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.