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.