By: Lew Folkerth, Principal Reliability Consultant

CIP Supply Chain Cyber Security Requirements in Depth (Part 3 of 3)

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 Jan/Feb 2019 article I provided a suggested structure for a risk management plan. This article completes my series on the in-depth study of the supply chain cyber security risk management Requirements that was begun in the Mar/Apr and May/Jun 2019 issues. I'll also answer some questions that have been presented to me and to the ERO Enterprise. 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.

CIP-010-3 R1 Part 1.6

In Order 829 at P 48-50, FERC required NERC to develop a Reliability Standard to address the verification of both the identity of the software publisher and the integrity of all software and patches for BES Cyber Systems. FERC stated that the objective of these changes is to reduce the likelihood of the installation of compromised software on a BES Cyber System.

In response to Order 829 P 48-50, one new part has been added to CIP-010-3. You are required to perform software verification by verifying the integrity of both the software source and the software itself. Here's the enforceable language of Part 1.6:

R2: Each Responsible Entity shall implement one or more documented process(es) that collectively include:

Port Sanilac, MI - Photo by Lew Folkerth

Applicable Systems	Requirements
High Impact BES Cyber Systems: and Medium Impact BES Cyber Systems Note: Implementation does not High Impact BES Cyber Systems; and require the Responsible Entity to renegotiate or abrogate existing contracts (including amendments to master agreements and purchase orders). Additionally, the following issues are beyond the scope of Part 1.6: (1) the actual terms and conditions of a procurement contract; and (2) vendor performance and adherence to a contract.	Part 1.6: Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.

Continued on page 11

Continued from page 10

Supply Chain Questions

The ERO has begun receiving requests for guidance regarding the application of the supply chain Standards, especially CIP-013-1. Here are the questions I've seen so far, and my answers to them.

Q: How many levels (tiers) of vendors must an entity consider for CIP-013-1 Compliance?

A: The responsibility for determining how deep into the vendor supply chain to delve lies with you, the Responsible Entity, through your supply chain cyber security risk management plan.

CIP-013-1 is silent on how deep into the vendor supply chain you must go. My recommendation is that you should know as much about your equipment, software, and services as possible. I suggest that you document as much as you can about your BES Cyber Systems and their makeup, using your CIP-010 baselines and expanding on each baseline with as much detail as you can gather. From this information you can compose a list of hardware, software, and services that are used in your systems.

You can then assess your hardware, software, and service list based on risk. For example, you would probably assess the cyber security risk of a server power supply as very low. You would probably assess the cyber security risk of a network-connected out-of-band server management device as high or severe.

You should then be able to create a list of vendors of your devices, software, and services, and prioritize that list based on the assessed risk of each component a vendor supplies.

Q: If I buy routers at Office Depot, does that constitute a "contract" or is that just a procurement?

A: Any equipment, software, or services whose acquisition is begun on or after July 1, 2020, that will become or will be directly related to a high or medium impact BES Cyber System must be acquired in accordance with your supply chain cyber security risk management plan. The plan must be used whether or not a contract is involved. The only place in the enforceable language of CIP-013-1 where the term "contract" appears is in the note to Requirement R2. Risks incurred by acquisitions from vendors such as Walmart (yes, they do carry business-grade Cisco products) or sellers of new and used equipment on eBay are some of the risks this Standard is intended to mitigate. In particular, there could be an elevated risk of compromised or counterfeit hardware from such sources.

The term "contract" also appears in the definition of "vendor" in the Rationale section of the Standard, but that definition does not appear in the enforceable elements of the Standard. The definition may be useful as guidance, but be cautious about relying on the exact wording. For example, the use of "contract" in the definition appears to restrict the application of CIP-013-1 to only those parties with which the Responsible Entity has a formal contract. This restriction is not supported by the enforceable elements of the Standard, which means you cannot rely on that aspect of the definition.

Q: Will a Responsible Entity be expected to perform and document initial cyber security risk assessments on all its existing vendors that provide their BES Cyber System products and services prior to the compliance effective date?

A: No, CIP-013-1 affects only new procurements. This answer is supported by the General Considerations section of the Implementation Plan:

"In implementing CIP-013-1, responsible entities are expected to use their Supply Chain Cyber Security Risk Management Plans in procurement processes (e.g., Request for Proposal, requests to entities negotiating on behalf of the responsible entity in the case of cooperative purchase agreements, master agreements that the responsible entity negotiates after the effective date, or

CORRECTION

In my Mar/Apr 2019 article I said, "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." This is incorrect. It should read, "Any procurement begun on or after the CIP-013-1 effective date of July 1, 2020, must be performed in accordance with your approved supply chain cyber security risk management plan."

Enforceable Elements of a Standard

From the NERC Standard Processes Manual Section 2.5, "The only mandatory and enforceable components of a Reliability Standard are the: (1) applicability, (2) Requirements, and the (3) effective dates. The additional components are included in the Reliability Standard for informational purposes and to provide guidance to Functional Entities concerning how compliance will be assessed by the Compliance Enforcement Authority."

In addition, Glossary terms and Implementation Plans may be separately approved as mandatory and enforceable.

Continued on page 12

Continued from page 11

direct procurements covered under the responsible entity's plan) that begin on or after the effective date of CIP-013-1. Contract effective date, commencement date, or other activation dates specified in a contract do not determine whether the procurement action is within scope of CIP-013-1."

In order to determine the begin date of a procurement, you must document that date in a manner suitable for use as audit evidence. Without such documentation, audit teams will use the earliest date that provides reasonable assurance of the beginning of the procurement process.

Q: If I procured hardware or software from a vendor prior to 7/1/2020, but installed that hardware or software after that date, must I perform a risk assessment of that vendor?

A: Risk assessments of vendors that provided equipment, software, or services prior to the CIP-013-1 effective date of July 1, 2020, are not required. Any procurements for high or medium impact BES Cyber Systems equipment, software, or services begun after July 1, 2020, must be performed in accordance with your documented CIP-013-1 R1 supply chain cyber security risk management plan. Any software installed on or after July 1, 2020, must have its identity and integrity verified, regardless of when the software was obtained.

Q: Contracts for procurement that are in place prior to July 1, 2020, are not in scope for CIP-013. What about contract renewals?

A: CIP-013-1 applies to any procurements begun after July 1, 2020, regardless of the existence of a standing contract, and regardless of any revisions to such a contract. You are not required to invalidate or renegotiate any contract, but you must demonstrate that any procurement begun after July 1, 2020, has been performed in accordance with your supply chain cyber security risk management plan. You will need to establish a beginning date for the procurement. The effective date of a contract is not necessarily the beginning of a procurement. The beginning date might be the date of an expenditure authorization or a request for bid, quote, etc. You will then need to show how you followed your risk management plan throughout the acquisition.

Q: My source for equipment says that they are not a "vendor," but rather a "supplier," and so they are not subject to CIP-013-1. How do I answer this?

A: Any organization or person that supplies equipment, software, or services to your entity must be considered a "vendor" in the meaning of CIP-013-1. Your "supplier" is quite correct to say that they are not subject to CIP-013. Only NERC Registered Entities that are procuring hardware, software, or services that will become or that will directly affect high or medium impact BES Cyber Systems are subject to CIP-013-1. It is your relationship with each vendor, supplier, etc. that is subject to CIP-013-1, not the vendor itself. In managing that relationship you may use many tools, including purchase or acquisition contracts, existing vendor practices such as incident notification, existing or emerging security practices, such as software verification, vendor web site features such as digital certificates and digital signatures, and so forth. Although you may choose to manage your vendors through contracts, CIP-013-1 does not explicitly require this. If your vendor will provide a feature or a service as part of its ongoing security practices, there may be no requirement for a contract for such matters. And you may show that the implementation of your risk management plan accomplishes its goal of reducing supply chain risk by means other than contracts.

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.

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.