The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Supply Chain Risk Management

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: CIP-013-1 will become effective on July 1, 2020. How do I prepare for this date and what will audits of this Standard look like?

A : Preparing for CIP-013-1

CIP-013-1 is the first CIP Standard that requires you to manage risk. Entities and audit teams will both need to make adjustments to prepare for this standard's effective date. I'll give you my present views on this subject as a starting point, and I will provide updates in 2019 and 2020 as the effective date nears and audit approaches are developed.

CIP-013-1 is a *plan-based* Standard.

You are required to develop (R1), implement (R2), and maintain (R3) a plan to manage supply chain cyber security risk. You should already be familiar with the needs of plan-based Standards, as many of the existing CIP Standards are also plan-based.

CIP-013-1 is an *objective-based* Standard.

CIP-013-1, and its affiliated Standards (CIP-005-6 R2 Parts 2.4 and 2.5; and CIP-010-3 R1 Part 1.6), are intended to address four security objectives (see FERC Order 850 at P2, excerpt below):

"[R]equire each affected entity to develop and implement a plan that includes security controls for supply chain management for industrial control system hardware, software, and services associated with bulk electric system operations. [T]he Reliability Standards focus on the following four security objectives:

Portage Upper Entry, MI - Photo by Lew Folkerth

1. software integrity and authenticity;
2. vendor remote access protections;
3. information system planning; and
4. vendor risk management and procurement controls."

Your actions in developing and implementing your plan should be directed toward achieving these four objectives. You should be prepared to demonstrate to an audit team that you meet each of these objectives. These objectives are not explicitly referenced in the Standard language. However, as outlined in the FERC Order, the achievement of these objectives is the reason the Standard was written.

This does not apply just to CIP-013-1. You should write every CIP-related process to achieve the security objective of the Standard, especially when the security objective is stated as clearly as it is for CIP-013-1. Keep in mind that your audit teams are required to consider your program's objectives (see GAGAS 2018 Section 8.36e) when they perform your audit. You will be on much firmer ground during your audit if you can show that your processes achieve the intended objective.

CIP-013-1 is a *risk-based* Standard.

You are required to "develop one or more documented supply chain cyber

Continued on page 11

Continued from page 10

security risk management plan(s)" and to "identify and assess cyber security risk(s)." Your plan should clearly show how you identify and address the risks in your supply chain. As CIP-013-1 is the first explicitly risk-based CIP Standard, this is new ground we'll be exploring.

You are not expected to address all areas of supply chain cyber security. You have the freedom, and the responsibility, to address those areas that pose the greatest risk to your organization and to your high and medium impact BES Cyber Systems.

You will need to be able to show an audit team that you have identified possible supply chain risks to your high and medium impact BES Cyber Systems, assessed those risks, and put processes and controls in place to address those risks that pose the highest risk to the BES. There are several sources to get you started. Approved Implementation Guidance is available on the NERC web site. Also, several National Institute of Standards and Technology (NIST) publications may be useful (see sidebar).

References

- NIST SP800-161, Supply Chain Risk Management Practices
- NIST SP800-30, Guide for Conducting Risk Assessments
- NIST SP800-39, Managing Information Security Risk
- ERO Enterprise-Endorsed Implementation Guidance

One example is NIST SP800-30. This guide discusses a risk management process. It proposes using four components for risk management: *frame* risk (establish a risk context), *assess* risk within the context of the organizational risk frame, *respond* to risk based on the assessment, and *monitor* risk over time. I expect developing a plan by implementing this document and approach would work well for CIP-013-1.

Preparing for an Audit of CIP-013-1

Fundamentally, an audit of CIP-013-1 will probably be similar to audits of other plan-based Standards, but with additional steps.

You will need to have evidence of your documented plan (or multiple plans if you've chosen that option) throughout the audit period.

Be prepared to show how your plan meets the four security objectives. You may accomplish this with a narrative internal to the plan, or by an external compliance narrative in the RSAW.

Be prepared to show how your plan manages risk. Again, a narrative will probably be needed. If you elect to use the NIST SP800-30 risk assessment process, providing detail of how you have implemented the four steps of the risk assessment might be part of this.

You will need evidence of your implementation of the plan. Do not rely on vendor contracts or contract language as evidence. Audit teams will be interested in the tangible results of what you have accomplished and how you've accomplished it, not what you've put in your contract language.

Finally, you will need evidence of your annual (15 calendar months) review of your supply chain cyber security risk management plan. This review should include the identification of any new or emerging risks since the last update of the plan. You should refresh the risk assessments in light of any new risks or changing circumstances in previously-identified risks. You should also review the steps taken to mitigate all identified risks.

Make sure your CIP Senior Manager (or delegate) approves each revision of the supply chain cyber security risk management plan.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any reliability-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

I may be reached here.