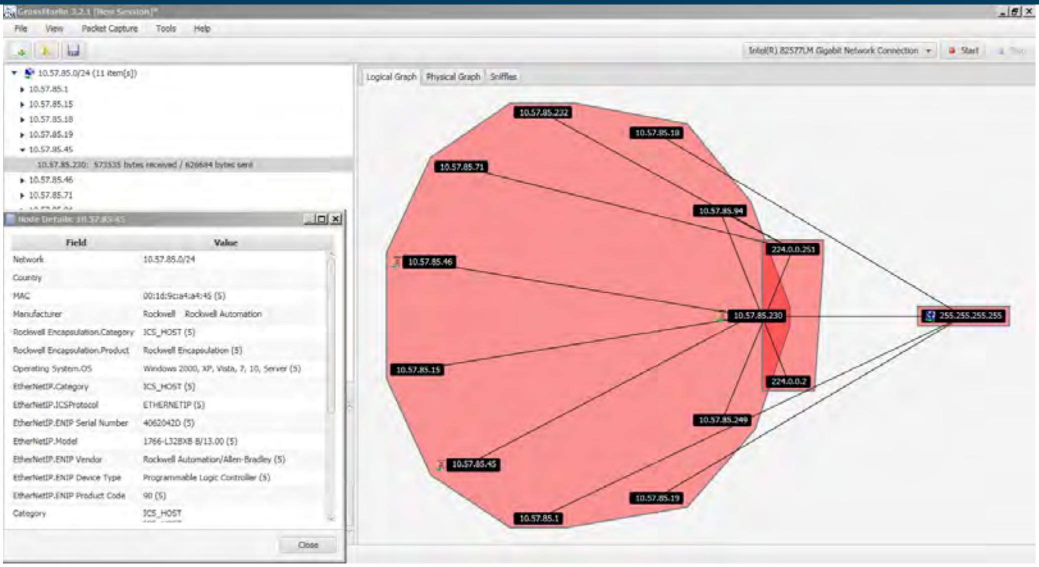
CSET Lighthouse Generation 1 Page 4

NIST CSRC

The National Institute of Standards and Technology (NIST) operates a Computer Security Resource Center (CSRC). The CSRC has many publications (read here) which are useful for our cybersecurity efforts. One of the most popular CSRC publications is Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This 462 page document contains an exhaustive set of controls for implementing IT

Continued on page 14

Continued from page 13



- 10.57.85.0/24 (11 item[s])
  - 10.57.85.1
  - 10.57.85.15
  - 10.57.85.18
  - 10.57.85.19
  - 10.57.85.45
    - 10.57.85.230: 573535 bytes received / 626684 bytes sent
  - 10.57.85.46
  - 10.57.85.71

Node Details: 10.57.85.45

Field	Value
Network	10.57.85.0/24
Country	
MAC	00:1d:9c:a4:a4:45 (5)
Manufacturer	Rockwell Rockwell Automation
Rockwell Encapsulation.Category	ICS_HOST (5)
Rockwell Encapsulation.Product	Rockwell Encapsulation (5)
Operating System.OS	Windows 2000, XP, Vista, 7, 10, Server (5)
EtherNetIP.Category	ICS_HOST (5)
EtherNetIP.ICSProtocol	ETHERNETIP (5)
EtherNetIP.ENIP Serial Number	4062042D (5)
EtherNetIP.Model	1766-L32BXB B/13.00 (5)
EtherNetIP.ENIP Vendor	Rockwell Automation/Allen-Bradley (5)
EtherNetIP.ENIP Device Type	Programmable Logic Controller (5)
EtherNetIP.ENIP Product Code	90 (5)
Category	ICS_HOST

Figure 2 - Grassmarlin

security and is used, among other things, to implement security controls in the US Government.

I recommend that you download a copy of SP800-82, *Guide to Industrial Control Systems (ICS) Security*. SP800-82 contains an excellent comparison of IT and OT security in Section 2.4. Chapter 4 discusses development of an OT security program, and Chapter 5 provides an in-depth look at designing a security architecture for OT systems.

Security Onion

Security Onion is a special-purpose version of the Linux operating system that performs monitoring and recording of network traffic using standard PCs. CIS Control 12, Boundary Defense, contains sub-control 12.5 which calls for configuration of monitoring systems to record network packets. Monitoring and recording network traffic is also an element of incident response, required by CIP-008-5 for high and medium impact BES Cyber Systems and by CIP-003-7 R2 Attachment 1 Section 4 for low impact BES Cyber Systems.

There are some very good commercial products available to do this, but those products can also be expensive. Security Onion is available for free here.

GRASSMARLIN

GRASSMARLIN is another free tool used for network monitoring, but GRASSMARLIN differs from Security Onion in that it is designed to passively monitor ICS networks and identify ICS systems and traffic patterns on those networks. Passive monitoring is important in ICS environments due to the sensitivity of some ICS systems to any change in the network environment. GRASSMARLIN can be used to monitor for unexpected or unwanted patterns of traffic, and can also be used as a discovery tool for ICS devices.

This can be useful in CIP-002 to ensure you have inventoried all of the systems that can have a 15-minute impact on the BES. GRASSMARLIN can identify ICS devices by network traffic analysis.

Figure 2 shows the result of a GRASSMARLIN monitoring session on a small test network. Note the control system icon next to three of the devices on the network. This denotes a device that is communicating with one or more ICS protocols, making it a subject of interest in the identification and protection of control systems.

GRASSMARLIN was developed by the NSA and is available for free here. This web page also has links to the User Guide and to a brief slide deck on the capabilities of GRASSMARLIN.

Security Testing Environment

You should not implement any of these tools directly into your control system environment. First, you should first familiarize yourself with the operation of each tool. You should understand the possible impact of each tool on your production environment.

If you don’t already have one, I strongly suggest that you set up a security testing environment to try out and evaluate any tool you plan to incorporate into your security program.

It is possible to set up your own security testing environment without expending a lot of resources. A couple of ICS devices and a small PC can provide a lot of benefit if your company can’t afford a full test environment. Figure 3 (on the next page) shows my personal testing environment as it was used to test GRASSMARLIN.   The used PLCs were obtained from eBay, the Ethernet hub from a garage sale, and other components from commercial sources. The wood backboard and legs (actually shelf brackets) were obtained

Continued on page 15

The Lighthouse

Continued from page 14

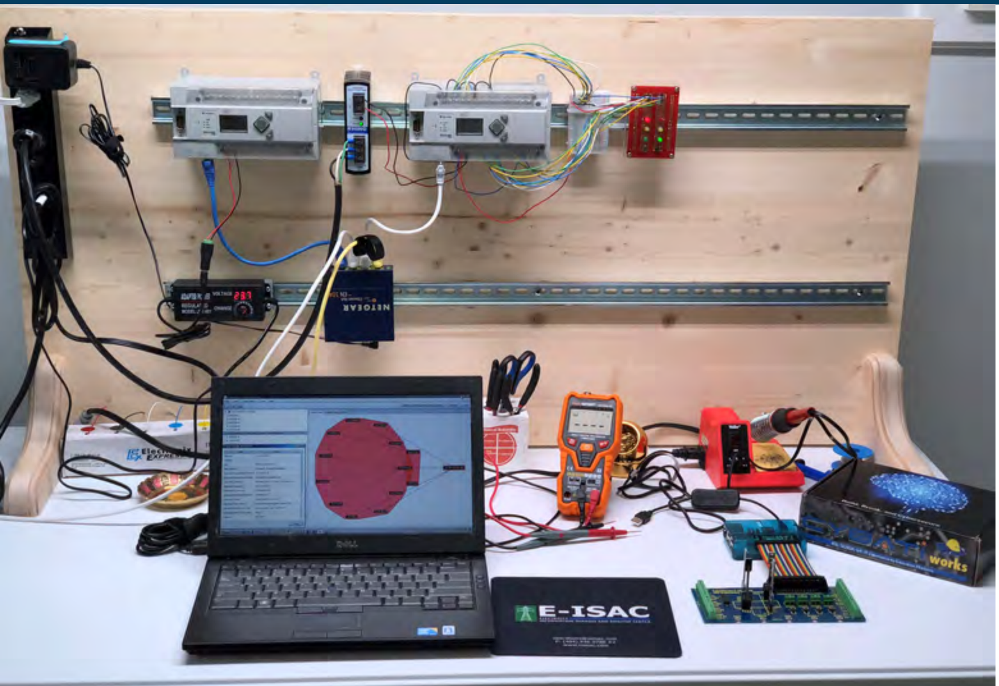


Figure 3 - A Simple Test Environment

from my local Lowe's. Except for the PC, which is an older repurposed laptop, the entire setup cost less than $500.

RF Knowledge Center – CIP

There are many resources available in addition to those I describe above. In recognition of this, RF is establishing a CIP area within the Knowledge Center on the RF website. We will update the CIP Knowledge Center with resources and links to resources for CIP compliance and ICS cybersecurity that we believe may help our entities. An expanded version of this article will be posted there as well.

Requests for Assistance

If you are an entity registered within RF 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 rfirst.org web site here.

Newsletter Correction

In our previous issue, an error was discovered in the Lighthouse article regarding the initial implementation date for low impact Cyber Security Incident response plans.

We promptly identified and corrected the pdf, but if you downloaded the original version of the May/June newsletter, please be aware of the correction to avoid any confusion.

Feedback

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

I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

"Achieve the Objective…"

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

Q: How do I show an audit team that I have "achieved the objective" of a CIP Requirement?

A: Objective-based Standards

The ERO Enterprise (NERC and the Regions) has been trending toward objective-based Reliability Standards for many years. This trend appears to be gaining momentum, especially with the CIP Standards.

Some Requirements, such as CIP-010-3 R4, Transient Cyber Assets and Removable Media, explicitly use the phrase "achieve the objective" within the language of the Requirement. FERC stated recently, "We expect responsible entities to be able to provide a technically sound explanation as to how their electronic access controls meet the security objective." [Order 843 at P28, referring to electronic access controls for low impact BES Cyber Systems]

I recommend that you treat all of the CIP Standards as objective-based, and that you write your policies, plans, processes, and procedures from this perspective.

The shift toward objective-based Standards is good for security and also makes good business sense. Why spend money on compliance and security programs that do not result in a robust security posture? Why not maximize the benefit of compliance expenses by implementing good security practices that achieve the intended objective, and use compliance as the governing layer to ensure those security practices are followed rigorously? Compliance should be a by-product of a robust security program, not an end in itself.

As an example, an entity implemented a network backup system for its primary Control Center. The backup system uses a network-attached storage system, which stores the backed-up files for the entire Control Center. This arrangement meets the language of CIP-009-6, Recovery Plans for BES Cyber Systems, by providing for the backup and storage of information required for recovery. However, online storage is subject to the threat posed by ransomware, which encrypts a victim's data and demands a ransom to provide decryption. If the Control Center's systems fall victim to this threat, the online backups that might be used to recover those systems could be encrypted as well. This would leave no way to recover the Control Center's systems without rebuilding those systems from scratch, a lengthy process which may result in a very different operating environment for the entity. If the entity had reviewed this approach against the objective of CIP-009-6, which might be stated as: "Be able to recover Control Center operability from any foreseeable event within a reasonable time," the entity would probably have seen the need for offline backups on its own.

Sand Hills Lighthouse, Ahmeek, MI – Photo: L Folkerth

Security Plan

In order to be able to demonstrate meeting objectives, your organization needs to have a documented plan in place. That plan needs to address all objective-based Requirements, but I recommend that you write your plan to address the objectives of all the Requirements that are applicable to you.

If you're subject to the CIP Standards, you already have a security plan that consists of a set of security processes tied together by a security policy. Let's build on this foundation to create a comprehensive security plan for your CIP assets.

Overall Security Objective

Your organization's security plan should include an objective for the plan as a whole. This overall objective will be the target all Requirement-based objectives

Continued on page 13

Continued from page 12

should support. For example, the overall objective for a Generator Operator might say, “Maintain the safety, operability, and integrity of ABC Generating Plant by rigorously implementing security practices that address the risk of compromise by a malicious actor or by inadvertent action.”

I’ll take this objective apart and explain what it means to me. I suggest that you perform this exercise for each of your objectives and keep the analysis in your documentation.

- “Maintain” implies a continuing process. Security is not something that you perform once and you’re done. Security is an ongoing set of actions that adapt to changing conditions.
- “Safety” is always the first priority. I included safety here because safety instrumented systems have been successfully compromised by malicious actors.
- “Operability” of an asset is the ability to have control over the operation of that asset. If you lose operability, the consequences could be extreme. For example, a set of relays at multiple substations could be operated in a way to cause extended overload of a transformer or transmission line, perhaps resulting in destruction of that equipment.
- “Integrity” is the health of the asset as a whole. If integrity is compromised, the asset could be damaged, you may lose the benefit of the asset for an extended time, and you may incur substantial costs to repair the asset.
- “Rigorously implementing” means that security that is partially implemented, or implemented on an irregular schedule, may not be effective in preventing the asset from being compromised. For example, the Equifax breach was reportedly possible because one security patch was not applied to a server in a timely manner.
- “Security practices” are the actions specified in this security plan.
- “Address the risk” means to look at or pay attention to risk. It is impossible to eliminate all risk, so we prioritize where we spend our resources based on our evaluation of the risk involved.
- “Compromise” can be any condition that affects the function of the asset. This could involve denial of service, installation of malicious code, damage or destruction of physical equipment, and so on.
- “Malicious actor” can be an employee, contractor, vendor, activist, criminal, nation-state, and many others. Your security plan should evaluate the risk of each type of actor and implement protections based on the assessed risks.
- “Inadvertent action” means any action taken that has unintended adverse consequences. For example, NERC Lesson Learned LL20181001 (available here) discusses the loss of a SCADA system for several hours after a seemingly simple patch cable change.

This is a simplified example. You should adopt the overall security objective that works best for your organization.

Requirement-based Security Objectives

In order to achieve the overall security objective, specialized security objectives should be created to address particular areas of security. You can combine multiple CIP Requirements into a program group, such as ports and services, with a common objective. Or you can address the CIP Requirements individually.

For the discussion below, I’ll assume we’re looking at the Requirements individually. Make sure your security plan can answer the following questions for each Requirement:

1. **What is the security objective of this Requirement?** Try to state the security objective, as you believe it applies to you, clearly and succinctly. For example, I might state the security objective of CIP-002-5.1 R1, BES Cyber System Categorization, as, “Identify and categorize each device that could be susceptible to cyber compromise and that could have a reliability impact before manual intervention can override the compromised device.”
2. **How will the security objective be met?** Your security plan must clearly show the steps you take to meet the security objective. You get to determine how you will achieve the objective, subject to review and assessment from an audit team. These steps will be what your performance is measured against, rather than a prescriptive requirement. For example, if your security plan calls for you to use application whitelisting to prevent malicious code, your audit will assess your effectiveness in the implementation of this approach.
3. **How will the security plan adapt to changing threats?** The threat environment changes far more quickly than Standards can be modified. Unless the standards development process changes, the CIP Standards will always lag far behind emerging threats. Therefore, it is important that your security plan is designed to recognize and deal

Continued on page 14

Continued from page 13

Internal Controls

If you want to learn more about internal controls, there are many sources of information. *Standards for Internal Control in the Federal Government* (the GAO "Green Book") is available here.

NERC's *ERO Enterprise Guide for Internal Controls* is available here.

If you are interested in a discussion of internal controls with RF staff, please request an Assist Visit. Details are at the end of this article.

with evolving threats. For example, your security plan might establish a threat analysis team that meets periodically to analyze changes to the threat environment and to plan responses to emerging or changing threats. In the CIP-009-6 R1 example I presented earlier, the entity designed the online backup scheme before the threat of ransomware became significant. A threat analysis team could have identified that threat as it became known and responded by ensuring an offline backup system was implemented to supplement the online backups.

4. **How will you measure performance of the plan?**
 Your security plan should include measures to provide reasonable assurance that the objectives of the plan will be achieved. This is one of the functions of internal controls. Your internal controls should be designed to identify potential problems before they become actual security or compliance issues. [See sidebar]

5. **How will you correct any shortcomings in the plan?**
 Especially in cyber security, plans can age and need updating. You should review your security plan and your performance measures periodically to ensure the plan is not beginning to weaken in any area. You will need to determine what the frequency of this review should be. This will depend on many factors, such as the emergence of new threats, changes in existing threats, the position of your entity within the BES, etc.

6. **Does the plan meet compliance requirements?**
 Whenever the plan changes, make sure you are still meeting the letter of each Requirement, in addition to your security objective. For example, an entity implemented application whitelisting to achieve the objective of preventing the introduction of unauthorized code into its systems. Since the entity achieved its objective in this way, the entity wanted to know if it could perform patch management on a quarterly cycle, rather than monthly. The audit teams have great flexibility, but the language of CIP-007-6 R2 is clear. The entity was advised to retain the monthly patch cycle until audit practices become sufficiently flexible to be able to permit alternate ways of achieving compliance.

7. **Will the plan produce sufficient, appropriate evidence of compliance?**
 For the prescriptive CIP Requirements, such as CIP-007-6 R2, Patch Management, make sure your security plan produces good quality evidence of compliance. As a guide to what evidence will be requested during an audit, Version 2 of the Evidence Request Tool is now available on the NERC web site. For objective-based CIP Requirements, such as CIP-007-6 R3, Malicious Code Prevention, produce documentation of the above six steps, with emphasis on steps 2 and 4. You can look at step 2 as providing the (self-imposed) prescriptive requirements that the objective-based Requirement lacks. Step 4 provides evidence that you are rigorously following the requirements you specified in step 2. Refer to the Evidence Request Tool for examples of the type of evidence needed to satisfy a prescriptive Requirement, and adapt these examples for your own use.

If you would like help in setting up a risk-based compliance program that addresses objective-based Standards and Requirements, or if you just want a different set of eyes to look at your work, you may request an Assist Visit via the web link below.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

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

I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Supply Chain Risk Management

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

Q: CIP-013-1 will become effective on July 1, 2020. How do I prepare for this date and what will audits of this Standard look like?

A : Preparing for CIP-013-1

CIP-013-1 is the first CIP Standard that requires you to manage risk. Entities and audit teams will both need to make adjustments to prepare for this standard's effective date. I'll give you my present views on this subject as a starting point, and I will provide updates in 2019 and 2020 as the effective date nears and audit approaches are developed.

CIP-013-1 is a *plan-based* Standard.

You are required to develop (R1), implement (R2), and maintain (R3) a plan to manage supply chain cyber security risk. You should already be familiar with the needs of plan-based Standards, as many of the existing CIP Standards are also plan-based.

CIP-013-1 is an *objective-based* Standard.

CIP-013-1, and its affiliated Standards (CIP-005-6 R2 Parts 2.4 and 2.5; and CIP-010-3 R1 Part 1.6), are intended to address four security objectives (see FERC Order 850 at P2, excerpt below):

"[R]equire each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. [T]he Reliability Standards focus on the following four security objectives:

Portage Upper Entry, MI - Photo by Lew Folkerth

1. software integrity and authenticity;
2. vendor remote access protections;
3. information system planning; and
4. vendor risk management and procurement controls."

Your actions in developing and implementing your plan should be directed toward achieving these four objectives. You should be prepared to demonstrate to an audit team that you meet each of these objectives. These objectives are not explicitly referenced in the Standard language. However, as outlined in the FERC Order, the achievement of these objectives is the reason the Standard was written.

This does not apply just to CIP-013-1. You should write every CIP-related process to achieve the security objective of the Standard, especially when the security objective is stated as clearly as it is for CIP-013-1. Keep in mind that your audit teams are required to consider your program's objectives (see GAGAS 2018 Section 8.36e) when they perform your audit. You will be on much firmer ground during your audit if you can show that your processes achieve the intended objective.

CIP-013-1 is a *risk-based* Standard.

You are required to "develop one or more documented supply chain cyber

Continued on page 11

Continued from page 10

security risk management plan(s)" and to "identify and assess cyber security risk(s)." Your plan should clearly show how you identify and address the risks in your supply chain. As CIP-013-1 is the first explicitly risk-based CIP Standard, this is new ground we'll be exploring.

You are not expected to address all areas of supply chain cyber security. You have the freedom, and the responsibility, to address those areas that pose the greatest risk to your organization and to your high and medium impact BES Cyber Systems.

You will need to be able to show an audit team that you have identified possible supply chain risks to your high and medium impact BES Cyber Systems, assessed those risks, and put processes and controls in place to address those risks that pose the highest risk to the BES. There are several sources to get you started. Approved Implementation Guidance is available on the NERC web site. Also, several National Institute of Standards and Technology (NIST) publications may be useful (see sidebar).

References

- NIST SP800-161, Supply Chain Risk Management Practices
- NIST SP800-30, Guide for Conducting Risk Assessments
- NIST SP800-39, Managing Information Security Risk
- ERO Enterprise-Endorsed Implementation Guidance

One example is NIST SP800-30. This guide discusses a risk management process. It proposes using four components for risk management: *frame* risk (establish a risk context), *assess* risk within the context of the organizational risk frame, *respond* to risk based on the assessment, and *monitor* risk over time. I expect developing a plan by implementing this document and approach would work well for CIP-013-1.

Preparing for an Audit of CIP-013-1

Fundamentally, an audit of CIP-013-1 will probably be similar to audits of other plan-based Standards, but with additional steps.

You will need to have evidence of your documented plan (or multiple plans if you've chosen that option) throughout the audit period.

Be prepared to show how your plan meets the four security objectives. You may accomplish this with a narrative internal to the plan, or by an external compliance narrative in the RSAW.

Be prepared to show how your plan manages risk. Again, a narrative will probably be needed. If you elect to use the NIST SP800-30 risk assessment process, providing detail of how you have implemented the four steps of the risk assessment might be part of this.

You will need evidence of your implementation of the plan. Do not rely on vendor contracts or contract language as evidence. Audit teams will be interested in the tangible results of what you have accomplished and how you've accomplished it, not what you've put in your contract language.

Finally, you will need evidence of your annual (15 calendar months) review of your supply chain cyber security risk management plan. This review should include the identification of any new or emerging risks since the last update of the plan. You should refresh the risk assessments in light of any new risks or changing circumstances in previously-identified risks. You should also review the steps taken to mitigate all identified risks.

Make sure your CIP Senior Manager (or delegate) approves each revision of the supply chain cyber security risk management plan.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

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

I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

A Structure for CIP Risk Management Plans

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

As I discussed in the November/December 2018 issue, CIP-013-1 will become effective and enforceable on July 1, 2020. On that date CIP-013-1 will become the first explicitly risk-based CIP Standard. I do not believe it will be the last such Standard. The Project 2016-02 Standard Drafting Team has posted a set of “CIP Virtualization Updates” that are mostly risk-based as well.

Whether a Standard says “[D]evelop one or more documented supply chain cyber security risk management plan(s)” (CIP-013-1) or “[I]mplement one or more documented processes to mitigate the risk posed by unauthorized communications to and from applicable systems...” (CIP-005-7 Draft 1), you will need to have a risk management plan or process in order to fulfill the requirements of the Standard. In this column I’ll explore what I think the structure of such a plan might look like.

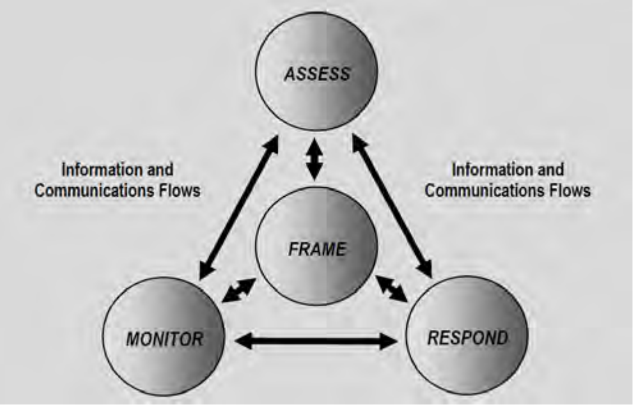

ASSESS
FRAME
MONITOR
RESPOND
Information and Communications Flows
Information and Communications Flows

Figure 1: Risk Assessment within the Risk Management Process
Source: SP800-30

Munising Range Lights, Munising, MI - Photo by Lew Folkerth

The structure that follows (see Figure 1) is based on NIST SP800-30, the Guide for Conducting Risk Assessments (found here). I also recommend reading NIST SP800-39, Managing Information Security Risk (found here).

FRAME

Your risk management plan for a CIP Standard should provide a frame for your approach to risk management. The frame provides the context for your risk-based decisions. The frame should contain the following elements:

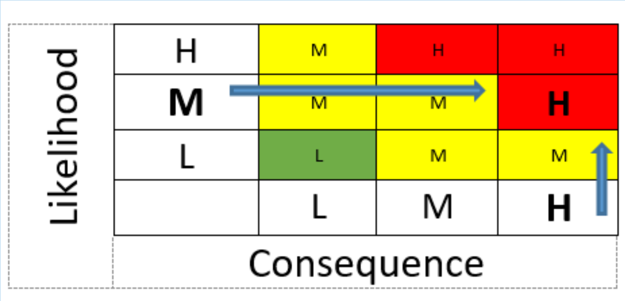
Scope:

You should carefully identify the scope for your plan. If the scope is too narrow, you risk violating the Standard by not considering all of the required risk areas. If your scope is too broad, you will expend resources and funds that may provide little benefit. You may want your scope to include an inventory of Cyber Assets that are covered by your plan, as well as a list of vendors that may be affected by implementation of the plan (such as for CIP-013-1).

Continued on page 11

Continued from page 10

Simplified Risk Assessment Methodology



Likelihood			
H	M	H	H
M	M	M	H
L	L	M	M
	L	M	H
	Consequence		

In this methodology, you qualitatively estimate the likelihood of a risk being manifested and the possible consequence if it does occur. For example, you might assess the likelihood of purchasing counterfeit equipment as medium, and the consequence of implementing such equipment as high. In the methodology above, this would assess as a high risk.

Objectives:

The objectives of the risk management plan should be clearly identified. For example, your CIP-013-1 risk management plan should include the four objectives from FERC Order 850 P2, as well as any additional objectives that are appropriate for supply chain risk management at your organization.

Risk Assessment Methodologies:

The methods you use to assess risk should be spelled out in this section. Each methodology (you can use more than one) will lay out the steps you will need to take to assess the risks you identify. These steps should take into account the inputs to the process (e.g., threat sources, threat events, vulnerabilities, predisposing conditions, etc.). Simpler may be better here (see sidebar), but you will need to select the methodologies that you determine are best suited to your organization. If you create a complex methodology to assess your risks, then you will need to be able to explain that methodology to an audit team.

Definitions:

Any terms used in risk management that may be ambiguous and that are not defined in the Standard should be defined here. Try to keep to generally accepted definitions – unusual definitions will probably be questioned.

ASSESS

Your risk management plan should include a process for assessing risks within the scope of the plan. Volumes have been written about this topic, so I will sketch out a possible outline for a CIP-related assessment.

Identify possible risks:

I think the best approach to identifying possible risks is to cast a wide net and then narrow down the results. Some possible sources of threats include:

- US-CERT
- NCCIC (formerly ICS-CERT)
- E-ISAC
- Vendors

Apply the scope for this process:

Screen for only those risks that are in-scope for this process. For example, one of the risks you identify might be the risk of opening an email attachment and thereby compromising a BES Cyber System.

This technique was used in the 2015 Ukraine attacks and so should be on your list of possible risks. However, this is not a risk that pertains to supply chain cyber security, so it is out of scope for your CIP-013-1 risk assessment. Instead, that risk should be handled by a different risk assessment process.

Apply the appropriate risk assessment methodology:

Once you apply your risk assessment methodology, you should obtain a risk score or risk rating for each identified risk.

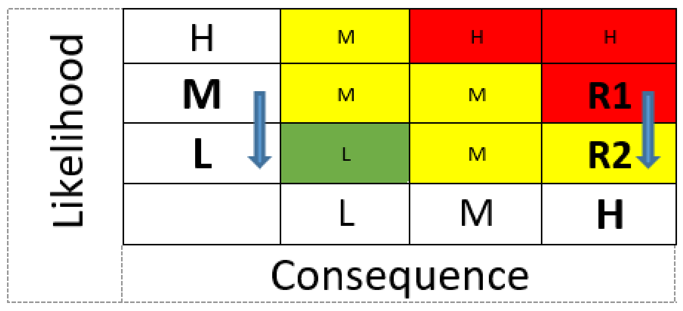
Prioritize the resulting risks:

You can't address all risks, so you will need to prioritize the risks you will address. The risk assessment methodology will result in a raw risk score, which you will need to temper with professional judgment. Analyze the risks with the highest ratings and determine how you could reduce each risk. This will help you determine the order in which you address the risks.

Continued on page 12

Continued from page 11

Reducing Risk



Likelihood

H	M	H	H
M	M	M	R1
L	L	M	R2
	L	M	H

Consequence

Based on the previous example, you might choose to reduce the likelihood of purchasing counterfeit equipment by purchasing only from the vendor or from an authorized distributor.

This changes the likelihood of the risk being realized from medium to low and also changes the original high risk (R1) to a medium risk (R2).

Evidence of this risk reduction might include your revised purchasing process that shows the acceptable equipment sources, and purchase orders showing that the process has been implemented.

RESPOND

After you have identified, assessed, and prioritized the identified risks, you will need to decide how to respond to those risks. Those responses should consider the need to produce evidence of compliance. You should also show how the actions you take reduce risk. (See the sidebar, Reducing Risk)

MONITOR

Your risk management plan should include a provision to monitor risk over time. This monitoring should:

- include an ongoing determination of the effectiveness of your risk mitigations,
- identify emerging risks and risks that were not included in the most recent assessment, and,
- ensure that sufficient compliance evidence is being produced and retained.

Disclaimer

If you choose to adopt this framework, you will need to modify it to suit your entity and your circumstances. This framework is intended only to demonstrate one possible approach to address the risk and achieve compliance.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

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

I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 1 of 2)

Big Sable Point, MI - Photo by Lew Folkerth

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

In my November/December 2018 article, I discussed CIP-013-1 at a high level. I discussed how I think CIP-013-1 is at the same time plan-based, objective-based, and risk-based. In my January/February 2019 article I provided a suggested structure for a risk management plan. In this article I'll dive into supply chain risk management Requirements for CIP-013-1 in more detail. I'll cover CIP-005-6 and CIP-010-3 in the next issue. Please remember that what follows are my opinions and my suggestions.

If you choose to adopt any of these suggestions, you must adapt them to your entity's position in the Bulk Electric System, and to your entity's systems and policies.

In the discussion that follows, I will quote only short phrases from the Standards. Please follow along in the actual Standards, available on the NERC web site here. In most cases I will paraphrase the Standards as I understand them. As always, the language of the Standard will govern in any compliance monitoring engagement.

CIP-013-1 Overview

CIP-013-1 is a forward-looking Standard that requires you to modify the way you work with your vendors in any future system, software, or service acquisition. You will have fulfilled the security objectives of CIP-013-1:

- if you integrate vendor and product security considerations into your vendor selection process,
- if your future acquisition contracts work to mitigate the cyber security risks posed by your selected vendor, and
- if you manage the relationship with each of your vendors, present and future, to mitigate risks you identify as applicable to the vendor.

CIP-013-1 applies to your high and medium impact BES Cyber Systems only. I recommend that you also include EACMS associated with high and medium impact BES Cyber Systems, as CIP-013-2 is expected to include these systems in its scope.

CIP-013-1 R1

You are required to develop and document at least one risk management plan. This plan must address the cyber security of your supply chain by implementing processes used in planning for procurement and in procuring systems. I discussed a possible structure for such a risk management plan in my January/February 2019 column. You may choose to create more than one plan for this purpose – for example, you might want to have separate plans for your control centers, transmission substations, and generating plants. Each plan must include the three types of processes specified by Parts 1.1 and 1.2, as discussed below.

Since these processes are part of a risk management plan, you will need to identify the risks applicable to your acquisition, assess those risks, select the risks you will address, and implement, in your purchasing process, remediation for those selected risks. The Standard is silent on exactly which risks you must address, which means you will need to develop this list on your own.

I recommend that your risk management plan include an assessment of the risks listed below, "Cyber Security Supply Chain Risk Consideration: A Starting Point." I intend this list to be used to spark your thinking and for you to build on as you identify additional risks. You should add risk identifications of your own to this list.

Continued on page 9

Continued from page 8

Addressing your identified risks will probably include some additions to the terms of any contract you use for acquiring BES Cyber Systems and systems or services related to BES Cyber Systems.

Two possible sources for acquisition contract language are:

- "Cyber Security Procurement Language for Control Systems," available here; and
- "Cybersecurity Procurement Language for Energy Delivery Systems," available here

The procurement language can be used as a source for possible risks, and for language to address selected risks in contracts. You will need to supplement your selected items with language to address threats that have emerged since these documents were published. For example, you may wish to ensure your vendor complies with US CERT's "SMB Security Best Practices" (here) in order to reduce the risk of ransomware within your ESPs.

Be careful when determining the scope of the risks you are considering. You can easily be distracted by valid risks that are outside the scope of CIP-013-1. CIP-013-1 only requires you to consider risks that can be addressed in planning and procuring systems and services related to BES Cyber Systems. Examples of risks that are outside the scope of CIP-013-1 might include an employee plugging in an unauthorized flash drive, or the risk of a poorly configured relay causing damage to BES components. These are both valid risks, and you should consider them elsewhere in your risk management plans, but they are not related to your supply chain and therefore are not in scope for CIP-013-1.

The processes specified by Parts 1.1 and 1.2 deal with vendor interaction, either in planning for procurement or in the actual procurement of systems. The term "vendor" is unofficially defined (see sidebar) in CIP-013-1. I say unofficially because the definition is not included in the NERC Glossary and is not part of the enforceable language approved by a regulatory authority. While I don't anticipate issues with the supplied definition, I recommend caution in relying on it.

Part 1.1 – Planning for Procuring and Installing

Your supply chain cyber security risk management plan must include a process that will be "used in planning for the procurement" of high and medium impact BES Cyber Systems. The process must address the identification and assessment of cyber security risks to the BES from vendor products or services. The cyber security risks addressed by this process would result from procuring and installing vendor equipment and software, or using services provided by the vendor. In other words, you must have a process that specifies how you will plan future acquisitions of products or services that will become, or will affect, BES Cyber Systems.

Part 1.1 – Planning for Transitions

In addition to the risks resulting from procuring and installing vendor equipment and software, Part 1.1 also requires your supply chain cyber security risk management plan to include a process that addresses cyber security risks resulting from transitions from one vendor to another. In other words, you must have a process that specifies how you will plan your future acquisitions of products or services such that the risks resulting from a vendor transition are minimized.

Part 1.2 – Procuring BES Cyber Systems

Your supply chain cyber security risk management plan must also include a process for procurement of BES Cyber Systems. Note that Part 1.1 requires processes to be used in *planning* for procurement and transitions; Part 1.2 requires a process to be used in actually procuring systems. These will probably be different but related processes.

Part 1.2 contains six sub-parts that specify items you must address in the procurement process. You should also include the additional procurement considerations identified by your Part 1.1 risk assessment.

In this article, I listed the required processes as separate processes, but there is no reason you can't combine processes to suit your needs. Just be sure you can clearly show an audit team that you address all required process types in your supply chain cyber security risk management plan.

CIP-013-1 R2

Any purchase arrangement or contract you enter into on or after the CIP-013-1 effective date of July 1, 2020, must be developed in accordance with your approved supply chain cyber security risk management plan.

For Requirement R2 you must implement all the supply chain cyber security risk management plans developed under R1. Any shortcoming in implementing your processes, and what they say you will do, could be considered a violation. This is different from a prescriptive Standard. For example,

Definition of *vendor*

"The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."

--- CIP-013-1 Guidelines and Technical Basis

Continued on page 10

Continued from page 9

if your personnel risk assessment process created by CIP-004-6 Requirement R3 says that you will perform personnel risk assessments every five years, but you miss that target by a year for some personnel, then that should not be a violation as you are still within the timeframe prescribed by the Standard. CIP-013-1 is different in that it is a non-prescriptive, risk-based Standard. You set the compliance rules in R1 by creating the plan and processes you will follow. You are then expected to follow through by implementing these self-generated requirements in R2.

Both contract language and vendor performance to a contract are explicitly taken out of scope for these Requirements by the Note to Requirement R2. I recommend that you do not rely on contract language to demonstrate your implementation of this Requirement. Instead, I suggest the implementation of your processes include documentation that you have followed these processes step-by-step.

This is in line with my recommendations in other articles that you always document your work so you can verify and validate that your processes are executed. For example, the effectiveness of your process for vendor incident notifications might be demonstrated by documenting actual or simulated notifications from the vendor, including your response to such notifications.

CIP-013-1 R3

You are required to obtain CIP Senior Manager (or designated delegate) approval for the supply chain cyber security risk management plan on or before the initial enforcement date of July 1, 2020.

To ensure that your supply chain cyber security risk management plan remains up-to-date, you are required to review it at least every “CIP year,” or 15 calendar months. I strongly recommend that you consider reviewing the plan on either a shorter timeframe or have a provision to review the plan based on need (such as an emerging threat or a pending major procurement).

Each review should take into account any additional risks that have emerged since the prior review and should require those newly-identified risks to be added to your existing risks.

The entire assessment and remediation cycle should be performed to include consideration of the new risks. Each review should be documented and each time the plan is revised it should be approved by the CIP Senior Manager (or delegate).

Cyber Security Supply Chain Risk Consideration: A Starting Point

1. Obsolescence of the underlying platform

The expected lifetime of a SCADA, DMS, or other type of control system frequently far exceeds the expected lifetime of its underlying commercial hardware and operating system. How will you manage the risk of your hardware or software becoming unsupported? Will your vendor support a migration to an updated platform at a reasonable cost?

2. State of the art security

Will your vendor enable use of state-of-the-art security enhancements such as application whitelisting or software defined networking? Is the vendor flexible enough to adapt to newer techniques as they emerge?

3. Virtualization

If your vendor supports, or even requires, use of virtual systems, does the vendor support them in ways that are compatible with the currently enforceable CIP Requirements? For example, if the vendor mixes traffic from trusted networks (such as Electronic Security Perimeters) and untrusted networks on the same network hardware, this may put you at risk of a compliance finding.

4. Purchasing counterfeit hardware or software

How will you know that all components of the system you are acquiring are those actually made or approved by the system vendor? This is not usually an issue when a trusted vendor supplies all the components. But if you plan to purchase some components from another source, how will you mitigate the risk of obtaining compromised or substandard equipment?

5. Installing compromised genuine hardware or software

In 2017, the Danish shipping company Maersk installed one copy of compromised software on an internal computer. This software was provided by the original developer, but that developer had been compromised and malicious code placed in an updated package. This resulted in the compromise of nearly every computer within the company and paralyzed its global operations for an extended period of time.

6. Vendor personnel

If vendor personnel are to be granted access to your systems for any reason,

Continued on page 11

Continued from page 10

how will the vendor demonstrate to you that those personnel have been appropriately screened and trained? What controls will the vendor agree to for this purpose?

7. Vendor VPN access

If vendor personnel are to be permitted remote access to your systems via VPN, how will the vendor manage the risk of compromising your systems due to weak security at the originating computer? If the originating computer has been compromised, the malware will have access to your Intermediate Systems and will put them at risk. Similarly, if the originating computer is permitted to talk to both your systems and to other networks (such as the Internet) at the same time, your systems may be exposed to traffic from unexpected sources. This is known as “split tunneling.”

8. Vendor system-to-system access

If systems at the vendor’s location are permitted direct access to your systems, any compromise or weakness in the vendor’s systems will put your systems at risk. How will the vendor manage this risk? How will you know that the vendor is managing this risk?

9. Vendor information management

If your vendor will retain sensitive information about your systems such as, for example, network diagrams or administrative account credentials, how will the vendor protect this information? Will you be notified if this information is compromised?

10. Vendor internal security precautions

If your vendor is providing a service to you, such as a managed security service provider that performs log analysis and alerting, how does the vendor protect its own internal systems? Will you be able to assess the effectiveness of the vendor’s protections? Will you be notified of any compromise of the vendor’s systems?

11. Vendor termination process

When you discontinue your relationship with a vendor, will this transition proceed in an orderly, defined manner? What happens to any sensitive information in the vendor’s possession?

12. Adaptability to new risks

When ransomware appeared as a threat in early 2018, many entities were forced to make rapid changes to their network environments. Will your vendor support rapid response to emerging threats?

13. Vendor acquisition or dissolution

If your vendor goes out of business or is acquired by a different company, how will you support your system? Will you have access to the source code? Will licenses expire?

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

In addition, if you would like RF Entity Development staff to review your supply chain cyber security risk management plan and provide you with feedback, you can request this through the Assist Visit link above. Be aware that RF will not make compliance determinations in advance of an audit, but can only raise concerns and indicate areas for improvement.

Feedback

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

I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 2 of 3)

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

In my Nov/Dec 2018 article, I discussed CIP-013-1, Supply Chain Risk Management, at a high level. I discussed how I think CIP-013-1 is at the same time plan-based, objective-based, and risk-based. In my Jan/Feb 2019 article I provided a suggested structure for a risk management plan. In this article I'll continue what I began in the Mar/Apr 2019 article, which was a detailed look at the supply chain risk management Requirements for CIP-013-1.

I had planned to cover the supply chain changes to both CIP-005-6, Electronic Security Perimeters, and CIP-010-3, Configuration Change Management and Vulnerability Assessments, in this article, but to allow me to get more in-depth I will cover CIP-010-3 in the Jul/Aug issue as the third part of this now three-part article. Please remember that if you choose to adopt any of my suggestions, you must adapt them to your entity's position in the Bulk Electric System, and to your entity's systems and policies.

On the May Reliability and Compliance Open Forum Call, I presented a brief overview of the supply chain Standards which includes a slide with links to relevant documents. The presentation from that call is here.

If you want to participate in these monthly calls, the information is on the Compliance Monitoring page of the RF Website.

Huron Lightship, Port Huron, MI - Photo by Lew Folkerth

Malicious Remote Access

Suppose you're the EMS engineer in charge of your primary control system. One afternoon as you're getting ready to go home, you get a call from the operations supervisor. Some of his operators are having trouble with their control consoles. The mouse associated with each console is not working properly. It seems to be moving the display cursor on its own, and not responding to the actual movements of the mouse. As you're speaking, he reports that a breaker controlled by one of the consoles has just been commanded to open. He asks what can be wrong with the systems, and why his operators have suddenly lost control of BES operations. How quickly can you fix this problem and get his operators back in control?

Is this fiction? No. This is the scenario that actually occurred on December 23, 2015, in Kiev, Ukraine (see *Analysis of the Cyber Attack on the Ukrainian Power Grid* here.) And this is the scenario that I believe motivated FERC to address the ability to control vendor remote access. In this article, I'll discuss how the risk of this scenario can be reduced, and how your response can be designed to quickly remediate an actual incursion.

CIP-005-6 R2 Parts 2.4 and 2.5

In Order 829 at P 51-55, FERC required NERC to develop a Reliability Standard to address the risk of vendor remote access to BES Cyber Systems. The new Standard was to cover both interactive and system-to-system remote access. FERC explained that its concerns included malicious use of stolen credentials, possible compromise of a trusted vendor, and use of a vendor's access to compromise or control a BES Cyber System. FERC also stated that an entity

Continued on page 15

Continued from page 14

should be able to “rapidly disable” remote access connections.

CIP-005-6 includes two new Parts. You are required to have methods “for determining” (Part 2.4) and “to disable” (Part 2.5) active vendor remote access sessions. Let’s look at the enforceable language of each Part in detail:

R2: Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in:

Applicable System	Requirements
High Impact BEC Cyber Systems and their associated PCA; and Medium Impact BES Cyber Systems with External Routable Connectivity and their associated PCA	Part 2.4: Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).
	Part 2.5: Have one or more method(s) to disable active vendor remote access (including Interactive Remote Access and system-to-system remote access).

Let’s look at some important points regarding this language:

1. We can look at these Parts as bringing certain Electronic Security Perimeters (ESPs) into scope. All ESPs that contain a high impact BES Cyber System are in scope. All medium impact ESPs that have at least one Electronic Access Point (EAP) associated with the ESP will also be in scope. Within these in-scope ESPs, all Cyber Assets will be in scope. Remember that if any Cyber Asset is within an ESP that has an EAP, the Cyber Asset will almost certainly have External Routable Connectivity (see *The Lighthouse* from Jul/Aug 2015 available here.)

2. Looking at the Requirements, we see we’re dealing with several terms not defined in the NERC Glossary. You may need to incorporate your own definitions of any non-glossary terms into your processes and procedures. If you do so, be careful to use commonly accepted definitions and apply them in a way that makes sense in the context in which they’re used and that achieves the intent and purpose of the standard.

3. The scope of these Parts includes all data communications into or out of every in-scope ESP, not just routable network traffic. Dial-up, serial leased line, or other communications can also be construed as “remote access,” even if it does not employ a routable protocol.

4. These Parts are silent as to how quickly you must be able to respond to an identified issue. In my opinion, identification of malicious remote access sessions and disabling of such access should be achieved in seconds or minutes, not hours or days. If you doubt this, ask your system operators how long a malicious actor should be allowed to control their systems.

5. While the term “vendor” is defined in the Rationale section of the Standard, remember that this section is considered to be guidance and is not enforceable. Rather than be concerned about the precise definition of “vendor,” I recommend that, for these Parts, you disregard the term and provide equal consideration for all communications into and out of an in-scope ESP. This will probably be simpler from a compliance perspective and certainly more effective from a security perspective.

6. These Parts are also silent on recovery. I recommend that your processes include methods of capturing forensic evidence, so you can identify the cause of the incursion and correct the weaknesses that led to it. As any malicious remote access meets the definition of a Cyber Security Incident, your CIP-008 incident response plan should be activated. Make sure the incident response plan has provisions for dealing with cases of malicious or unauthorized remote access. Also, when recovering systems back to normal operating mode your CIP-009 recovery plan may need to be invoked. Ensure it has provisions for these circumstances.

Continued on page 16

Continued from page 15

How can you control remote access in a manner that meets the security objective of Parts 2.4 and 2.5? I suggest a layered approach to this problem:

Identification:

Control of remote access traffic begins with understanding all traffic that crosses the ESP border, including any traffic that bypasses the ESP border such as dial-up or serial communications. You should already have a good handle on this from the existing CIP-005-5 Requirements, but I think it's time to revisit this topic in more depth. You should clearly understand (and document) the need for each type of traffic permitted into or out of the ESP.

> What are the endpoints of the traffic, the source and destination, and what service is provided?
>
> Who uses this service, and why is it needed?
>
> Which firewall rules permit this traffic?
>
> How does it contribute to reliability? What would be the impact if the traffic is blocked?

If the far endpoint for this traffic is compromised, can this traffic be used to compromise BES reliability?

All of these questions should be answered and documented for use in the items below.

Categorization:

Once you identify the traffic, you should categorize the traffic based on reliability need. Consider these as possible categories for your traffic:

- Required for operations under all conditions, normal and emergency
  - This traffic will probably include ICCP feeds to your BA, RC, and/or TOP. It will also probably include monitoring and control links between Control Centers and field devices like a substation RTU or a generator DCS.
- Required for normal operations, but may be suspended for emergencies
  - This category might include engineering workstation access into the production network for routine maintenance and configuration. Traffic that is part of a historian system that is not used for situational awareness might also be included here.
- Convenience connections, not necessary but useful for saving time or labor
  - Most Interactive Remote Access probably falls here, such as engineering connections from home to permit after-hours response.
- Other connections
  - In my opinion, there should be no traffic in this category. If it doesn't support operations, and doesn't save time or labor, why is it permitted into or out of the ESP?

Classification:

Classify the traffic by the type of party you're communicating with:

- Internal: Communication is within your entity's networks or within secure communication links between such facilities.
- Registered Entity: Communication is to another Registered Entity (BA, TOP, etc.).
- External Party: Communication is to another party not subject to the CIP Standards. I consider this traffic to be "vendor" traffic.

Prioritization:

Determine which traffic must be kept operational under various conditions. You might develop three conditions of operation: normal conditions (no suspected threat), heightened security (response to a suspected threat), and maximum security (response to a probable or confirmed active threat).

Response Preparation:

There are some actions you can take to proactively reduce your exposure to remote access threats.

- Architecture:

  Your vendors should not have direct access into your ESPs. If a vendor must have remote access, consider giving your vendor access to a test or QA environment rather than the production control systems. To the greatest extent possible, modify your architecture so that only traffic that is absolutely necessary is permitted into the ESP.

Continued on page 17

Continued from page 16

- Network Configuration:

  You should review your network configuration to determine if modifications can increase the isolation of systems that are capable of remote access. For example, it may be possible to restrict the network visibility of a console that is the target of Interactive Remote Access by placing it on its own VLAN internal to the ESP and restricting traffic to and from that VLAN to the rest of the ESP. This type of segmentation can be valuable in increasing security, but be careful that it doesn't disrupt operations.

- Simplification:

  There may also be opportunities to prevent traffic from crossing the ESP boundary. Services such as Active Directory or network printing could be moved to dedicated devices within the ESP to prevent that traffic crossing the ESP boundary. Analyze this type of change carefully to make sure you are actually improving overall security.

- Security Appliances:

  You may be able to incorporate security systems such as a Security Information and Event Management system or Intrusion Detection System into your remote access protections. Remember, though, that you are after very fast response times and there may not be time to run reports or do extensive analysis.

Response Planning:

Once you know your traffic and have optimally configured your networks, you should plan your response scenarios. At a minimum, you must be able to turn off access to any traffic classified as "vendor" traffic above. A good way to organize the response is to incorporate the prioritization levels identified above. Your target here is to get maximum improvement in security for a minimum in response time. To me, this indicates the need for pre-planned and pre-tested configuration changes that can be implemented with minimum risk to reliability.

These configuration changes should be manually-initiated automated processes so that manual processes don't slow the response or introduce errors in the network configuration. In planning for this type of response, be sure to consider your change control processes.

You don't want to have a required change approval slow down your response to an emergency. Test your automated processes thoroughly. The goal is to improve reliability, but these processes could also have unintended consequences if not properly vetted.

Training and Exercises:

Ensure all personnel who will be responsible for recognizing and reporting instances of malicious or unauthorized remote access are trained in these skills and that their training stays fresh. Ensure the personnel who are to receive these reports are confident and proficient in their roles so they can respond quickly and properly to any identified incursion. Frequent exercises will help with this.

How you detect a remote intrusion and how you disable any such detected access will depend greatly on your position in the BES, on the systems you use, and on your personnel. While I don't have specific advice for detecting and disabling malicious connections that defeat your protective measures, I do believe the planning and preventive actions I've described above will help.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

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

I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 3 of 3)

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

In my November/December 2018 article, I discussed CIP-013-1 at a high level. I discussed how I think CIP-013-1 is at the same time plan-based, objective-based, and risk-based. In my Jan/Feb 2019 article I provided a suggested structure for a risk management plan. This article completes my series on the in-depth study of the supply chain cyber security risk management Requirements that was begun in the Mar/Apr and May/Jun 2019 issues. I'll also answer some questions that have been presented to me and to the ERO Enterprise. Please remember that what follows are my opinions and my suggestions. If you choose to adopt any of these suggestions, you must adapt them to your entity's position in the Bulk Electric System, and to your entity's systems and policies.

CIP-010-3 R1 Part 1.6

In Order 829 at P 48-50, FERC required NERC to develop a Reliability Standard to address the verification of both the identity of the software publisher and the integrity of all software and patches for BES Cyber Systems. FERC stated that the objective of these changes is to reduce the likelihood of the installation of compromised software on a BES Cyber System.

In response to Order 829 P 48-50, one new part has been added to CIP-010-3. You are required to perform software verification by verifying the integrity of both the software source and the software itself. Here's the enforceable language of Part 1.6:

R2: Each Responsible Entity shall implement one or more documented process(es) that collectively include:

Port Sanilac, MI - Photo by Lew Folkerth

Applicable Systems	Requirements
High Impact BES Cyber Systems: and Medium Impact BES Cyber Systems Note: Implementation does not High Impact BES Cyber Systems; and require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Part 1.6: Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.

Continued on page 11

Continued from page 10

Supply Chain Questions

The ERO has begun receiving requests for guidance regarding the application of the supply chain Standards, especially CIP-013-1. Here are the questions I've seen so far, and my answers to them.

Q: How many levels (tiers) of vendors must an entity consider for CIP-013-1 Compliance?

A: The responsibility for determining how deep into the vendor supply chain to delve lies with you, the Responsible Entity, through your supply chain cyber security risk management plan.

CIP-013-1 is silent on how deep into the vendor supply chain you must go. My recommendation is that you should know as much about your equipment, software, and services as possible. I suggest that you document as much as you can about your BES Cyber Systems and their makeup, using your CIP-010 baselines and expanding on each baseline with as much detail as you can gather. From this information you can compose a list of hardware, software, and services that are used in your systems.

CORRECTION

In my Mar/Apr 2019 article I said, "Any purchase arrangement or contract you enter into on or after the CIP-013-1 effective date of July 1, 2020, must be developed in accordance with your approved supply chain cyber security risk management plan." This is incorrect. It should read, "Any procurement begun on or after the CIP-013-1 effective date of July 1, 2020, must be performed in accordance with your approved supply chain cyber security risk management plan."

You can then assess your hardware, software, and service list based on risk. For example, you would probably assess the cyber security risk of a server power supply as very low. You would probably assess the cyber security risk of a network-connected out-of-band server management device as high or severe.

You should then be able to create a list of vendors of your devices, software, and services, and prioritize that list based on the assessed risk of each component a vendor supplies.

Q: If I buy routers at Office Depot, does that constitute a "contract" or is that just a procurement?

A: Any equipment, software, or services whose acquisition is begun on or after July 1, 2020, that will become or will be directly related to a high or medium impact BES Cyber System must be acquired in accordance with your supply chain cyber security risk management plan. The plan must be used whether or not a contract is involved. The only place in the enforceable language of CIP-013-1 where the term "contract" appears is in the note to Requirement R2. Risks incurred by acquisitions from vendors such as Walmart (yes, they do carry business-grade Cisco products) or sellers of new and used equipment on eBay are some of the risks this Standard is intended to mitigate. In particular, there could be an elevated risk of compromised or counterfeit hardware from such sources.

Enforceable Elements of a Standard

From the NERC Standard Processes Manual Section 2.5, "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority."

In addition, Glossary terms and Implementation Plans may be separately approved as mandatory and enforceable.

The term "contract" also appears in the definition of "vendor" in the Rationale section of the Standard, but that definition does not appear in the enforceable elements of the Standard. The definition may be useful as guidance, but be cautious about relying on the exact wording. For example, the use of "contract" in the definition appears to restrict the application of CIP-013-1 to only those parties with which the Responsible Entity has a formal contract. This restriction is not supported by the enforceable elements of the Standard, which means you cannot rely on that aspect of the definition.

Q: Will a Responsible Entity be expected to perform and document initial cyber security risk assessments on all its existing vendors that provide their BES Cyber System products and services prior to the compliance effective date?

A: No, CIP-013-1 affects only new procurements. This answer is supported by the General Considerations section of the Implementation Plan:

"In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or

Continued on page 12

Continued from page 11

direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in a contract do not determine whether the procurement action is within scope of CIP-013-1."

In order to determine the begin date of a procurement, you must document that date in a manner suitable for use as audit evidence. Without such documentation, audit teams will use the earliest date that provides reasonable assurance of the beginning of the procurement process.

Q: If I procured hardware or software from a vendor prior to 7/1/2020, but installed that hardware or software after that date, must I perform a risk assessment of that vendor?

A: Risk assessments of vendors that provided equipment, software, or services prior to the CIP-013-1 effective date of July 1, 2020, are not required. Any procurements for high or medium impact BES Cyber Systems equipment, software, or services begun after July 1, 2020, must be performed in accordance with your documented CIP-013-1 R1 supply chain cyber security risk management plan. Any software installed on or after July 1, 2020, must have its identity and integrity verified, regardless of when the software was obtained.

Q: Contracts for procurement that are in place prior to July 1, 2020, are not in scope for CIP-013. What about contract renewals?

A: CIP-013-1 applies to any procurements begun after July 1, 2020, regardless of the existence of a standing contract, and regardless of any revisions to such a contract. You are not required to invalidate or renegotiate any contract, but you must demonstrate that any procurement begun after July 1, 2020, has been performed in accordance with your supply chain cyber security risk management plan. You will need to establish a beginning date for the procurement. The effective date of a contract is not necessarily the beginning of a procurement. The beginning date might be the date of an expenditure authorization or a request for bid, quote, etc. You will then need to show how you followed your risk management plan throughout the acquisition.

Q: My source for equipment says that they are not a "vendor," but rather a "supplier," and so they are not subject to CIP-013-1. How do I answer this?

A: Any organization or person that supplies equipment, software, or services to your entity must be considered a "vendor" in the meaning of CIP-013-1. Your "supplier" is quite correct to say that they are not subject to CIP-013. Only NERC Registered Entities that are procuring hardware, software, or services that will become or that will directly affect high or medium impact BES Cyber Systems are subject to CIP-013-1. It is your relationship with each vendor, supplier, etc. that is subject to CIP-013-1, not the vendor itself. In managing that relationship you may use many tools, including purchase or acquisition contracts, existing vendor practices such as incident notification, existing or emerging security practices, such as software verification, vendor web site features such as digital certificates and digital signatures, and so forth. Although you may choose to manage your vendors through contracts, CIP-013-1 does not explicitly require this. If your vendor will provide a feature or a service as part of its ongoing security practices, there may be no requirement for a contract for such matters. And you may show that the implementation of your risk management plan accomplishes its goal of reducing supply chain risk by means other than contracts.

Requests for Assistance

If you are an entity registered within RF 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 rfirst.org web site here.

In addition, if you would like RF Entity Development staff to review your supply chain cyber security risk management plan and provide you with feedback, you can request this through the Assist Visit link above. Be aware that RF will not make compliance determinations in advance of an audit, but can only raise concerns and indicate areas for improvement.

Feedback

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

I may be reached here.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Low Impact Update and Final Check; Supply Chain Update

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

Low Impact Update

There are three pending changes to the Reliability Standards that will have an effect on entities with low impact BES Cyber Systems.

CIP-003-7

CIP-003-7 will become effective on January 1, 2020.

The Implementation Plan for CIP-003-7 states that CIP-003-6 Attachment 1 Sections 2 and 3, the sections governing physical and electronic access controls, do not become enforceable. Instead, they are replaced by CIP-003-7 Attachment 1 Sections 2 and 3 which become enforceable on January 1, 2020. Additional changes in CIP-003-7 are discussed below.

CIP-003-8

CIP-003-8 will become effective on April 1, 2020, just three months after the effective date of CIP-003-7. The only change to the enforceable language of the Standard is the addition of a requirement to mitigate detected malicious code in third-party Transient Cyber Assets (TCAs).

CIP-012-1

As I write this, CIP-012-1 is pending regulatory approval. If approved, CIP-012-1 will be applicable to all Control Centers, including those BA and GOP Controls Centers that contain only low impact BES Cyber Systems. I plan to cover CIP-012-1 in depth in a future article.

Fort Gratiot Lighthouse, Port Huron, MI - Photo by Lew Folkerth

Low Impact Final Check

Since the effective dates of CIP-003-7 and CIP-003-8 are rapidly approaching, it's time for a final check of your compliance posture for low impact BES Cyber Systems before these revisions go live. Below I list the Standards and Requirements that are applicable to low impact BES Cyber Systems and provide a brief summary of each Requirement.

The accompanying summaries are written from the low impact perspective only. Unless otherwise noted, the language from an older version is unchanged in the newer versions. Upcoming dates are italicized. You must refer to the Standards for the exact wording of each Requirement.

This "Low Impact Final Check" is written from the perspective of an entity that has low impact BES Cyber Systems only.

If you also have high or medium impact BES Cyber Systems, many of your policies, processes, and procedures can be adapted to encompass your low impact BES Cyber Systems as well.

Continued on page 10

Continued from page 9

CIP-002-5.1 R1 Part 1.3 (Effective Date July 1, 2016)

You are required to identify each asset (such as a Control Center, substation, or generating facility) that contains at least one low impact BES Cyber System. While you are not explicitly required to identify each BES Cyber System at the low impact level, you may need to do so for other requirements. This is further explained in CIP-003-7 R2 Attachment 1 Sections 2 and 3, below.

Evidence for CIP-002-5.1 R1 Part 1.3 should include:

- Your determination of any assets that are not BES assets (assets with no component that meets the BES definition are out of scope for the CIP Standards);
- A description of how you determined that each asset contains (or does not contain) a BES Cyber System; and
- A description of how you determined that each BES Cyber System contained by the asset has a low impact rating (as opposed to a medium or high impact rating).

CIP-002-5.1 R2 (Effective Date July 1, 2016)

You are required to review the asset identifications from Part 1.3 every "CIP year" (15 calendar months). This review must be documented as audit evidence, and any changes to the asset identifications should be explained.

For example, if a new substation was commissioned, you should provide the commissioning date and any impact the new substation might have on the impact rating of neighboring substations. You also need evidence of your CIP Senior Manager's (or delegate's) approval for these identifications every CIP year.

CIP-003-6 R1 Part 1.2 (Effective Date April 1, 2017)

Cyber security policies that apply to the assets identified in CIP-002-5.1 R1 Part 1.3 must be documented. The policies must address four areas: cyber security awareness, physical and electronic access controls, and incident response.

Your evidence should include the documented policies, the review of these policies at least every CIP year, and your CIP Senior Manager's approval (no delegation permitted) at least once every CIP year.

CIP-003-7 R1 Part 1.2 (Effective Date January 1, 2020)

Cyber Security policies must be added to address Transient Cyber Assets (TCAs), Removable Media, and CIP Exceptional Circumstances at assets containing a low impact BES Cyber System.

CIP-003-6 R2 Attachment 1 Section 1 (Effective Date April 1, 2017)

Section 1 requires reinforcement of security awareness at least once every CIP year. You should keep evidence of the type and content of the reinforcement, the dates the reinforcement was provided, and that the reinforcement was provided to all groups, such as employees and contractors, who have access to assets containing low impact BES Cyber Systems.

CIP-003-6 R2 Attachment 1 Sections 2 and 3 (No Effective Date)

Sections 2 and 3 of version 6 will not become enforceable. They have been superseded by Sections 2 and 3 of version 7.

CIP-003-7 R2 Attachment 1 Section 2 (Effective Date January 1, 2020)

You are required to control physical access. You have two options to control access. You may choose to control physical access to the asset containing a low impact BES Cyber System or you may control physical access to the low impact BES Cyber Systems at the asset. I

f you choose to control physical access to the low impact BES Cyber Systems, you must be able to identify all BES Cyber Systems at the asset and show that physical access to each BES Cyber System is controlled.

You must also control physical access to Cyber Assets that control electronic access to low impact BES Cyber Systems. Your evidence will need to identify these systems and show that physical access to them is controlled.

These systems do not need to be located at the asset they are protecting (see Reference Model 3 in the Guidelines and Technical Basis). But wherever they are located you must control physical access to them.

Your evidence should include a description of the controls in place, and you should take credit for multiple layers of control if you use them. For example, you might list a gated and locked substation perimeter fence, a locked control house, and a locked equipment cage within the control house as layers of physical access control.

CIP-003-7 R2 Attachment 1 Section 3 (Effective Date January 1, 2020)

You are required to control routable electronic access to and from your low impact BES Cyber

Continued on page 11

Continued from page 10

Systems. The Guidelines and Technical Basis of CIP-003-7 contains ten Reference Models that explain possible methods of protection. Some reference models show protections for the entire asset containing the low impact BES Cyber Systems.

Others show protections at the BES Cyber System level. If you choose to protect just the BES Cyber Systems, you will need to be able to identify all BES Cyber Systems at the asset.

Your evidence should identify the types of access you permit and the business or operational need for the access. Remember that you must provide the justification for each type of permitted access, not just what the access is.

For example, just identifying that port 502 is permitted will be insufficient. You should state that the MODBUS/TCP protocol is permitted over port TCP/502 to and from switchyard equipment in order to monitor and control that equipment from the SCADA system.

Your evidence should include a discussion of how you meet the security objective of reducing the attack surface of your BES Cyber Systems through electronic access controls. Your discussion should also include why you think your controls will be effective in meeting the security objective.

If you permit dial-up access into a BES Cyber System, your evidence should show how you authenticate a dial-up user.

CIP-003-6 R2 Attachment 1 Section 4 (Effective Date April 1, 2017; New Terms Effective January 1, 2021)

Section 4 requires development and testing of Cyber Security Incident response plans for low impact BES Cyber Systems. Be aware that Section 4 relies on the NERC Glossary definitions of *Cyber Security Incident* and *Reportable Cyber Security Incident*, which will change when CIP-008-6 becomes effective on January 1, 2021.

Your evidence for Section 4 should include all incident response plans that are applicable to assets containing low impact BES Cyber Systems. You should be able show that each asset containing a low impact BES Cyber System has at least one applicable incident response plan.

Each incident response plan must include the components specified by Sections 4.1 through 4.6. Each incident response plan must be tested at least once every 36 months. When testing, be sure you can document that the incident response plan itself was actually tested.

One of the best ways to do this is to include an incident response checklist in your plan, and complete the checklist whenever the plan is tested. Keep the completed and dated checklists as evidence of testing of the plan. Note that you can use a response to an actual Reportable Cyber Security Incident as a test of the plan.

The last step in an incident response is usually a “lessons learned” review of the test or the actual incident. As no plan is ever perfect, you can usually find items to improve in your plan after each use of the plan. Track these items and be able to show that you have updated the plan within 180 days of the test or actual incident.

One way to do this is to keep a detailed revision history for the incident response plan, including the source of each change and the dates of the changes.

CIP-003-7 R2 Attachment 1 Section 4 (Effective Date January 1, 2020)

Version 7 of Section 4 updates the ES-ISAC reference to a reference to the E-ISAC.

CIP-003-7 R2 Attachment 1 Section 5 (Effective Date January 1, 2020)

Section 5 permits the use of, and requires controls for, TCAs and Removable Media at your assets containing low impact BES Cyber Systems. The existing NERC Glossary definitions of *Transient Cyber Asset* and *Removable Media* have been modified slightly to accommodate low impact considerations.

You must develop one or more plans to mitigate the risk of malicious code being introduced to a low impact BES Cyber System. Each plan should include provisions for TCAs managed by you, the Responsible Entity. The plan may call for managing these TCAs in either an ongoing or on-demand manner, or both. The plan also needs provisions for TCAs managed by a third party, such as a vendor or contractor. Finally, the plan must address detection and removal of malicious code on Removable Media.

Evidence for Section 5 should include each applicable plan, and each plan should show how you achieve the objective of mitigating the risk of introducing malicious code to a low impact BES Cyber System.

For TCAs managed in an ongoing manner, evidence should focus on the process of preventing malware from being introduced to the TCA. For TCAs managed in an on-demand manner, evidence should focus on the process used to ensure the TCA may be safely connected to a low impact BES

Continued on page 12

Continued from page 11

Cyber System prior to such use, including removal of any detected malicious code.

Evidence regarding use of Removable Media should include the controls used to ensure all Removable Media is cleared of any malicious code prior to connection to a BES Cyber System.

CIP-003-8 R2 Attachment 1 Section 5 (Effective Date April 1, 2020)

The only change to the enforceable language in CIP-003-8 is the addition of an explicit requirement to clean any malicious code from a third-party TCA before connecting the TCA to a BES Cyber System. Your plans should already require this, but be sure to review your plans to ensure they meet the new language.

CIP-003-6 R3 (Effective Date July 1, 2016)

You are required to document the identification of a CIP Senior Manager. Evidence of this designation must include the CIP Senior Manager's name, the date of the designation, and the date the designation was documented.

CIP-003-6 R4 (Effective Date July 1, 2016)

This Requirement permits the delegation of the CIP Senior Manager's authority as permitted by the Standards. For example, the CIP Senior Manager may delegate the authority to approve the list of assets containing low impact BES Cyber System, but may not delegate the approval of cyber security policies.

If delegations are used, evidence must include the name or title of the delegate, the specific actions delegated, the date of delegation, the approval of the CIP Senior Manager (usually a signature), and the date of the documentation of the delegation.

Supply Chain Update

The NERC Critical Infrastructure Protection Committee (CIPC) has issued five Security Guidelines and associated training materials related to supply chain cyber security. The Guidelines address five topics:

1. Risk Considerations for Open Source Software
2. Provenance
3. Cyber Security Risk Management Lifecycle
4. Secure Equipment Delivery
5. Vendor Risk Management Lifecycle

Each is a short (4-5 pages) paper accompanied by a training presentation. The papers and presentations are available on the NERC web site here (Security Guidelines - CIP Security.)

Note that these Guidelines are not directly compliance related. They are not Implementation Guidance, and they are not enforceable. Rather, they are a discussion of good security practices related to their specific topic. I recommend reading them, as they provide insight into various areas of supply chain cyber security that you may not have previously considered.

Requests for Assistance

If you are an entity registered within RF 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 rfirst.org web site here.

In addition, if you would like RF Entity Development staff to review your supply chain cyber security risk management plan and provide you with feedback, you can request this through the Assist Visit link above. Be aware that RF will not make compliance determinations in advance of an audit, but can only raise concerns and indicate areas for improvement.

Feedback

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

I may be reached here.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Remote Access - Advanced Topics

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.

In the March/April 2015 Newsletter I explored the basics of Electronic Security Perimeters (ESPs) and remote access (see article here). In this column, I'll discuss some advanced topics regarding remote access, including ways you can improve your compliance and security postures. Since I've seen many entities experience compliance issues in this area, my recommendations will go beyond the minimum requirements of the Standards. I do this to encourage you to improve the security of your BES Cyber Systems and to provide your entity with a more robust means of demonstrating compliance. One way of looking at remote access is that any communications traffic crossing your ESP boundary is remote access. However, the CIP Standards provide specific definitions and corresponding requirements for various types of remote access. While looking at this topic, I'll include considerations for CIP-005-6, Electronic Security Perimeter(s), which will take effect in the U.S. on July 1, 2020. Also, I will include considerations for CIP-012-1, Communications between Control Centers, even though it has not yet received regulatory approval in the U.S. In discussing electronic access control, I'll assume you are using a firewall as your access control device, but the discussion applies to other forms of access control as well, such as a router and its access control list (ACL).

Remote Cyber Asset Capabilities

In any remote access scenario, the capability of the remote Cyber Asset is of critical importance. At the high and medium impact levels, the remote Cyber Asset is any device outside the ESP that communicates with a device inside the ESP. At the low impact level, the remote Cyber Asset is any device outside the asset containing low impact BES Cyber Systems that communicates with a device inside the asset.

Sturgeon Point Light Station, MI - Photo by Lew Folkerth

You must ensure, and be able to demonstrate to an audit team, that any remote Cyber Asset does not meet the definition of a BES Cyber Asset. In other words, the remote Cyber Asset cannot have a 15-minute impact on the reliable operation of the BES. If the remote Cyber Asset does have this capability, then it meets the definition of a BES Cyber Asset and must be included in a BES Cyber System at the appropriate impact level. The BES Cyber System must then be accorded the protections of CIP-003-8 through CIP-013-1, as applicable to its impact rating. This applies to all remote access at all impact levels, not just Interactive Remote Access.

In support of this stance, let's refer to the FERC order that remanded an Interpretation of CIP-002-4, Critical Cyber Asset Identification, in March of 2013 (see inset). That order clearly states FERC's concern over the capabilities of remote Cyber Assets. While this order applies to CIP-002-4, which never became enforceable, the principle carries forward into CIP-002-5.1, BES Cyber System Categorization.

I'll add an example to that provided in the inset: a transmission operator's laptop computer is capable of Interactive Remote Access to the operator's normal workstation, which is a console within the Control Center. This console is a BES Cyber Asset included in a high impact BES Cyber System. Once the remote access is established, the operator can access the console as if the

Continued on page 16

Continued from page 15

14. For example, a laptop computer connected to an EMS network through the Internet may be used to supervise, control, optimize, and manage generation and transmission systems, all of which are essential operations. However, the proposed interpretation of "essential" may leave certain cyber assets lacking the required CIP Reliability Standards protection that could, if compromised, affect the operation of associated Critical Assets even though the unprotected cyber assets are using similar access and exerting the same control as cyber assets that are deemed under the proposed interpretation to be "necessary or inherent to the operation of the Critical Asset." The proposed interpretation, in effect, would create a window into the EMS network that could be exploited.

[Order on Interpretation of Reliability Standard, Docket RD12-5-000, March 21, 2013, at P14]

operator were sitting at the console keyboard. This will grant the operator the same operating capability as the console, which includes the ability to control various elements of the BES in real time. The operator's laptop computer can therefore have a 15-minute impact on the BES, which makes the laptop computer a BES Cyber Asset.

Another concern is the ability of the remote Cyber Asset to access or store BES Cyber System Information (BCSI). BCSI must be protected and securely handled during storage, transit and use as required by CIP-011-1 R1, Information Protection. If the remote Cyber Asset has the ability to access BCSI, then such access must conform to your information protection program required by CIP-011-1 R1. If the remote Cyber Asset has the ability to store BCSI, then it must be designated as a storage location for BCSI, and access to it must be authorized and verified in accordance with CIP-004-6 R4, Personnel & Training.

Procedural vs. Technical Controls

CIP-005-6 requires technical controls for each Requirement and Part. It's a good idea to layer procedural controls on top of the technical controls. This will reinforce the concept that remote access to protected systems must obey strict rules. But you must not rely on the procedural controls alone. Your firewall rules must protect your networks from inadvertent and malicious use of remote access.

Remote Access Protocols

Let's take a closer look at what constitutes a remote access client. The language of the Interactive Remote Access definition says that Interactive Remote Access uses a remote access client but doesn't further define what a remote access client is. This isn't really a problem because there is no way to determine what software is being used to initiate the access from a remote Cyber Asset. The only indication we have is the communication protocol being used to access the system within the ESP.

Your audit team will look at your firewall ruleset to see if any communication protocols capable of interactive access are permitted from a location other than an Intermediate System.

Here are some common remote access clients and the protocols they use:

Remote Access Client	Protocol	Well-known Port(s)
Remote Desktop	Remote Desktop Protocol (RDP)	TCP/3389
Terminal Emulator	Telnet	TCP/23
Many free and commercial programs	Secure Shell (SSH)	TCP/22
Web browser	HTTP, HTTPS	TCP/80, TCP/443
FTP Client	File Transfer Protocol (FTP)	TCP/20, TCP/21
File explorer, etc.	SMB	TCP/445
File explorer, etc.	NFS	TCP/2049, UDP/2049
MIB Browser	SNMP	TCP/161, UDP/161
Unix r-commands	rlogin, rcp, rsh, etc.	TCP/513

CIP-005-6 R2 Part 2.1 requires all Interactive Remote Access to utilize an Intermediate System. In order to enforce this Requirement you will need technical controls that do one of the following:

- Ensure that all communication protocols that permit interactive access into the ESP originate only at an Intermediate System. The firewall ruleset (or router ACL) will provide your auditors with the evidence they need to determine compliance.

- If you permit a remote access communication protocol from a Cyber

Continued on page 17

Continued from page 16

Asset other than an Intermediate System, you must provide additional technical controls to ensure that interactive access is not permitted.

One of the protocols listed in the table above is Secure Shell (SSH). SSH has many capabilities and can present problems in demonstrating that your Intermediate Systems are not being bypassed. The SSH client, which communicates with the SSH protocol, is designed for interactive access. But the SSH protocol is also commonly used for system-to-system access.

Interactive and system-to-system access both use the same protocol, so your firewall can't tell the difference. Neither can your auditors. It is up to you to be able to demonstrate that a remote connection using the SSH protocol from a Cyber Asset other than an Intermediate System cannot be used for interactive access. I plan to discuss methods of doing this in a future article.

Demonstrating Compliance

CIP-005-6 R2 Parts 2.1-2.3 do not require you to implement Interactive Remote Access. If you choose not to permit Interactive Remote Access into your ESPs, then you do not need Intermediate Systems, multi-factor authentication, etc. But you must still be able to demonstrate that your technical controls do not permit interactive access. And, as discussed above, if you do implement Interactive Remote Access you must still show that your Intermediate Systems cannot be bypassed with an interactive-capable protocol. Since this topic is inextricably entwined with firewall rule management as a whole, I'll base my discussion on CIP-005-6 R1 Part 1.3.

Demonstrating compliance with CIP-005-6 R1 Part 1.3 begins with your change management program for firewall rules. Before a new rule is put into production, it should receive a rigorous review. To avoid common problems with the documentation of access control rules, and to ensure your security is as effective as possible, I strongly recommend going beyond the minimal requirements of the Standard.

Here are the items I recommend you consider and document for each rule:

- Nature of the remote device: What type of device is at the far end of this connection? Who owns it? How is its security managed?
- What port or port range will need to be permitted? Is the traffic inbound or outbound?
- What protocol will be used on this connection?
- What is the operational purpose of this traffic? What does it contribute to the reliable operation of the BES?
- What type of access does this rule permit?
    - Interactive Remote Access
    - ESP-to-ESP
    - System-to-system
    - Vendor remote access
        - If so, you must have a method to disable the access per CIP-005-6 R2 Part 2.5
    - Control Center to Control Center
        - Prepare for CIP-012-1 protections (e.g., encryption)
    - Other?
        - If so, what?
- When this rule is implemented, what capability will the remote device have?
    - Could it have a 15-minute impact on the BES?
        - If so, it must be identified as a BES Cyber Asset, included in a BES Cyber System, and protected.
    - Could it have access to BCSI?
        - If so, your information protection program must be applied.
        - If it will be able to store BCSI, it must be identified as a BCSI storage location and access controlled per CIP-004-6 R4.
- What changes to remote systems, companies, etc. might cause this rule to be modified or removed? You should have a method of monitoring for events that should trigger a re-evaluation of a rule.

When you have the information listed above, I recommend that you perform a risk assessment of the rule in the context of the operational purpose of the rule. Your risk assessment should answer these questions:

- Does the capability provided by this rule justify the risk this rule adds?
- Can this traffic be intercepted?
- Can this traffic be compromised?
- Is this traffic considered Interactive Remote Access? If so, is it through an Intermediate System?

And, once you have assessed the risk of a rule, what mitigations should you apply to minimize the risk the rule presents?

- Can the scope of the rule (e.g., port ranges, address ranges) be

Continued on page 18

Continued from page 17

reduced?

- Should this traffic be monitored? If so, how?
- Should this traffic cause an alert? If so, under what circumstances?
- Does this traffic need additional protections? If so, what is needed?

In order to keep this information up to date, I recommend that you periodically review the information and assessments listed above. This is not explicitly required by CIP-005-6 but is a good practice to minimize both your security risk and compliance risk by catching changes that might slip through your normal processes.

I also recommend that you monitor traffic crossing your ESP boundary to look for patterns of traffic that are new, unexpected, or vary from your normal patterns. There are several commercial and open source tools to help you do this.

On the topic of monitoring, I also recommend monitoring the content of Interactive Remote Access sessions. Monitoring remote sessions can provide assurance that the remote access is being used in accordance with the need for which it was granted. This may need to be implemented on the Intermediate System, since encryption is required up to the Intermediate System.

Remote Cyber Asset Security

Many of the Cyber Assets that remotely access devices within the ESP are not within the scope of the CIP Standards. Even though they are not in scope, I recommend that you consider implementing controls to reduce the security risk these Cyber Assets present. For example, a device engaged in Interactive Remote Access over a Virtual Private Network (VPN) should not permit other network traffic at the same time as VPN traffic. This is known as split tunneling and is a serious risk to the protected Cyber Asset being accessed.

Protections on the remote Cyber Asset should include:

- Prohibiting split tunneling;
- Ensuring no personal devices can be used for remote access;
- Managing access permissions on the device – ensuring administrative access is strictly controlled;
- Managing security patches for all software on the device;
- Hardening the device to reduce its attack surface;
- Ensuring no unauthorized software can be installed on the device;
- Storing the device in a secure location when not in use;
- Keeping anti-malware software and signatures up to date; and
- Enabling a host-level firewall on the device.

This is not an exhaustive list, but it might serve as a starting point in your consideration of this issue.

General Recommendations

In summary, CIP-005-6 requires that you tightly control all traffic crossing the ESP border. You should document all traffic so there is no question of what the traffic is for and why it is needed. Meeting minimum compliance Requirements in this area may not be enough. You may find it useful to go beyond minimum compliance to ensure you have the documentation to provide an audit team with reasonable assurance that you are meeting compliance for each Requirement.

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.

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.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Out-of-Band Management

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 is a condensed version of a more detailed article that can be found in full length on the RF website here.

What is Out-of-Band Management?

Out-of-band management is a method of managing computer systems that does not rely on having a physical presence at the computer system. This approach involves a network interface on the computer system that is used outside of the normal network connectivity, hence the term “out-of-band.” Since the purpose of out-of-band management is to manage the server remotely, almost all out-of-band management is a form of remote access.

Most data center-class servers have the capability for out-of-band management. For example, Dell offers its “integrated Dell Remote Access Controller (iDRAC),” and Hewlett Packard Enterprise offers the “integrated Lights Out (iLO)” controller. All server vendors I’ve researched offer some form of this capability.

Out-of-band management is usually implemented by adding a controller with its own network interface to the server. The controller is an additional small computer with extensive monitoring and control capabilities for the server.

Remote Console

A significant feature of a management controller is the ability to access the server’s hardware console remotely. This is not the same as using remote access client software to sign in to a Windows or Linux operating system. Once you sign in to the management controller, you can bring up the remote console and see the same display as the hardware video port on the server. The remote keyboard and mouse behave exactly like they are directly connected to the server.

40 Mile Point Lighthouse, Rogers City, MI – Photo: L Folkerth

Why is this important? The remote access capability is available even before the system boots its installed operating system. On power up, the remote console sees the boot-up sequence and can enter BIOS and other console-only modes to configure the system, possibly without further authentication.

Web Interface

The management controller has many more capabilities. Many of these can be accessed through a web interface via the management port on the server. The web interface capabilities include:

- Monitoring server temperatures, voltages and power consumption;
- Setting the device that the server will boot from next;
- Power on, power off, or perform a hardware reset to cause a reboot;
- Upload a disk image to the management controller internal storage and then boot from that image;
- Create a blank disk image on the internal storage and make that image accessible to the server; and
- Download an image from the internal storage.

Continued on page 6

Continued from page 5

One of the exercises I've performed involved obtaining administrative access to the server through documented features of the management controller (and a little password cracking). With only default credentials, I was able to obtain files containing encrypted passwords. I then cracked the encrypted passwords on a penetration testing system and was able to remotely sign in to the server's operating system with full administrative privileges.

Are out-of-band management capabilities inherently bad? Of course not. They can be very useful in managing a server at locations such as substations or control centers that do not have local IT staff to manage the IT-type systems. Use of out-of-band management capabilities can improve reliability by shortening downtime and by permitting monitoring of systems so preventive actions can be taken in a timely manner.

Compliance and Security Recommendations

Identification

The best approach I've seen in applying the CIP Standards is to identify the management controller as a Cyber Asset that is part of the hardware of the server. Since it is part of the server, it must be classified the same as the server. For example, if the server is part of a high impact BES Cyber System, then the management controller would be identified as part of the same BES Cyber System. The controller would be tracked in your documentation as a separate Cyber Asset, even though it is actually part of the server.

Whether you use this approach or devise an approach of your own, be sure to identify and document ALL of these management controllers. Audit teams are aware that these capabilities, if not protected, can present a high risk to reliability, and they are actively monitoring for any of these interfaces you might miss.

Networking

Most server vendors recommend connecting the management controller to a network that is separate from the other networks connected to the server, hence the "out-of-band" designation. For servers within an ESP, this separate network must also be within an ESP. Otherwise the management controller would be an EAP, a role it is not suited to adopt.

Access Control

You must control access to the management controller at least as tightly as you control access to the server itself. Interactive Remote Access to a management controller within an ESP must be through an Intermediate System.

Baselines, Patching, Etc.

The management controller should be subject to the same requirements as the server for baselines and change control, patch management, vulnerability assessment, ports and services, and password management.

Conclusion

Be sure to review all of your Cyber Assets within CIP scope and identify the out-of-band management capabilities of each. Document the presence of this capability on each applicable server, identify these devices in your Cyber Asset lists or baselines, and apply the appropriate CIP Standards to each. Be certain you have changed the default passwords.

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.

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.

The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Jan/Feb 2020

40 Mile Point Lighthouse, Rogers City, MI – Photo: L Folkerth

Out-of-Band Management

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.

What is Out-of-Band Management?

Out-of-band management is a method of managing computer systems that does not rely on having a physical presence at the computer system. This approach involves a network interface on the computer system that is used outside of the normal network connectivity, hence the term "out-of-band." Since the purpose of out-of-band management is to manage the server remotely, almost all out-of-band management is a form of remote access.

Most datacenter-class servers have the capability for out-of-band management. For example, Dell offers its "integrated Dell Remote Access Controller (iDRAC)" and Hewlett Packard Enterprise offers the "integrated Lights Out (iLO)" controller. All server vendors that I've researched offer some form of this capability.

Out-of-band management is usually implemented by adding a controller with its own network interface to the server. The controller is an additional small computer with extensive monitoring and control capabilities for the server. Server vendors implement the management controller in different ways: as an integral capability of the core server board, as a daughterboard on the core server board (illustrated in Figure 1), or as a separate device outside the core server.

In this article I'll discuss the functionality of the Dell iDRAC 6 Enterprise (see *Figure 1*) installed in a Dell R710 server in a security testing environment (see Figure 2). If you're up on Dell technology, you'll realize that this equipment is at least three generations old. But the capabilities remain in modern hardware, and in most cases the capabilities have been enhanced. Please note that neither RF nor I endorse or criticize any individual vendor. I am using Dell because used equipment is readily available and that's one of the systems I have access to in the security testing environment. In the exercises below, I am using only documented features of the equipment. I do not use any exploits or other penetration testing techniques against the iDRAC.

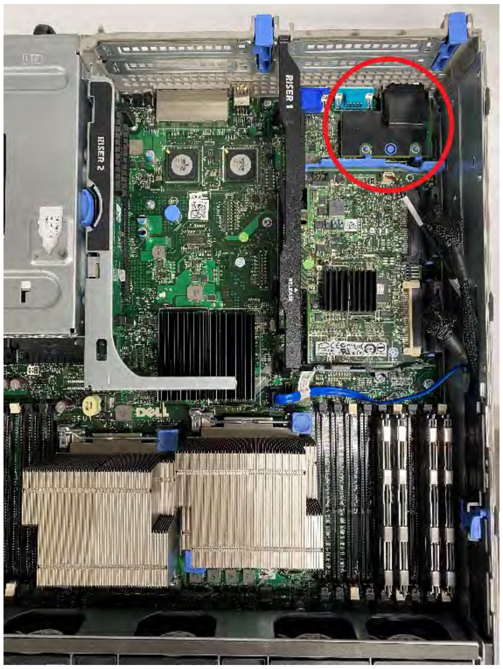


Figure 1 - The R710 Server with iDRAC 6 Enterprise Circled in Red

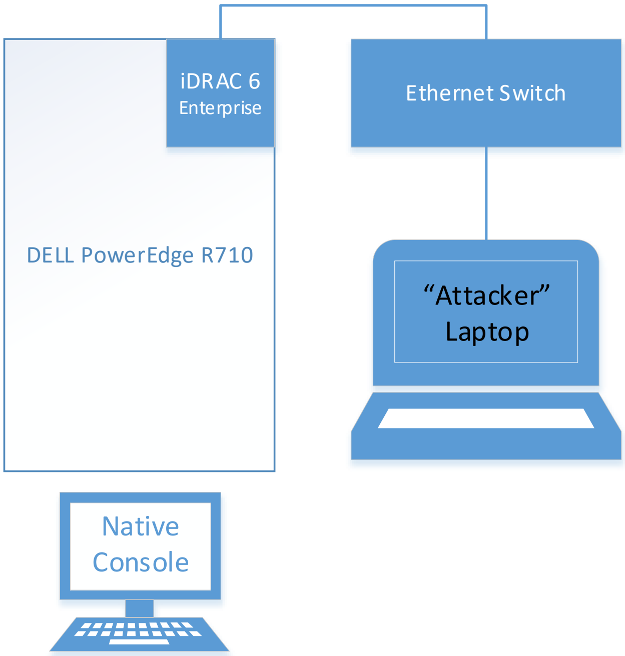


Figure 2 – Security Testing Environment

Remote Console

A significant feature of the iDRAC is the ability to access the server's hardware console remotely. This is not the same as using remote access client software to sign in to a Windows or Linux operating system. Once you have signed in to the iDRAC, you can bring up the iDRAC remote console and see the same display as the hardware video port on the server. The remote keyboard and mouse behave exactly like they are directly connected to the server. Why is this important? The remote access capability is available even before the system boots its installed operating system. On power up, the remote console sees the boot-up sequence and can enter BIOS and other console-only modes to configure the system, possibly without further authentication.

Figure 3 shows the security testing environment setup with the R710 at the BIOS screen and the native console being mirrored by the iDRAC remote console running on the laptop. In this mode I can make BIOS changes and any other changes that can be made from the local console.

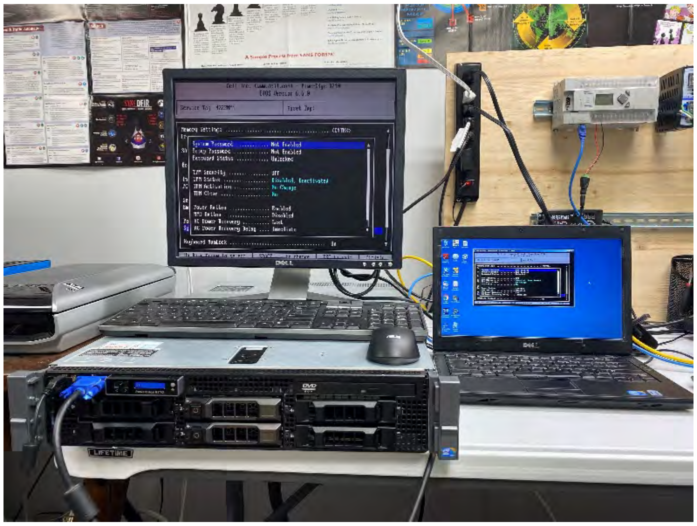


Figure 3 – Laptop Running iDRAC Remote Console at BIOS Screen

Web Interface

The iDRAC has many more capabilities. Many of these capabilities can be accessed through a web interface via the iDRAC port on the server. The web interface capabilities include:

- Monitoring server temperatures, voltages, and power consumption;
- Setting the device that the server will boot from next;
- Power on, power off, or perform a hardware reset to cause a reboot;
- Upload a disk image to the iDRAC internal storage, and then boot from that image;
- Create a blank disk image on the internal storage and make that image accessible to the server; and
- Download an image from the internal storage.

One of the exercises I’ve performed involved obtaining administrative access to the R710 through documented features of the iDRAC (and a little password cracking). With only the default iDRAC credentials, I was able to obtain files containing encrypted passwords. I then cracked the encrypted passwords on a penetration testing system, and was able to remotely sign in to the server’s operating system with full administrative privileges.

Are out-of-band management capabilities inherently bad? Of course not. They can be very useful in managing a server at locations such as substations or control centers that do not have local IT staff to manage the IT-type systems. Use of out-of-band management capabilities can improve reliability by shortening downtime and by permitting monitoring of systems so preventive actions can be taken in a timely manner.

Compliance and Security Recommendations for Out-of-Band Management

The out-of-band management controller has extensive capabilities to remotely control, modify and operate its host computer. But the price of that functionality is risk. For any BES Cyber System, Protected Cyber Asset (PCA), Electronic Access Control and Monitoring System (EACMS), or Physical Access Control System (PACS), that risk must be mitigated. We need to apply our best security and compliance practices to protect the management controller of an in-scope system. We begin by appropriately identifying the management controller within the CIP scope, and then apply the appropriate protections to the controller. The protections will include all applicable CIP Requirements, but may include additional protections as needed.

Identification – Integrated Management Controllers

Most servers will have the management controller built in to the server's motherboard or internally connected as a daughterboard (the R710 uses a daughterboard as seen in *Figure 1*). This means the controller is part of "the hardware, software, and data in those devices" per the definition of Cyber Asset.

The best approach I've seen in applying the CIP Standards is to identify the management controller as a Cyber Asset that is part of the hardware of the server. Since it is part of the server it must be classified the same as the server. For example, if the server is part of a high impact BES Cyber System, then the management controller would be identified as part of the same BES Cyber System. The controller would be tracked in your documentation as a separate Cyber Asset, even though it is actually part of the server.

Whether you use this approach or devise an approach of your own, be sure to identify and document ALL of these management controllers. Audit teams are aware that these capabilities, if not protected, can present a high risk to reliability and are actively monitoring for any of these interfaces you might miss.

Identification – Shared Management Controllers

Some servers employ shared management controllers. This can occur when more than one computer shares a single chassis. For example, Dell's VxRail Series G can contain four "nodes" (independent computers) in a single chassis. The iDRAC interface is housed in the chassis, not the node. The entire chassis, including the four nodes, is accessed through the single iDRAC controller in the chassis. If the chassis and all four nodes are considered to be one Cyber Asset, or all nodes are identified as the same classification, then the approach used for an integrated management controller could be used.

If the nodes are considered to be separate Cyber Assets with different classifications, the identification process becomes much more complex. You will need to demonstrate that internal access between nodes in the chassis is controlled, and that access through the management controller is controlled to the level required by the applicable Standards.

Let's look at some examples:

1. Assume a chassis has two nodes; Node 1 is classified as a BCA that is part of a high impact BES Cyber System and Node 2 is out of scope for the CIP Standards (see Figure 4). This is a case of mixed-trust within the chassis and will need to be carefully addressed. You will need to provide evidence that Node 2 has no access to Node 1 except through an Electronic Access Point (EAP). This will involve providing evidence that the management controller does not provide a communication path between the nodes, and the chassis does not provide a shared path to storage, memory, network, or other facility that could be used to transfer data to Node 1 or control Node 1. The management controller must be within an Electronic Security Perimeter (ESP) as it provides remote access to a BES Cyber System but cannot be an Intermediate System (an Intermediate System must be outside an ESP, so an EAP would need to be identified

between the management controller and Node 1). The management controller should be identified as an EACMS as it controls access to Node 1. The network interface of the management controller should be within an ESP, as the management controller does not have the ability to act as an EAP.

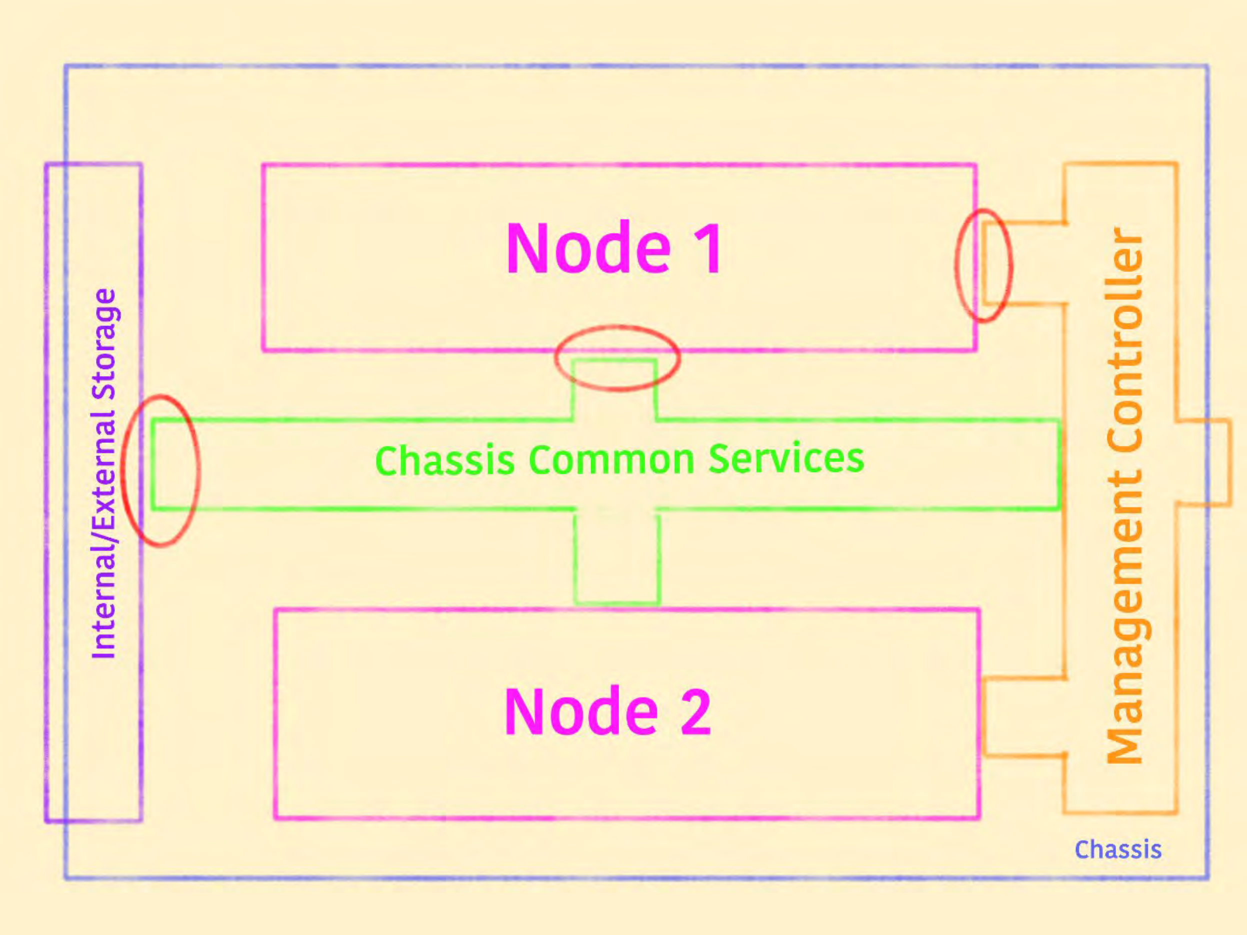


Figure 4 – Showing a two-node chassis with critical access points circled in red

2. While it may be possible to mix a node within an ESP and a node not inside an ESP on the same chassis and share a management controller, I do not recommend this approach. In order to demonstrate the logical separation of the nodes to an audit team, you will need to be able to provide evidence of the internal isolation of each node for each possible interface within the chassis (see Figure 4). I have not seen this done successfully in the field.

3. Now let's assume that Node 1 is an EACMS that is outside of an ESP and Node 2 is again out of scope (see Figure 4 again). Since we are outside of an ESP we don't need to have external network access to Node 1 or its management controller go through an EAP. How we identify the management controller in this situation gets very tricky. The controller itself does not meet the definition of an EACMS, since the definition only applies to a Cyber Asset that controls access to an ESP or BES Cyber System. That leaves no category within the CIP Standards with which to designate the management controller.

> However, the management controller does control access to Node 1 which is an EACMS. This means that to control access to Node 1, we must control access to the management controller in addition to controlling all other forms of access. That brings CIP-004-6 R4, Access Management Program, and R5, Access Revocation, into scope for the management controller.
>
> In addition, I strongly recommend voluntarily applying the full security protections of the CIP Standards to the controller, including restriction of network traffic (firewall), remote access through a jump host with multi-factor authentication, patch management, vulnerability assessment, security status monitoring, and change management. Above all, the default accounts and passwords for these devices are well known, so be absolutely sure you have changed the default passwords!

The remaining discussions assume an integrated controller for a system within an ESP.

Networking

Most server vendors recommend connecting the management controller to a network that is separate from the other networks connected to the server, hence the “out-of-band” designation. For servers within an ESP, this separate network must also be within an ESP. Otherwise the management controller would be an EAP, a role it is not suited to adopt.

Access Control

You must control access to the management controller at least as tightly as you control access to the server itself. Interactive Remote Access to a management controller within an ESP must be through an Intermediate System.

Baselines, Patching, etc.

The management controller should be subject to the same requirements as the server for baselines and change control, patch management, vulnerability assessment, ports and services, and password management.

Conclusion

Be sure to review all of your Cyber Assets within CIP scope and identify the out-of-band management capabilities of each. Document the presence of this capability on each applicable server, identity these devices in your Cyber Asset lists or baselines, and apply the appropriate CIP Standards to each. Be certain you have changed the default passwords.

In this short article I’ve only scratched the surface of management controllers and out-of-band management capabilities and concerns. As CIP and cyber security professionals, we must keep in mind the risks and benefits of using these capabilities, minimizing the risks and maximizing the benefits. We also need to monitor the Standards drafting efforts to ensure new CIP Standards meet our current and future needs.

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.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated. I may be reached at lew.folkerth@rfirst.org.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Foundations - Part 1

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 had some discussions recently that point out how much background is needed to be proficient in the CIP Standards. I think it's time to look at what all CIP professionals should have in their toolbox. Some may need more depth in certain areas, but the foundations of CIP should be fairly constant across all professionals. I don't advocate memorizing the Standards or other documents, but you should know where to find the essential documents and where to find the appropriate information within those documents.

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 Our Industry

In order to identify and protect the appropriate equipment and supporting systems, you should have a basic understanding of the electric industry and how it works. The electric industry is engaged in the generation, transmission and distribution of electric power.

To have the proper context in which to understand the CIP Standards, you should understand the industry's fundamentals and the associated terminology.

Our industry is based on electricity, in particular alternating current. You should understand the difference between electric potential, measured in volts and sometimes called "voltage," and electric current, measured in amperes or amps. You should understand the difference between real power, measured in watts; reactive power, measured in vars; and energy, measured in watt hours.

Old Presque Isle Lighthouse, Presque Isle, MI – Photo: L Folkerth

Generation is the process of taking energy in one form, such as heat, and turning it into electrical energy. **Transmission** moves the electrical energy from where it's produced (generation), to near where it's needed. **Distribution** takes electric energy from transmission and moves it to where it's finally used, known as "demand" or "load."

Generation of electric energy must match – on a moment-to-moment basis – the demand for electric energy.

As the demand for electric energy changes, generation must be adjusted to match so that neither too much nor too little energy is available at any time. This is known as "balancing" and is a critical process in the electric industry.

Understand the Role of Compliance in Our Industry

Priorities

As part of the electric industry, you must be aware of the proper place of compliance within the overall picture of the industry.

Continued on page 10

Continued from page 9

Electric Industry Priorities

1. Safety
2. Reliability
3. Compliance

The first priority is the **safety** of electrical employees and the general public. The second priority is **reliability**, “keeping the lights on.” Security, both physical and cyber, is considered to be part of reliability.

The third priority is **compliance**. The purpose of the CIP Standards is to improve reliability by keeping the equipment essential to reliability secure. The concept of CIP Exceptional Circumstances written into the CIP Standards is an acknowledgment of this fact.

Risk

Regulators and industry are coming to understand that the role of compliance is to manage and reduce risks to reliability. One of our newest Standards, CIP-013-1, Supply Chain Risk Management, is explicitly written to require risk to be managed. You should be familiar with risk management methods and risk assessments.

Understand Our Essential Documents and How to Read Them

Standards

In order to understand the CIP Standards, we need to understand the documents governing these Standards. First and foremost are the Standards themselves, but you need to know how to read them.

The NERC Reliability Standards, of which the CIP Standards are a part, are created according to the Standard Processes Manual. You should at least review this manual, which is Appendix 3A to the NERC Rules of Procedure, but carefully read Section 2.5.

The last paragraph of this Section tells us that the only mandatory and enforceable parts of a Standard are the applicability, the effective dates, and the Requirements.

In addition to these three enforceable components of the Standards, defined terms may be developed and approved for use in the Standards. These defined terms, once approved, appear in “Glossary of Terms Used in NERC Reliability Standards” (NERC Glossary) and are an officially recognized component of the Standards.

A Standard may also have an accompanying implementation plan containing effective dates and other information, such as initial performance of periodic Requirements. Implementation plans are approved as part of the Standard and are also enforceable.

All other parts of a Standard are considered guidance and may not be directly enforced. This guidance can help in understanding the Standard, but it cannot override the language of a Requirement.

For example, if a statement in the Measures section of a Standard conflicts with the language of a Requirement, the language of the Requirement prevails.

Guidance

The NERC Guidance Policy defines two types of approved guidance documents: Implementation Guidance and Compliance Monitoring and Enforcement Program (CMEP) Practice Guides.

Implementation Guidance is developed by industry and approved for adoption by the ERO. It provides examples of how a Standard or Requirement might be implemented.

CMEP Practice Guides are instructions for auditors and other CMEP staff to consider when assessing compliance to a Standard. They are developed by the ERO Enterprise and posted publicly.

Guidelines

Guidelines are developed by one or more NERC standing committees and are posted to the NERC website. Guidelines provide recommendations on how to improve or maintain the reliability of the BES. Although they are not enforceable, industry is encouraged to understand and follow them.

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.

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.

The Lighthouse

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

The Lighthouse

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.

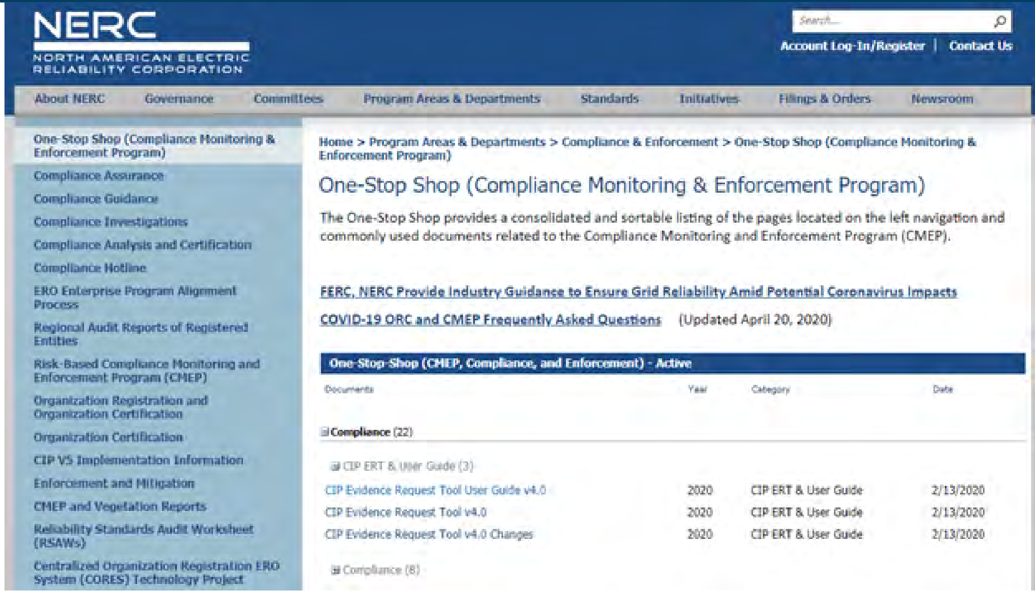
For a CMEP monitoring engagement (audit or spot check) within the RF footprint, you obtain the RSAW for a Standard from the NERC website and fill it out prior to the monitoring engagement. You will supply, in the appropriate sections:a list of subject matter experts responsible for the Standard, a list 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.


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
Search...
Account Log-In/Register | Contact Us
About NERC
Governance
Committees
Program Areas & Departments
Standards
Initiatives
Filings & Orders
Newsroom
One-Stop Shop (Compliance Monitoring & Enforcement Program)
Compliance Assurance
Compliance Guidance
Compliance Investigations
Compliance Analysis and Certification
Compliance Hotline
ERO Enterprise Program Alignment Process
Regional Audit Reports of Registered Entities
Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
Organization Registration and Organization Certification
Organization Certification
CIP V5 Implementation Information
Enforcement and Mitigation
CMEP and Vegetation Reports
Reliability Standards Audit Worksheet (RSAWs)
Centralized Organization Registration ERO System (CORES) Technology Project
Home > Program Areas & Departments > Compliance & Enforcement > One-Stop Shop (Compliance Monitoring & Enforcement Program)

One-Stop Shop (Compliance Monitoring & Enforcement Program)

The One-Stop Shop provides a consolidated and sortable listing of the pages located on the left navigation and commonly used documents related to the Compliance Monitoring and Enforcement Program (CMEP).

FERC, NERC Provide Industry Guidance to Ensure Grid Reliability Amid Potential Coronavirus Impacts

COVID-19 ORC and CMEP Frequently Asked Questions (Updated April 20, 2020)

One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active

Documents	Year	Category	Date
⊟ Compliance (22)			
⊟ CIP ERT & User Guide (3)			
CIP Evidence Request Tool User Guide v4.0	2020	CIP ERT & User Guide	2/13/2020
CIP Evidence Request Tool v4.0	2020	CIP ERT & User Guide	2/13/2020
CIP Evidence Request Tool v4.0 Changes	2020	CIP ERT & User Guide	2/13/2020
⊞ Compliance (8)			

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.

The Lighthouse

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.

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.

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.”

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

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.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Incident Response and Incident Management

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.

What's New in CIP-008-6?

CIP-008-6 will become effective on January 1, 2021. Changes in CIP-008-6 include:

- Electronic Access Control or Monitoring Systems (EACMS) are explicitly included in the Applicable Systems. This will include Intermediate Systems used for Interactive Remote Access and Electronic Security Perimeter boundary devices such as firewalls.
- The definitions "Cyber Security Incident" and "Reportable Cyber Security Incident" have changed to clarify that they apply to BES Cyber Systems at all impact levels. They also clarify that references to Electronic Security Perimeter, Physical Security Perimeter, and EACMS apply to high and medium impact BES Cyber Systems only.
- Your incident response plan now explicitly requires you to evaluate and define "attempts to compromise."
- Your incident response plan must include a process to determine if an event is an incident, a Cyber Security Incident, a Cyber Security Incident that was an attempt to compromise an Applicable System, or a Reportable Cyber Security Incident.
- You must use your incident response plan when responding to an attempt to compromise an Applicable System.
- You must retain records of your response to attempts to compromise an Applicable System.
- The new Requirement R4 contains explicit reporting language:
  - You must report Reportable Cyber Security Incidents and attempts to compromise an Applicable System.
  - Your incident reports must include certain specific information.
  - There are specified timelines for reporting:
    - Reportable Cyber Security Incident: 1 hour;
    - An attempt to compromise an Applicable System: Next calendar day;
    - Information updates: 7 calendar days.

As always, carefully read the enforceable language of the Standard (Requirements including referenced attachments, Applicability, Effective Date and Glossary terms) and base your compliance program on that language.

Big Sable Point, MI – Photo: L Folkerth

Also, there is a proposed Implementation Guidance document (not ERO approved as of this writing) that provides an overview of the structure and techniques for implementing CIP-008-6.

Low Impact

CIP-003-8, (Security Management Controls) Attachment 1 Section 4 uses the definitions for Cyber Security Incident and Reportable Cyber Security Incident. Even though CIP-003-8 doesn't

Continued on page 8

Continued from page 7

change on January 1, 2021, these definitions change and will be applicable to your CIP-003-8 compliance programs:

- The new definitions clarify that the Electronic Security Perimeter and Physical Security Perimeter language only applies to high and medium impact BES Cyber Systems.
- The term Reportable Cyber Security Incident now explicitly references BES Cyber Systems. You should know which systems owned by your entity are low impact BES Cyber Systems for incident reporting purposes. You can't just rely on asset-level determinations and still be consistent with the language of Section 4 and the Glossary.

CIP-005-6

The new language in CIP-005-6, contained in Parts 2.4 and 2.5, requires that you have the ability to "determine" and "disable" remote vendor connections. You may want to incorporate language to respond to Parts 2.4 and 2.5 in the appropriate incident response plan.

If an unauthorized party succeeds in exploiting a remote vendor connection, and that exploit results in the connection being disabled per CIP-005-6 Part 2.5, this will almost certainly meet the definition of a Reportable Cyber Security Incident and will require activation of your incident response plan. It would be prudent to have these actions already incorporated into your incident response plan.

Incident Management and Incident Response

The concept of incident response as applied to operational cyber assets has been around for decades. The concept of incident management began to be applied to these assets only in the last few years. Incident management is the art and science of providing leadership and pre-established processes to support incident response personnel. Incident management began in the 1970's with firefighters at California wildfires, but has been expanded and adopted in many areas. Electric utilities usually have mature incident management programs for disaster or storm response, but have not usually applied these techniques to Cyber Security Incidents.

If you want to learn more about incident management, I suggest the book "Incident Management for Operations" (Schnepp, Vidal & Hawley, O'Reilly 2017) as a good place to start. For example, one section explains the incident command structure and why such a structure is needed for incident response.

There is also an initiative underway to formally adapt incident management techniques to our operational control systems. Incident Command System for Industrial Control Systems (ICS4ICS) is being developed to bring the concepts of incident management to all aspects of our control systems. A good introduction to this concept, including links to FEMA advanced training on incident management, was presented by Megan Samford at the S4x20 industrial control system security conference. The video is available here.

CYPRES Report

FERC recently released a new study, "Cyber Planning for Response and Recovery Study (CYPRES)," available here. This document is a report based on observations from interviews of electric utilities by a joint team from FERC, NERC and Regional Entities. "Key Take-Aways" identified throughout the report may help you strengthen your incident response and recovery plans.

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 may be reached here.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Foundations Part 3 - Implied Requirements

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.

What is an Implied Requirement?

In the CIP Standards, an implied requirement is an action your entity must perform to comply with the Standards, even though that action is not directly stated in the text of a Requirement.

For example, CIP-006-6 (Physical Security of BES Cyber Systems) R1 Part 1.2 requires a physical access control to manage access into a Physical Security Perimeter (PSP). PSP is defined in the Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

NERC Glossary terms are developed in accordance with the Standard Processes Manual (Appendix 3A to the NERC Rules of Procedure) and approved by industry, the NERC board and FERC. When these NERC Glossary terms are capitalized in the text of a Requirement, they are part of the enforceable language of the Standard.

In order to control access into a PSP, you must know where the physical boundary of the PSP is, which means you need to identify the PSP and all of its access points. Therefore, identification of a PSP is required, even though such identification is not directly mandated by any Reliability Standard.

Identifications Implied by the Standards

Except for high and medium impact BES Cyber Systems and assets that contain a low impact BES Cyber System, which are explicitly required to be identified by CIP-002-5.1, all other types of systems or devices contain an implied requirement to identify them. This includes:

- BES Cyber Assets (BCA)
- Cyber Assets
- Dial-up Connectivity
- Electronic Access Control or Monitoring Systems (EACMS)
- Electronic Access Points (EAP)
- Electronic Security Perimeters (ESP)
- Intermediate Systems
- Physical Access Control Systems (PACS)
- Physical Security Perimeters (PSP)
- Protected Cyber Assets (PCA)
- Storage locations for BES Cyber System Information
- Transient Cyber Assets (if managed in an ongoing manner)

Windmill Point, MI – Photo: L Folkerth

Identification of Low Impact BES Cyber Systems

CIP-002-5.1 (BES Cyber System Categorization) R1 Part 1.3 requires you to identify each asset that contains a low impact BES Cyber System. But depending on how you implement the low impact protections, you also may need to identify each low impact BES Cyber System. To see why, let's look at CIP-003-8 Attachment 1 Section 2 (Physical Security Controls).

You are required to control physical access to "the asset or the locations of the low impact BES Cyber Systems within the asset." If you control physical access at the BES Cyber System level, such as by placing the low impact BES Cyber Systems in a locked cabinet (see Figure 1), then you will need to know which systems need to be protected, and you must be able to identify those systems to an audit team.

This reasoning also applies to Section 3 (Electronic

Continued on page 17

Continued from page 16

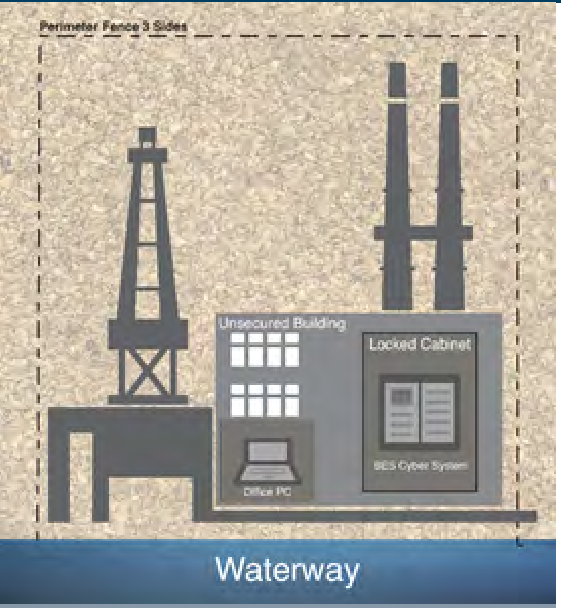


Figure 1 – It is not possible to control power plant access by a perimeter fence due to the waterway. In this case, the building also cannot be secured sufficiently to control access. Physical access to the low impact BES Cyber System is controlled by a locked cabinet. In this case, you must identify the BES Cyber Systems at this location so you know which systems must be protected.

Access Controls), Section 4 (Cyber Security Incident Response), and Section 5 (Transient Cyber Assets). If you don't apply the protections for these Sections at the asset level, then you must apply them at the Cyber Asset level which will require that you identify your low impact BES Cyber Systems.

Additional Examples of Implied Requirements

Some firewall vendors provide management consoles, which are separate workstations with proprietary programs that help manage and deploy firewall rules. A firewall administrator can authenticate with one of these management consoles and make changes to the firewall rules for an ESP boundary firewall. Those changes then can be deployed to the ESP firewall without further authentication. Since there is unrestricted access between the management console and the firewall, both the management console and the firewall must be identified as components of one EACMS.

All Interactive Remote Access must utilize an Intermediate System. Therefore you must either have technical controls in place to ensure protocols that can be used for Interactive Remote Access are not permitted to enter the ESP, or you must have technical controls in place to ensure these protocols cannot be used interactively.

I've discussed some of the most frequently violated implied requirements. There are many more, and I keep finding more as my understanding of the CIP Standards continues to mature.

Are Implied Requirements Enforceable?

All findings of Possible Non-Compliance (PNC) must be tied to a specific NERC Reliability Standard and Requirement. Since an implied requirement does not appear in the language of any Requirement, you will never see a violation of an implied requirement written as a PNC. What you will see is a PNC written for the consequence of not following the implied requirement. In our example, if you do not identify the physical boundary and access points of a PSP, you cannot demonstrate that you have controlled entry into the PSP. In this case, a PNC would be written for CIP-006-6 R1 Part 1.2.

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 may be reached here.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Using Advanced IT Technologies in an OT Environment Part 1 - Principles

Cooper Harbor, MI – Photo: L Folkerth

The Difference between Information Technology (IT) and Operational Technology (OT)

For the purposes of this discussion, I'll say that IT is the set of computing resources that deals with information, finances, inventory management, human resources, business processes – almost anything to do with a business and how it is managed falls into this category. One of the main concerns within an IT environment is cost of ownership, which drives return on investment.

In contrast, OT is the set of computing resources and devices that monitor and control equipment. Sensors might monitor temperature, voltage, current, pressure, fluid levels or other parameters. Actuators can be used to control equipment from afar, without human presence. In the area of the NERC Reliability Standards, OT encompasses all Cyber Assets subject to the CIP Standards. The primary concerns of OT are reliability, resilience and security.

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, resilience 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.

Lew's Principles for Adopting IT Technologies in an OT Environment

This is the first in a series of articles where I will discuss adopting technologies developed for IT environments into your OT environment.

I'll start by suggesting some core principles to apply to the analysis of IT technologies that are new to an OT environment.

1. Clearly identify the IT technology to be implemented

In order to effectively assess a technology for implementation in an OT environment, you must clearly understand the technology you will be implementing. Each technology has its own vocabulary, core concepts and principles. You need to review vendor claims and determine the parts of the technology that will be useful. Your entity must have a subject matter expert (SME) who understands the technology and can apply that knowledge to your environment.

As an example, let's say you plan to implement cloud computing in your Control Center. Rather than making such a broad statement, it might be better to say that you will implement a private cloud infrastructure to be contained wholly within the Electronic Security Perimeter. A private cloud is a type of cloud computing that does not carry all of the risks of a public cloud implementation. By using the more specific language, you have better defined the expectations of management and compliance staff.

2. Objectively assess the benefits

Any new IT technology will have obvious benefits in the IT environment, or you wouldn't be considering it for the OT environment. But take a close look at the technology from an OT perspective. Will the new technology improve reliability? Resilience? Security? If so, try to quantify your expectations. If not, why are you adding complexity for no operational benefit?

Continued on page 11

Continued from page 10

Be careful of vendor claims of benefits and performance. Remember that these vendors are generally selling into the IT market where reliability concerns are not as important. A 30-minute server outage in the IT environment is not usually a major concern, but a 30-minute SCADA outage is a reportable event. Once you've identified and quantified the potential benefits, make sure those benefits can be realistically achieved.

You might identify cost savings and reliability improvements from a private cloud implementation, for instance. Your staff will need full training on this technology prior to implementation. Also, don't neglect the ongoing skills maintenance needed to keep your staff fully effective in maintaining the new technology. Be sure to consider any actions needed to retain your now more-qualified staff. Factor these and other costs into the cost/benefit analysis. Providing the necessary training may erode the cost benefits, but if you don't train your staff, you will forfeit reliability benefits.

3. Objectively assess the risks

Any new technology will likely present new or heightened risks to your OT operations. You will need to identify and assess those risks and determine how to address them. Be sure you're assessing risks in the OT context – reliability, resilience and security. You should also include compliance risk in terms of the enforceable language of the NERC Reliability Standards and any other applicable standards. If the technology could increase the likelihood of a compliance violation, that should be factored into the decision. Also include in your assessment any side effects of implementing the technology, such as generating unit downtime.

In our private cloud example, be sure to contain the private cloud within an Electronic Security Perimeter if the cloud will be hosting high or medium impact BES Cyber Systems. If you are using or considering advanced technologies, such as a private cloud, you should be actively involved with the development efforts for the CIP Standards. See the NERC Reliability Standards under Development webpage for more information.

4. Perform a risk/benefit analysis in addition to a cost/benefit analysis

Most businesses require a cost/benefit analysis in order to make a procurement. In an OT environment you should also perform a risk/benefit analysis. In other words, do the benefits of the new technology justify the additional risk? Add the cost of mitigating the identified risks to the cost/benefit analysis. Make sure you include the cost of new and ongoing training and credential acquisition and maintenance for your staff. Factor retention of staff into both the risk/benefit and the cost/benefit analyses.

Review the risk/benefit analysis to ensure that the new technology improves the reliability, resilience and/or the security of the operation without impairing its compliance posture.

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.

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.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Using Advanced IT Technologies in an OT Environment Part 2 - Containers

In my previous article I discussed some recommended principles to follow when adopting new technologies into your Operational Technology (OT) environment. In this article I provide considerations for adopting container technology for use in OT systems.

Virtual Systems Old and New

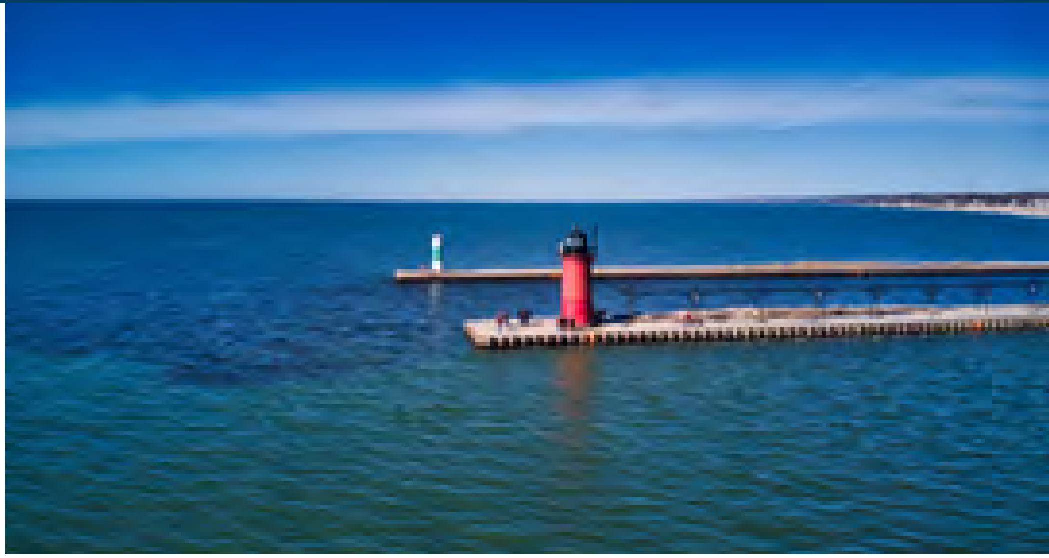
NERC recently published three Compliance Monitoring and Enforcement Program (CMEP) Practice Guides related to the use of virtualization technologies. The practice guides provide guidance to CMEP staff on how to assess the use of virtual systems, virtual storage and virtual networks in a CIP environment. I've seen many Entities use these three virtualization technologies successfully. You need to be careful to adopt these technologies in a way that doesn't compromise CIP compliance. The three CMEP Practice Guides should be useful in that effort.

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.

Recently, I've seen Entities begin to use a newer virtualization technology called **containers** or **containerization**. Containers are a way of encapsulating an application program to isolate it from other applications and to make deployment of the application easier and faster.

What are Containers?

Containers can be thought of as a lightweight form of virtualization. The technology uses features of the operating system to isolate the application in each container from the operating system and other containers. A container reduces the overhead required for a full virtual system, enabling more efficient and flexible use of computing assets.



South Haven N & S Pier Lights, South Haven, MI – Photo: L Folkerth

Each container begins with building a container **image**. The image will include an application and can include everything the application needs to run, such as libraries, programming language runtimes, utilities and configuration settings. Once an image is built, it cannot be modified. If an image needs modification, a new image must be built.

Container images that are in production typically reside in a **registry**, which is a method of storing and controlling approved container images. Once an image is built and tested, it is **pushed** to a registry. To run an application, it is **pulled** (copied) from the registry and executed.

Lew's Principles for Adopting IT Technologies in an OT Environment

1. Clearly identify the IT technology to be implemented
2. Objectively assess the benefits
3. Objectively assess the risks
4. Perform a risk/benefit analysis in addition to a cost/benefit analysis

Don't confuse containers with other types of virtualization. Containers can be, and frequently are, used in conjunction with virtual machines, but containerization is a separate technology that should be evaluated on its own merits.

Continued on page 13

Continued from page 12

Benefits of Containers

Packaging – The primary benefit of using containers is that application code is packaged with all the dependencies the application relies upon, such as libraries and runtimes. This keeps applications from interfering with each other. A patch or update to a runtime for one application might, without warning, break another application that uses the same runtime. For example, use of the Java language is common in development of real-time systems. Programs written in Java are compiled to an intermediate format known as bytecode. Bytecode is executed by the Java Virtual Machine (JVM) runtime. Java programs can be very sensitive to the version of the JVM being used. By placing the appropriate JVM in each container image, you can be certain that an incompatible version of the JVM will never be used.

Encapsulation – A container can expose only needed and expected network ports when it runs. If an application unexpectedly opens a new port, that port will not be accessible outside the container unless it is specifically permitted.

Abstraction – You can think of containers as systems at the application level, since each container includes dependencies needed for the application to run. The application and its dependencies can be tested and deployed as a unit.

Agility – Containers permit more flexibility in where and how applications are run. If one server becomes heavily loaded, containers can easily be started on other servers, which will reduce the load on the original server.

Immutability – Container images are **immutable**, meaning their contents cannot be changed after they are built. This helps prevent unauthorized changes to an application. Applications in running containers may become compromised, but if an application in a container image is compromised it will no longer run. This means that any malware that compromises a running container will not be able to persist through a restart of that container, making the malware's task more difficult.

Risks of Containers

Authenticity – Public container registries are convenient and easy to use, but these registries may not fully examine the software in the containers to ensure the software is free of malware. In this case, ease of use equates to higher security risk. Also, when building container images locally, building tools are usually configured by default to pull dependency software from public repositories.

Proliferation – Once software developers begin using containers, the use of containers tends to proliferate. This may lead to issues with change management and version control.

Environment – Containers can be configured to run on most modern operating systems. This may lead to containers being run in unintended environments.

Configuration – While containers help simplify some software deployment tasks, containers come with their own complexities. This may permit insecure configurations without the knowledge of the system owners.

Containers in a CIP Environment

If you're going to use containers in a CIP environment, you should carefully architect your internal controls to ensure you maximize the system's reliability, resilience and security while remaining within the bounds of compliance. The items below may serve as a starting point for your considerations.

→ BES Cyber Systems Identification

When you begin planning to bring containers into a CIP environment you will need to decide how you will identify the containers. The most popular method of identifying container images is through the baselines of CIP-010-3 R1, Configuration Change Management. Each container image can be documented by applying a unique identifier to the container image and then identifying the name and version of each software component in the image. The documentation should also include the Cyber Asset that each container created from the image is permitted to use.

→ Software Inventory and Version Control

You should maintain a list of container images authorized to run in your CIP environment. For each image, keep track of when the image was built; when, where and how it was tested; when it entered into service; what image was superseded by it; and change authorization records.

→ Software Integrity and Authenticity

One of the popular features of containers is the ease with which they can be built and deployed. There are public repositories with thousands of pre-built images ready for use by executing a single "pull" command. While easy and convenient, this functionality does not play well in a CIP environment. You must

Continued on page 14

Continued from page 13

be able to document the source of each software component in a container image. Each component must have integrity and authenticity (identification of software source) records in compliance with CIP-010-3 R1 Part 1.6. In addition, make sure you protect the registry where your container images are stored.

→ Patch Management

Each software component in a container image should be tracked by your patch management system. Because container images are immutable, whenever any component needs to be patched you will follow your process to create a new image.

→ Anti-Malware

After a container image is built, it should be scanned by your anti-malware tools. As the container image cannot be changed, malware cannot infect the image without causing the image to become invalid. Of course, container images should continue to be scanned as new malware signatures are published, but be sure to prevent a malware detection from quarantining files within the image, or that image will no longer be valid. If the malware detection is valid, you should immediately rebuild the image with clean components.

→ Vulnerability Management

Your processes for CIP-010-3 R3, Vulnerability Assessments, should be implemented as part of the testing process for each container image.

→ Audit Considerations

Containers are a new technology in CIP environments. You should let your Audit Team Lead (ATL) know you are using containers as early in the audit process as feasible. The ATL can then ensure the audit team has adequate preparation before reviewing your evidence. This should allow the audit to proceed normally, rather than needing to bring your audit team up to speed on the particular container implementation you are using during the busiest part of the audit.

→ Beyond the Standards

Advanced technologies need advanced security. Consider adding additional protections to your containers beyond the minimums required by the CIP Standards. For example, software defined networking permits much more control over network traffic than what is required by CIP-005-6, Electronic Security Perimeters. This tighter level of control may be appropriate in container environments.

Since container technology isn't yet directly addressed by the CIP Standards, you should develop a set of practices you adhere to when employing containers in a CIP environment. These practices should restrict how containers are built and deployed in order to maximize reliability, resilience, security and compliance.

Conclusion

Done properly, using containers in your CIP environment can improve reliability, resilience and security and streamline some compliance processes. But as with all things CIP: document, document, document!

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.

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.

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.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Keeping Up with a Changing World

In the last five years, our electricity industry has seen significant changes. We're seeing a whole new generation mix driven by the reduction in use of fossil fuels and the increasing use of renewable energy sources. Our operational systems are evolving. Non-substation based monitors located mid-span on transmission lines are being used to determine line ratings dynamically. Advanced Distribution Management Systems (ADMS) are driving new efficiencies and increased reliability at the sub-transmission and distribution levels. Synchrophasor measurements are beginning to be used in real-time systems. The technologies that drive our operational systems are being revolutionized by the expanding use of virtualization, containers and cloud computing. At the same time, new threats have arisen, such as ransomware and the public release of advanced cyberattack tools.

However, our current CIP Standards went into effect more than five years ago. Yes, we've seen the addition of Standards for supply chain and for communications security. And we've seen additional, but relatively minor, changes in other areas. But the core fabric of the CIP Standards remains unchanged since mid-2016. The CIP Standards are Reliability Standards, and Reliability Standards change slowly. This is a good thing in many ways. We have a stable set of cyber and physical security Standards that are effective in reducing risk to the Bulk Electric System (BES). On the other hand, some see the CIP Standards as getting in the way of new technologies and new forms of cyber protections. Let's see if there's a way to incorporate some of these new technologies or address new threats while staying within the bounds of compliance with the existing Standards.

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.

Pt Iroquois, MI – Photo: Lew Folkerth

Risk-based Standards

In my opinion, one way to keep pace with the rapid changes our industry is seeing is to develop a risk-based approach to the present CIP Standards. We already have a fully risk-based Standard in CIP-013-1, Supply Chain Risk Management. In CIP-013-1, you're required to develop, implement and maintain a risk management plan for certain areas of supply chain risk. I believe we can adopt risk-based techniques in our approach to compliance for most CIP requirements.

How do we begin? Let's start by choosing one area to improve using a risk-based approach. Figure 1 illustrates some of the areas we might consider. I'll choose a non-prescriptive Requirement, CIP-009-6, Recovery Plans for BES Cyber Systems, R1 Parts 1.3 and 1.4 covering backups and verification of backups.

Next, we'll need to identify the risks that we'll be addressing. This is somewhat backwards to the usual risk approach where we would identify and mitigate the highest risks in our risk register. In this case, one of the classic threats that can be mitigated by performing backups is the loss of a building by fire or other disaster. A new, at least in our context, threat is the encryption of systems and backups by ransomware.

Continued on page 11

Continued from page 10

Plan of Action

Figure 1 shows a modified risk management process. We'll use our known mitigation, backups, to select the risks that can be mitigated by backups. Then we will assess and prioritize these risks and design our backup systems to mitigate the highest priority risks.

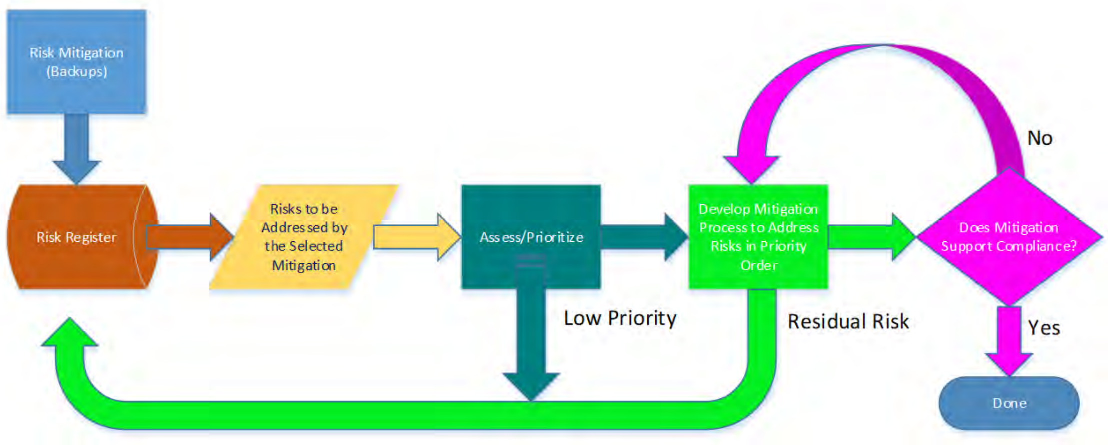

Risk Mitigation (Backups)
Risk Register
Risks to be Addressed by the Selected Mitigation
Assess/Prioritize
Develop Mitigation Process to Address Risks in Priority Order
Does Mitigation Support Compliance?
No
Yes
Done
Low Priority
Residual Risk

Figure 1

We'll partially mitigate the threat of fire by keeping the backups in a data center that is at a different location than the operational systems we're backing up. Mitigating the threat of ransomware will require a different approach. Ransomware works by encrypting all files accessible to a compromised system. If we keep our backups online, as is common practice, those backups are at risk of being encrypted along with the live files on our operational systems. In addition to keeping our backups at a different site, those backups must also either be offline or not writable by online systems.

When we have a process to mitigate the selected risks, we need to make sure that the process will meet the needs of our compliance program. If not, we need to re-design the mitigation process until it does meet our compliance needs. For example, we will need to make sure that all backup media is stored in a manner that conforms to our information protection program as required by CIP-011-2/3.

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.

Candidates for Risk-based Approach

Explicitly risk-based Requirements

- Supply chain
- Communications between Control Centers

Implicitly risk-based Requirements

- Vulnerability assessments
- Malicious code prevention
- Low impact BES Cyber Systems

Less-prescriptive Requirements

- Firewall rules
- Security event monitoring and alerting
- Incident response
- Recovery capability (backups)
- Information Protection

Risks not addressed by CIP (out of scope)

- Below the radar
  - ADMS
- Not operational technology
  - IT/corporate systems
- Historically out of scope but changing
  - PMU/PDC
- Beyond reach
  - Cloud infrastructure

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.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

BCSI Revisions

Crisp Point, MI – Photo: Lew Folkerth

On December 7, 2021, FERC issued a letter order approving CIP-004-7 (Cyber Security – Personnel & Training), CIP-011-3 (Cyber Security — Information Protection) and the associated Implementation Plan. The revised Standards implement changes in how BES Cyber System Information (BCSI) is protected. These changes were initiated by industry to address the growing need to be able to store BCSI in cloud environments. Vendor systems such as work management and trouble ticketing are migrating to cloud-only environments, and you need to use these systems to be able to fulfill other CIP requirements.

The revisions to CIP-004-7 move authorization for BCSI access from Requirement R4 to a new Requirement, R6. R6 explains what is meant by the term "access" and introduces a new term, "provisioned access."

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.

The language in CIP-011-3 Requirement R1 has been simplified to provide greater clarity and flexibility in implementing information protection.

CIP-004-7 sets requirements for managing access to BCSI, and CIP-011-3 requires an information protection program (IPP) to protect the confidentiality of BCSI. You should design your programs for CIP-004-7 R4, R5 and R6 and for CIP-011-3 R1 to work in concert to prevent compromising the confidentiality of BCSI.

"Obtain and Use"

One of the key concepts introduced in CIP-004-7 R6 is the clarification of the meaning of the word "access." R6 states, "To be considered access to BCSI in the context of this requirement, an individual has both the ability to *obtain* and *use* BCSI." [emphasis added] The "obtain and use" concept focuses our attention on the actual information being protected, rather than the storage locations for the information, and gives us the ability to store BCSI in cloud computing environments.

Think of BCSI as a car parked in your locked garage. Only you and your family may obtain (be able to touch) the car. However, this level of access is worthless without the ability to get into the car and drive away.

That requires that you can both *obtain* the car and have the keys to unlock and

Continued on page 11

Continued from page 10

drive (*use*) the car. You might park the car on a street (cloud environment) so that an unauthorized individual could *obtain* the car, but if you lock (encrypt) the car, no unauthorized individual can *use* the car.

The car might be towed away, denying you the ability to obtain the car, but whoever towed the car still cannot use the car without the keys.

"Provisioned Access"

CIP-004-7 R6 also introduces the concept of *provisioned access*. Based on the language in R6, *provisioned access* has these attributes:

- The access is for an individual (not a system);
- The access is granted as the result of "specific actions";
- The access is authorized;
- The access is needed ("based on need, as determined by the Responsible Entity");
- The access is either:
  - "Electronic access to electronic BCSI," or
  - "Physical access to physical BCSI".

Provisioned access must be authorized (Part 6.1), periodically reviewed (Part 6.2) and revoked as needed (Part 6.3). Access that is not provisioned access, such as unauthorized access, system access, etc. should be addressed by your CIP-011-3 IPP.

The use of the term *provisioned access* in R6 lets your BCSI access management program focus on the actions it is intended to perform – access by authorized individuals to BCSI within your control. All other forms of access should be addressed by your IPP.

Information Protection

CIP-011-3 R1 still requires an IPP, but the two Parts specifying the content of the IPP have been modified. Part 1.1 requires that your IPP have one or more methods to identify BCSI.

Part 1.2 requires one or more methods to mitigate the risks of the loss of confidentiality of BCSI. This new language makes CIP-011-3 R1 a limited risk-based Requirement, in that only confidentiality is addressed by R1. BCSI integrity and availability are not in scope for R1.

I recommend that you apply and document risk management techniques (see sidebar for references) to the tasks of protecting and securing your BCSI.

Consider IPP provisions based on risk that include:

- Prevention of unauthorized forms of access to BCSI;
- Loss of confidentiality of BCSI, perhaps to trigger an incident response and a compliance self-report; and
- Key management, for BCSI protected by encryption.

References

NIST SP800-209, Security Guidelines for Storage Infrastructure, October 2020

Security Guideline for Electricity Sector,Primer for Cloud Solutions and Encrypting BCSI, June 10, 2020

ERO Enterprise CMEP Practice Guide:BES Cyber System Information, April 26, 2019

Lessons Learned from Commission-Led CIP Reliability Audits

- 2019
- 2020
- 2021

A Structure for CIP Risk Management Plans, The Lighthouse, Jan/Feb 2019

SERC/RF Online Risk Management Training

NIST Publication SP800-209, Security Guidelines for Storage Infrastructure, lists various threats and risks to stored information that can be applied to BCSI. SP800-209 also provides insight into the attack surfaces that could be exploited by an attacker to compromise BCSI. The sidebar lists additional resources to help you in updating your IPP for the new Standards.

Continued on page 12

Continued from page 11

Authorization Paths

The revised Standards allow multiple paths for authorization of access to BCSI.

1. BCSI can and frequently does reside on the applicable BES Cyber Systems, EACMS and PACS themselves. When that is the case, provisioned access to that electronic and physical BCSI can be authorized by your CIP-004-7 R4 access management program and does not need to be repeated by your CIP-004-7 R6 BCSI access management program.

2. Other provisioned access to BCSI, such as document management systems, cloud storage, etc., is authorized by your CIP-004-7 R6 BCSI access management program.

3. Access not covered by CIP-004-7 R4 and R6 should be addressed by your CIP-011-3 IPP. The IPP should consider:
   a. Authorized access to BCSI that is not in scope for CIP-004-7, such as BCSI pertaining to medium impact BES Cyber Systems, EACMS and PACS without External Routable Connectivity.
   b. Authorized system (not individual) access to BCSI, if any.

Early Adoption

If you wish to take advantage of the increased flexibility afforded by CIP-004-7 and CIP-011-3, you may elect to adopt these Standards before their official (in the U.S.) effective date of January 1, 2024. If you choose to adopt them early these considerations will apply:

- Required:
  - You must notify all Regional Entities with which you are registered of the date you will begin compliance with CIP-004-7 and CIP-011-3.
  - You must continue to comply with CIP-004-6 and CIP-011-2 until that date.
  - Your new BCSI access management program should become effective on or before the date you begin compliance with CIP-004-7.
  - Your IPP should be reviewed for applicability with the new Standards, and any changes should become effective before the date you begin compliance with CIP-011-3.

- Recommended:
  - You are requested to notify your Regional Entities at least 90 days prior to the date you will adopt CIP-004-7 and CIP-011-3.
  - You are requested to adopt CIP-004-7 and CIP-011-3 on the first day of a calendar quarter.

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.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

CIP-014 Update

A lot has happened in the seven years since CIP-014, Physical Security, became effective. The ERO Enterprise (NERC and the six Regional Entities) now have significant experience with how industry implemented CIP-014. Note that on June 16, 2022, FERC approved CIP-014-3, which became effective on that date. As CIP-014-3 does not change any of the enforceable language of CIP-014-2, all references in this article will be applicable to both versions. In this article we'll discuss some of the things we've learned about CIP-014 and some new reference materials that apply to CIP-014. I'll review existing reference materials and bring out-of-date references up to date.

CIP-014 Summary

CIP-014 was created in response to the attack on the Metcalf Substation in California on April 16, 2013 [link in Reference 1]. The purpose of CIP-014 is to identify and protect high-consequence BES targets, including substations and Control Centers. CIP-014 requires, in part, risk assessments to identify applicable substations and Control Centers (R1), threat and vulnerability analysis (R4), and development and implementation of physical security plans (R5).

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.

Marquette Harbor, MI – Photo: Lew Folkerth

CMEP Practice Guide for CIP-014

A CMEP Practice Guide (PG) for CIP-014 R1 [link in Reference 1] was published on Nov. 21, 2021. This PG goes into depth describing how audit teams should evaluate an entity's performance of the risk assessments required by R1. The reason for this attention to R1 is that it is critical to have an accurate list of applicable Transmission stations and substations for the remainder of this Standard. The PG is divided into three main topics:

- **Reviewing the list of substations to be studied:** The PG details how to determine if CIP-014 is applicable to a given Transmission station or substation. The PG also discusses aspects of identifying assets that must be protected, including operating voltages, physical proximity, common facilities, diverse ownership and other considerations.
- **Selection and preparation of the models used in risk assessments:** The PG discusses topics such as the completeness of the model, characteristics of the model such as the load levels assumed and the appropriateness of the model for the risk assessments required.
- **Determining the completeness of the technical analysis performed:** The PG directs audit teams on how to review the entity's performance of system stability analyses, uncontrolled separation assessments and cascading analyses.

Although the CMEP Practice Guide's intended audience is CMEP staff (e.g., audit teams), the document is publicly available. You can gain a lot of insight into how you will be audited on CIP-014 R1 by studying it.

RSAW

The first version of the CIP-014 Reliability Standard Auditor Worksheet (RSAW) [link in Reference 1] contained instructions to the auditors that presumed reliance on the third-party verifications required by CIP-014 R2 and R6. The RSAW is being revised to remove impediments to fair and consistent auditing, enabling use of the CIP-014 R1 CMEP Practice Guide and the Evidence Request Tool during the audit. I expect the RSAW including these revisions, and updated for CIP-014-3, to be published soon after the publication of this Newsletter.

Continued on page 11

Continued from page 10

Implementation Guidance

The ERO has endorsed three Implementation Guidance documents for CIP-014 pertaining to R1, R4 and R5 [links in Reference 1]. All three were authored by the North American Transmission Forum (NATF) and provide guidance on identifying and assessing Transmission Facilities (R1), identifying and assessing threats to Transmission Facilities (R4), and developing and implementing a physical security plan (R5).

The Implementation Guidance for R5, "NATF Practices Document for NERC Reliability Standard CIP-014-2 Requirement R5," contains a good list of resources for developing physical security plans. In Reference 2 I've provided updates to these references as well as my description of each reference. Reference 3 contains my suggested additional references for your use.

Low Impact Considerations

If you compare the CIP-014 Transmission Owner applicability criteria 4.1.1.1 through 4.1.1.4 to CIP-002-5.1a Impact Rating Criteria 2.4 through 2.7 you will find they are identical. This may lead you to conclude that if you haven't identified any medium impact BES Cyber Systems at a substation, then you're not in scope for CIP-014-3. This is not necessarily correct. You should review these three considerations to determine if your substations are in scope for CIP-014:

1. Unlike CIP-002, CIP-014 is not about BES Cyber Systems, but instead is about physical assets. You need to evaluate your substations for CIP-014 applicability independent of your CIP-002 evaluation.
2. If you own a substation that is physically near another substation, you and the owner of the other substation should assess whether the two substations combined will meet any of the CIP-014 applicability criteria. If so, those substations are in scope for CIP-014 and must comply with at least Requirements R1 and R2.
3. Also unlike CIP-002, you must consider existing substations and also substations planned to be in service within 24 months from the time of your assessment. If those planned changes will bring a substation into scope for CIP-014, you must perform the R1 assessment and R2 third-party review for that substation.

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.

Reference Documents

Reference 1

- ***CIP-014-3: Click here***
- ***Metcalf sniper attack: Click here***
- ***CMEP Practice Guide CIP-014-2 R1: TBD***
- ***CIP-014-2, R1 Transmission System Risk Assessment (NATF): Click here***
- ***CIP-014-2 R4 Evaluating Potential Physical Security Attack (NATF): Click here***
- ***CIP-014-2, R5 Developing and Implementing Physical Security Plans (NATF): Click here***
- ***Petition for Modification to Compliance Section of CIP-014: Click here***
- ***Order Approving Modifications to the Compliance Section of Reliability Standard CIP-014, FERC Docket RD22-03-000, June 16, 2022: Click here***
- ***RSAWs: Click here***

Reference 2

Reference List (Additional Resources) from *NATF Practices Document for NERC Reliability Standard CIP-014-2 Requirement R5* (Lew's Updates and Descriptions)

ASIS

- ***Physical Asset Protection Standard (ASIS PAP-2021): Click here***
  - Softcover Member $35/Non-member $70; eBook $0/$35
  - 61 Pages
  - The documents referenced by the NATF Practices Document, *ASIS Facilities Physical Security Measures 2009* and *ASIS Security Management Standard: Physical Asset Protection 2012* have both been replaced by *ASIS PAP-2021*. *ASIS PAP-2021* walks the reader through developing and implementing a continuous improvement framework for a physical security program. An annex (appendix)

Continued on page 12

The Lighthouse

Continued from page 11

provides a high-level overview of physical protection techniques and technologies that can be employed.

DHS/CISA

- ***Energy Sector-Specific Plan 2015:*** ***Click here***
  - No charge
  - 39 Pages
  - While somewhat dated, the Energy Sector-Specific Program (SSP) provides a general risk overview that is still useful. It also provides a picture of where the Electric Subsector fits in the overall Energy Sector. This is one of the few documents in this list that mentions the importance of incident response.

IEEE

- ***IEEE Guide for Physical Security of Electric Power Substations (IEEE 1402-2021):*** ***Click here***
  - PDF $49/$61 Softcover $61/$76
  - 38 Pages
  - *IEEE 1402-2021* is a guideline written specifically to address considerations for physical protection of substations. Of particular interest are the sections on threat assessment, design considerations for threat mitigation, and a template for a substation physical security vulnerability assessment checklist.

IES

- ***The Lighting Library:*** ***Click here***
  - Annual Subscription $400/$800
  - *The Lighting Library* is the replacement for *The Lighting Handbook, 10th edition* (out of print, 1087 pages) referenced by the *NATF Practices Document*. *The Lighting Library* is a subscription-based service that provides access to the resources of the Illuminating Engineering Society. By my count, there are 140 documents in the *Library* covering all aspects of lighting science and engineering. I found the document listed below to be of particular interest.

- ***Security Lighting for People, Property, and Critical Infrastructure:*** ***Click here***
  - PDF $84/$120
  - 87 Pages
  - This document provides an in-depth look at the design of lighting for physical security purposes. It discusses basic principles of security lighting, visibility concerns, security zones, lighting equipment and applications.

NERC

- ***NERC Security Guideline for the Electricity Sector: Physical Security 2012:*** ***Click here***
  - 13 Pages
  - No longer available on the NERC website.
- ***NERC Security Guideline for the Electricity Sub-sector: Physical Security Response 2013:*** ***Click here***
  - 13 Pages
  - This was a draft version of the above document. No longer available on the NERC website.

Reference 3 – Lew's Additions to the Reference 2 List and Other References from Around the ERO

ASIS

- ***Protection of Assets – Physical Security, 2021 edition (PoA):*** ***Click here***
  - $159/$225
  - 643 Pages
  - The standards and guidelines above discuss "what" to do to provide physical protection for assets, this volume provides the "how" and "why." It provides an in-depth look at security risk management, security practices, design principles, tools, techniques and many other topics.
- ***Implementing Physical Protection Systems, A Practical Guide, 2nd edition:*** ***Click here***
  - David G. Patterson, CPP, PSP
  - $55/$65 (also available in Kindle $40)
  - 197 Pages
  - This book concentrates on the practical aspects of installation and operation of physical security systems.

Continued on page 13

Continued from page 12

O'Reilly

- ***Incident Management for Operations:*** ***Click here***
  - Schnepp, Vidal & Hawley
  - $18.41
  - 156 Pages
  - Beyond incident response there is incident management. This book discusses why incident management is needed and how to set up an incident management program.

NERC

- ***Security Guideline: Physical Security Considerations at High Impact Control Centers, December 12, 2018:*** ***Click here***
  - 13 Pages
  - This guideline discusses threat assessment, planning and security measures for control centers. While written with high impact BES Cyber Systems in mind, this guideline is useful at all impact ratings.
- ***Physical Security Guideline for the Electricity Sector, June 2019:*** ***Click here***
  - *Assessments and Resiliency Measures for Extreme Events*
  - 22 Pages
  - This guideline takes a different look at physical security from the perspective of extreme events. It includes discussions of planning for extreme events, vulnerability assessments, physical security assessments, drills and exercises, and information sharing.

MRO

- ***CIP-014-2 R1 Assessment Observations and Common Practices, November 2019:*** ***Click here***
  - 10 Pages
  - This presentation discusses audit considerations and common practices for CIP-014.

- ***CIP-014-2 Physical Security, R1, R2, R3 1st Quarter 2016 Guided Self-Certification 1Q 2016:*** ***Click here***
  - 13 Pages
  - This document was used for a 2016 self-certification in MRO.It contains a compliance checklist that may prove valuable.

- ***CIP-014-2 R1 Assessment Observations and Common Practices - ATC Assessment Practices, October 2019:*** ***Click here***
  - 13 Pages
  - This is a discussion of considerations regarding the risk assessment required by R1.

WECC

- ***Internal Controls Failure Points and Guidance Questions CIP-014-2, September 2020:*** ***Click here***
  - 8 Pages
  - This paper discusses internal controls and possible failure points in CIP-014 compliance.

RF

- ***CIP-014 R1 Methodologies, September 2015:*** ***Click here***
  - 18 Pages
  - An entity's perspective of the NATF guidance.
- ***CIP-014-X Update, April 2015:*** ***Click here***
  - 13 Pages
  - A discussion of the foundations of CIP-014.

SERC

- ***CIP-014-2 Audit Approach,* September 2019:** ***Click here***
  - 17 Pages
  - A discussion of audit approaches for CIP-014 with humorous touches.

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.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

CIP in the Cloud

This article is based on a presentation I gave at the 2022 NAES NERC Conference and the September Technical Talk with RF. It included additional background information about cloud services that you can read by viewing the presentation here.

In contacts with some of RF's Registered Entities, I'm seeing a movement of some operational functions to cloud-based technologies. A prime example is workflow management, where the software providers are well along in a Software as a Service (SaaS) delivery model. Some of these providers use methods that do not fit well with even the latest CIP Standards. Note that I am not necessarily promoting the use of cloud systems in the Operational Technology (OT) space, but I believe some cloud adoption is inevitable and we should get ahead of the adoption curve.

Potential Cloud Drivers for OT

Why move OT systems to the cloud? Unlike the move of IT systems into the cloud, moving OT systems should not be about cost. The only good reason to move OT systems to a cloud environment will be to improve reliability, resilience or security.

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.

Reliability consists of not letting problems happen. This is normally accomplished in OT systems by redundancy. Cloud environments can provide a large amount of redundancy, as this is their strength. Making use of a multi-cloud environment using more than one cloud service provider (CSP) in a failover situation may also help to achieve a highly reliable OT architecture.

Resilience means recovering swiftly and smoothly if problems do occur. Improved resilience might be achieved by leveraging some of the features of cloud computing such as geographic diversity. This can prevent a widespread event (hurricane, wildfire, flooding, etc.) from affecting all of your OT resources. Another cloud benefit is elasticity, where resources available to a service can dynamically expand when needed.

Grand Haven, MI – Photo: Lew Folkerth

Security includes assuring availability, integrity and confidentiality. Moving to a cloud environment can improve security in some areas, but can also pose challenges in other areas. The CSP provides security for the physical facilities, servers and networks. Depending on the service model (see background information referenced above), the CSP may also provide security for the operating system and the application software.

Elasticity is a property of cloud computing that permits dynamically expanding the resources available to a process or service. When computationally intense processes are used in real-time or near-real-time environments, these processes may be able to benefit from the effectively unlimited computational resources available in the cloud.

Operational Challenges for OT Cloud Services

In counterbalance to the benefits above, any move of OT services to cloud providers will present significant operational challenges. I've listed some of those challenges below.

Availability is a measure of the "uptime" of a system, usually measured as a percentage. Major CSPs quote various levels of availability depending on services, some levels as high as 99.99% (four nines, or 52 minutes of downtime per year) availability. However, SCADA systems target a higher availability, usually 99.999% (five nines, or five minutes of downtime per year). In addition to

Continued on page 9

Continued from page 8

system availability, network and storage availability will also be critical factors.

Latency is a measure of the delay from data generation to data consumption. Major CSPs use the public Internet for communications, so there is the possibility of delay and dropped communications between the data endpoints.

Mobile access is the ability to easily access cloud services from any device anywhere in the world. While this feature can be a huge benefit for IT systems, it can present serious problems for OT. We do not want anyone, anywhere, to be able to control the breakers in a substation or the feed pump in a steam generator.

Financial challenges include not just the cost of cloud services, but the type of money used. For some utilities, on-premises computer systems are capitalized and can be added to the utility's rate base. Cloud services will use operational dollars.

Cyber security tools and processes will be different in a cloud environment. Entities using cloud services for operational systems will need to train personnel and adapt processes and tools to the new environment.

Compliance Challenges for OT Cloud Services

The use of cloud services will not be possible under the present CIP Standards except in the most limited case, such as some forms of BES Cyber System Information (BCSI) in the cloud. New Reliability Standards will be required, and those Standards will need to be risk-based. There are too many variables in cloud environments to be able to write prescriptive Standards for these cases.

Compliance processes will need to be very mature and integrated with operational processes and procedures. Internal controls will become even more important.

Auditing processes will need to be adapted to cloud environments to determine the type, quality and quantity of evidence that will be needed to provide reasonable assurance of compliance.

Path Forward

To adequately prepare for the adoption of cloud services, I believe we need to develop use cases for this technology. We can then address the operational, security and compliance challenges for each use case. We should begin with known needs, such as cloud-based service providers (such as work management systems) that store BCSI in the cloud. After we take these initial steps, we can evaluate additional use cases.

We will need an environment in which we can test these concepts without incurring compliance risk to the Responsible Entities involved in this forward-looking work. There is precedent for this in the CIP version 5 Transition Advisory Group (v5TAG). The v5TAG provided a forum where transition from the version 3 CIP Standards to version 5 could be tested and modified as needed without incurring compliance risk. I suggest that a Cloud Technology Advisory Group (CTAG) be formed to experiment with and monitor the transition to cloud technologies.

If a CTAG is formed, it should be a partnership with ERO Enterprise staff and a small group of Responsible Entities that are interested in pioneering cloud technologies. Cloud services can be tested, and operational and security issues addressed. Potential revisions or additions to Reliability Standards can be outlined and compliance processes and evidence tested for effectiveness. In this way, cloud transitions can be performed in a small, controlled environment before right-sizing the use of cloud services.

Conclusions

I am not advocating the migration of OT systems and services to the cloud, but I believe some movement in this direction is inevitable.

Reduced cost, the primary driver of early cloud adoption, should not be a significant driver for real-time cloud migration. Rather, the leveraging of cloud technologies for improved reliability, resilience and security should be the drivers, but the associated risks must be effectively managed.

The CIP Standards will need to be modified or new Standards developed to address cloud risks. These Standards will need to be explicitly risk-based to effectively adapt to the wide range of cloud service provider options and features.

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.

The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Finding and fixing trouble spots in your Incident Response Program

In the past few months, RF has observed multiple issues with incident response in both CIP-008-6 (Incident Reporting and Response Planning) and CIP-003-8 Attachment 1 Section 4 (Cyber Security Incident Response). In this article I'll discuss some of the finer points of incident response at both the high/medium and the low impact ratings. I'll designate which impact ratings are applicable with a [H/M/L] at the beginning of each section.

[H/M] Define attempts to compromise

CIP-008-6 R1 Part 1.2.1 requires you to include a definition of "attempts to compromise" in your Cyber Security Incident Response Plan (CSIRP). This definition should provide your incident response team (IRT) with a well-defined set of criteria to determine if an event is an attempt to compromise an applicable system. This should not be a judgment call, but rather a formal set of criteria that is clearly documented and that your IRT can implement during a suspected incident.

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.

[H/M/L] Scope of CSIRP

Each BES Cyber System (BCS) should be covered by one and only one CSIRP. You must be able to demonstrate to CMEP staff which CSIRP applies to a selected BCS. This is not usually an issue if you have only one CSIRP for all your applicable systems, but some entities have a separate CSIRP for field assets such as substations. In this case, there should be a bright line to determine the scope of the substation CSIRP. Does the substation CSIRP include the front-end processors that communicate with the substation RTUs? Or are the front-end processors part of the SCADA CSIRP? You're free to handle a circumstance like this as you choose, but your choice must be clearly documented.

[H/M] Interaction with CIP-007-6 R4 Part 4.1

CIP-007-4 R4 (Security Event Monitoring) requires you to log events for the identification of Cyber Security Incidents. During development and exercise of your CSIRP, you should review the logs available to the IRT. If additional logging is needed, you should address these needs in your CIP-007-6 R4 process.

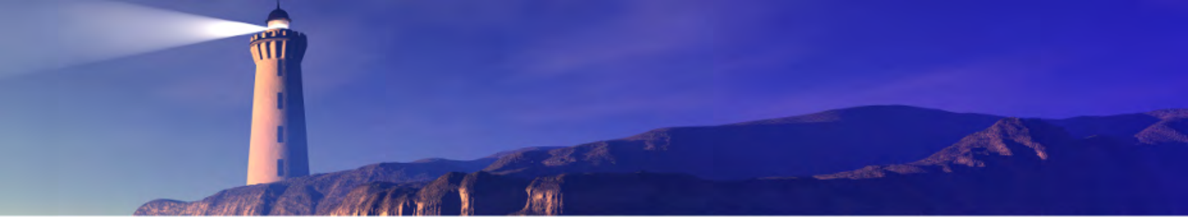
[H/M/L] Ensure the CSIRP addresses operational needs

Some entities use a CSIRP developed for use by their entire organization. Such a comprehensive CSIRP is usually developed by the organization's Information Technology (IT) group. There is nothing inherently wrong with this. You should

Mainstique East Breakwater, MI – Photo: Lew Folkerth

Continued on page 9

The Lighthouse



Continued from page 8

ensure, however, that your CSIRP meets the needs of your Operational Technology (OT) assets. This will require close collaboration between your IT and OT security groups. For any OT incident response, you will need OT representation on the incident response team. As a case in point, I've seen CSIRPs that call for immediate network isolation and/or shutdown of a compromised asset. This may be an issue for a substation relay or a controller in an operating plant. Your CSIRP should address these types of systems in an appropriate manner.

[H/M/L] Use of OE-417 to report a Reportable Cyber Security Incident

If you are submitting an OE-417 to report an issue to the Department of Energy, there are boxes you can check to have the report forwarded to NERC, the E-ISAC, or CISA Central. This may be a valid method to perform the required reporting but be aware that you are still responsible for ensuring that E-ISAC and CISA Central have received the report, and that those organizations have received the report within the time required by the Standards. I recommend directly reporting any Reportable Cyber Security Incident to the E-ISAC and CISA Central. You should record the following for compliance purposes:

- Date and time the determination of a Reportable Cyber Security Incident was made
- A copy of the report sent to each required entity and the date and time the report was submitted
- A copy of the acknowledgement of receipt of each report

[H/M/L] Testing the CSIRP

When testing your CSIRP, be sure that you are testing using a Reportable Cyber Security Incident. Testing the plan using a physical incident or a Cyber Security Incident that is not reportable will not fulfill your compliance obligations in this area. You must choose a scenario that models a compromise or disruption of an applicable BES Cyber System, Electronic Security Perimeter or Electronic Access Control or Monitoring System.

If your CSIRP is part of a larger plan, ensure you test the part of the CSIRP that applies to your CIP systems.

Ensure you test each CSIRP for each Registered Entity. If you are using the same CSIRP for multiple Registered Entities, you must test the plan for each Registered Entity. If you have multiple CSIRPs for a single Registered Entity, you must test each CSIRP. As part of each test, you should ensure that the events logged as required by CIP-007-6 R4 Part 4.1 are sufficient to enable your incident response team to respond to an incident and to make a determination of a Reportable Cyber Security Incident.

RF provides the Incident Response Preparedness Assessment (IPRA) service to enable you to assess your preparedness for an incident. See the Resources section below for a link.

[H/M/L] Participate in development (2022-05)

NERC has established Project 2022-05 to draft revisions to CIP-008-6 to address "Modifications to CIP-008 Reporting Threshold." I recommend that you participate in, or at least monitor, this effort to strengthen the reporting threshold for Cyber Security Incidents. I included low impact as being affected by this because any change to the definitions will affect the low impact requirements as well.

[H/M/L] Resources

Incident Response Preparedness Assessment (IPRA) is an RF service to assist you in assessing your preparedness for an incident.

Cyber Planning for Response and Recovery Study (CYPRES) contains recommendations for incident response and recovery.

Computer Security Incident Handling Guide (NIST SP800-61r2) provides fundamental IT incident handling practices. This is the go-to guide for incident response in the IT community.

Locate training for OT incident handling using this Google search: ICS SCADA incident response training

Top 5 ICS Incident Response Tabletops and How to Run Them explains how to conduct a tabletop incident response exercise for OT assets.

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.