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.

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.

Big Bay Lighthouse, MI - Photo: L. Folkerth

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

Continued from page 14

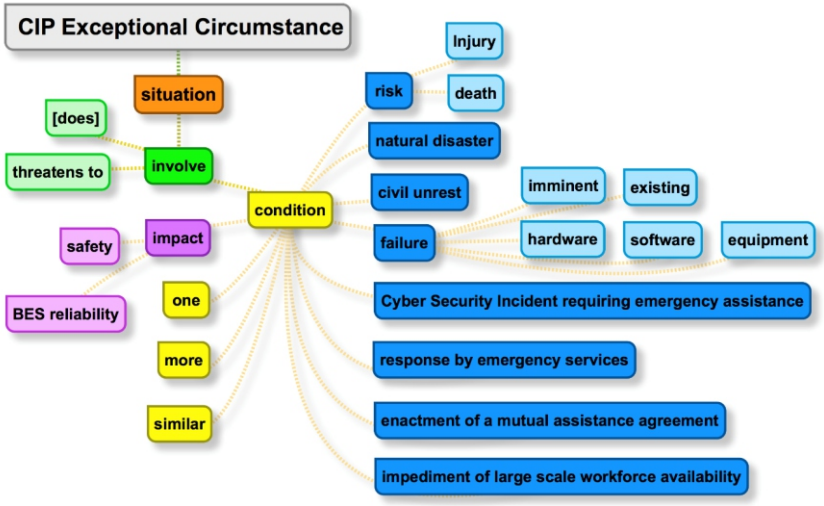

Figure 1 CIP Exceptional Circumstance Definition Analysis

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

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.

Figure 2 CIP Exceptional Circumstance Lifecycle Example A

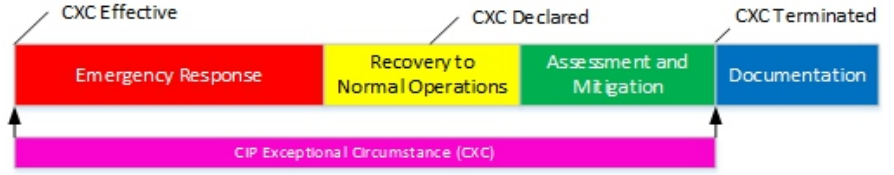

Figure 3 CIP Exceptional Circumstance Lifecycle Example B

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.