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

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.