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

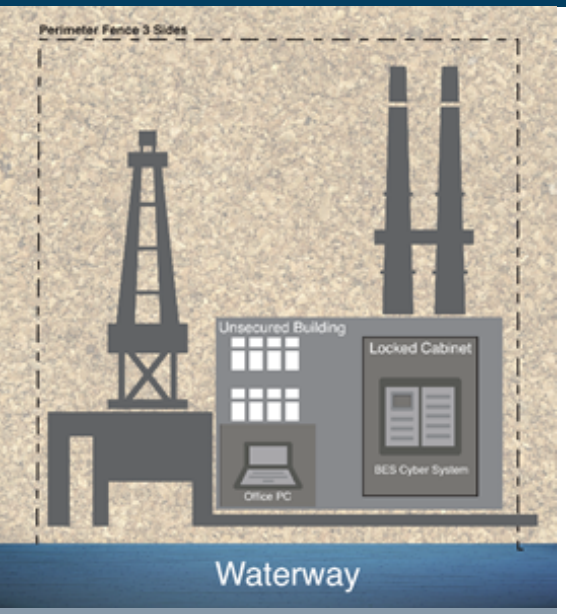

Figure 1 – It is not possible to control power plant access by a perimeter fence due to the waterway. In this case, the building also cannot be secured sufficiently to control access. Physical access to the low impact BES Cyber System is controlled by a locked cabinet. In this case, you must identify 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.