By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 1 of 2)

Big Sable Point, MI - Photo by Lew Folkerth

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.

In my November/December 2018 article, I discussed CIP-013-1 at a high level. I discussed how I think CIP-013-1 is at the same time plan-based, objective-based, and risk-based. In my January/February 2019 article I provided a suggested structure for a risk management plan. In this article I'll dive into supply chain risk management Requirements for CIP-013-1 in more detail. I'll cover CIP-005-6 and CIP-010-3 in the next issue. Please remember that what follows are my opinions and my suggestions.

If you choose to adopt any of these suggestions, you must adapt them to your entity's position in the Bulk Electric System, and to your entity's systems and policies.

In the discussion that follows, I will quote only short phrases from the Standards. Please follow along in the actual Standards, available on the NERC web site here. In most cases I will paraphrase the Standards as I understand them. As always, the language of the Standard will govern in any compliance monitoring engagement.

CIP-013-1 Overview

CIP-013-1 is a forward-looking Standard that requires you to modify the way you work with your vendors in any future system, software, or service acquisition. You will have fulfilled the security objectives of CIP-013-1:

- if you integrate vendor and product security considerations into your vendor selection process,
- if your future acquisition contracts work to mitigate the cyber security risks posed by your selected vendor, and
- if you manage the relationship with each of your vendors, present and future, to mitigate risks you identify as applicable to the vendor.

CIP-013-1 applies to your high and medium impact BES Cyber Systems only. I recommend that you also include EACMS associated with high and medium impact BES Cyber Systems, as CIP-013-2 is expected to include these systems in its scope.

CIP-013-1 R1

You are required to develop and document at least one risk management plan. This plan must address the cyber security of your supply chain by implementing processes used in planning for procurement and in procuring systems. I discussed a possible structure for such a risk management plan in my January/February 2019 column. You may choose to create more than one plan for this purpose – for example, you might want to have separate plans for your control centers, transmission substations, and generating plants. Each plan must include the three types of processes specified by Parts 1.1 and 1.2, as discussed below.

Since these processes are part of a risk management plan, you will need to identify the risks applicable to your acquisition, assess those risks, select the risks you will address, and implement, in your purchasing process, remediation for those selected risks. The Standard is silent on exactly which risks you must address, which means you will need to develop this list on your own.

I recommend that your risk management plan include an assessment of the risks listed below, "Cyber Security Supply Chain Risk Consideration: A Starting Point." I intend this list to be used to spark your thinking and for you to build on as you identify additional risks. You should add risk identifications of your own to this list.

Continued on page 9

Continued from page 8

Addressing your identified risks will probably include some additions to the terms of any contract you use for acquiring BES Cyber Systems and systems or services related to BES Cyber Systems.

Two possible sources for acquisition contract language are:

- "Cyber Security Procurement Language for Control Systems," available here; and
- "Cybersecurity Procurement Language for Energy Delivery Systems," available here

The procurement language can be used as a source for possible risks, and for language to address selected risks in contracts. You will need to supplement your selected items with language to address threats that have emerged since these documents were published. For example, you may wish to ensure your vendor complies with US CERT's "SMB Security Best Practices" (here) in order to reduce the risk of ransomware within your ESPs.

Be careful when determining the scope of the risks you are considering. You can easily be distracted by valid risks that are outside the scope of CIP-013-1. CIP-013-1 only requires you to consider risks that can be addressed in planning and procuring systems and services related to BES Cyber Systems. Examples of risks that are outside the scope of CIP-013-1 might include an employee plugging in an unauthorized flash drive, or the risk of a poorly configured relay causing damage to BES components. These are both valid risks, and you should consider them elsewhere in your risk management plans, but they are not related to your supply chain and therefore are not in scope for CIP-013-1.

The processes specified by Parts 1.1 and 1.2 deal with vendor interaction, either in planning for procurement or in the actual procurement of systems. The term "vendor" is unofficially defined (see sidebar) in CIP-013-1. I say unofficially because the definition is not included in the NERC Glossary and is not part of the enforceable language approved by a regulatory authority. While I don't anticipate issues with the supplied definition, I recommend caution in relying on it.

Part 1.1 – Planning for Procuring and Installing

Your supply chain cyber security risk management plan must include a process that will be "used in planning for the procurement" of high and medium impact BES Cyber Systems. The process must address the identification and assessment of cyber security risks to the BES from vendor products or services. The cyber security risks addressed by this process would result from procuring and installing vendor equipment and software, or using services provided by the vendor. In other words, you must have a process that specifies how you will plan future acquisitions of products or services that will become, or will affect, BES Cyber Systems.

Part 1.1 – Planning for Transitions

In addition to the risks resulting from procuring and installing vendor equipment and software, Part 1.1 also requires your supply chain cyber security risk management plan to include a process that addresses cyber security risks resulting from transitions from one vendor to another. In other words, you must have a process that specifies how you will plan your future acquisitions of products or services such that the risks resulting from a vendor transition are minimized.

Part 1.2 – Procuring BES Cyber Systems

Your supply chain cyber security risk management plan must also include a process for procurement of BES Cyber Systems. Note that Part 1.1 requires processes to be used in *planning* for procurement and transitions; Part 1.2 requires a process to be used in actually procuring systems. These will probably be different but related processes.

Part 1.2 contains six sub-parts that specify items you must address in the procurement process. You should also include the additional procurement considerations identified by your Part 1.1 risk assessment.

In this article, I listed the required processes as separate processes, but there is no reason you can't combine processes to suit your needs. Just be sure you can clearly show an audit team that you address all required process types in your supply chain cyber security risk management plan.

CIP-013-1 R2

Any purchase arrangement or contract you enter into on or after the CIP-013-1 effective date of July 1, 2020, must be developed in accordance with your approved supply chain cyber security risk management plan.

For Requirement R2 you must implement all the supply chain cyber security risk management plans developed under R1. Any shortcoming in implementing your processes, and what they say you will do, could be considered a violation. This is different from a prescriptive Standard. For example,

Definition of *vendor*

"The term vendor(s) as used in the standard is limited to those persons, companies, or other organizations with whom the Responsible Entity, or its affiliates, contract with to supply BES Cyber Systems and related services. It does not include other NERC registered entities providing reliability services (e.g., Balancing Authority or Reliability Coordinator services pursuant to NERC Reliability Standards). A vendor, as used in the standard, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators."

--- CIP-013-1 Guidelines and Technical Basis

Continued on page 10

Continued from page 9

if your personnel risk assessment process created by CIP-004-6 Requirement R3 says that you will perform personnel risk assessments every five years, but you miss that target by a year for some personnel, then that should not be a violation as you are still within the timeframe prescribed by the Standard. CIP-013-1 is different in that it is a non-prescriptive, risk-based Standard. You set the compliance rules in R1 by creating the plan and processes you will follow. You are then expected to follow through by implementing these self-generated requirements in R2.

Both contract language and vendor performance to a contract are explicitly taken out of scope for these Requirements by the Note to Requirement R2. I recommend that you do not rely on contract language to demonstrate your implementation of this Requirement. Instead, I suggest the implementation of your processes include documentation that you have followed these processes step-by-step.

This is in line with my recommendations in other articles that you always document your work so you can verify and validate that your processes are executed. For example, the effectiveness of your process for vendor incident notifications might be demonstrated by documenting actual or simulated notifications from the vendor, including your response to such notifications.

CIP-013-1 R3

You are required to obtain CIP Senior Manager (or designated delegate) approval for the supply chain cyber security risk management plan on or before the initial enforcement date of July 1, 2020.

To ensure that your supply chain cyber security risk management plan remains up-to-date, you are required to review it at least every "CIP year," or 15 calendar months. I strongly recommend that you consider reviewing the plan on either a shorter timeframe or have a provision to review the plan based on need (such as an emerging threat or a pending major procurement).

Each review should take into account any additional risks that have emerged since the prior review and should require those newly-identified risks to be added to your existing risks.

The entire assessment and remediation cycle should be performed to include consideration of the new risks. Each review should be documented and each time the plan is revised it should be approved by the CIP Senior Manager (or delegate).

Cyber Security Supply Chain Risk Consideration: A Starting Point

1. Obsolescence of the underlying platform

The expected lifetime of a SCADA, DMS, or other type of control system frequently far exceeds the expected lifetime of its underlying commercial hardware and operating system. How will you manage the risk of your hardware or software becoming unsupported? Will your vendor support a migration to an updated platform at a reasonable cost?

2. State of the art security

Will your vendor enable use of state-of-the-art security enhancements such as application whitelisting or software defined networking? Is the vendor flexible enough to adapt to newer techniques as they emerge?

3. Virtualization

If your vendor supports, or even requires, use of virtual systems, does the vendor support them in ways that are compatible with the currently enforceable CIP Requirements? For example, if the vendor mixes traffic from trusted networks (such as Electronic Security Perimeters) and untrusted networks on the same network hardware, this may put you at risk of a compliance finding.

4. Purchasing counterfeit hardware or software

How will you know that all components of the system you are acquiring are those actually made or approved by the system vendor? This is not usually an issue when a trusted vendor supplies all the components. But if you plan to purchase some components from another source, how will you mitigate the risk of obtaining compromised or substandard equipment?

5. Installing compromised genuine hardware or software

In 2017, the Danish shipping company Maersk installed one copy of compromised software on an internal computer. This software was provided by the original developer, but that developer had been compromised and malicious code placed in an updated package. This resulted in the compromise of nearly every computer within the company and paralyzed its global operations for an extended period of time.

6. Vendor personnel

If vendor personnel are to be granted access to your systems for any reason,

Continued on page 11

Continued from page 10

how will the vendor demonstrate to you that those personnel have been appropriately screened and trained? What controls will the vendor agree to for this purpose?

7. Vendor VPN access

If vendor personnel are to be permitted remote access to your systems via VPN, how will the vendor manage the risk of compromising your systems due to weak security at the originating computer? If the originating computer has been compromised, the malware will have access to your Intermediate Systems and will put them at risk. Similarly, if the originating computer is permitted to talk to both your systems and to other networks (such as the Internet) at the same time, your systems may be exposed to traffic from unexpected sources. This is known as "split tunneling."

8. Vendor system-to-system access

If systems at the vendor's location are permitted direct access to your systems, any compromise or weakness in the vendor's systems will put your systems at risk. How will the vendor manage this risk? How will you know that the vendor is managing this risk?

9. Vendor information management

If your vendor will retain sensitive information about your systems such as, for example, network diagrams or administrative account credentials, how will the vendor protect this information? Will you be notified if this information is compromised?

10. Vendor internal security precautions

If your vendor is providing a service to you, such as a managed security service provider that performs log analysis and alerting, how does the vendor protect its own internal systems? Will you be able to assess the effectiveness of the vendor's protections? Will you be notified of any compromise of the vendor's systems?

11. Vendor termination process

When you discontinue your relationship with a vendor, will this transition proceed in an orderly, defined manner? What happens to any sensitive information in the vendor's possession?

12. Adaptability to new risks

When ransomware appeared as a threat in early 2018, many entities were forced to make rapid changes to their network environments. Will your vendor support rapid response to emerging threats?

13. Vendor acquisition or dissolution

If your vendor goes out of business or is acquired by a different company, how will you support your system? Will you have access to the source code? Will licenses expire?

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.

In addition, if you would like RF Entity Development staff to review your supply chain cyber security risk management plan and provide you with feedback, you can request this through the Assist Visit link above. Be aware that RF will not make compliance determinations in advance of an audit, but can only raise concerns and indicate areas for improvement.

Feedback

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

I may be reached here.