
NERC CIP-013-1
Supply Chain Risk Management for the Electric Sector
ARCHER
Patrick C Miller and Steve Reed | Webinar | 29 May 2019

About Archer

Archer is a critical infrastructure protection services firm providing the highest grade security, compliance and operational consultants in the business. Our specialists are individually selected for their diverse skill sets, deep knowledge of their industry and respective regulations as well as their productivity, professionalism and integrity.

Our roots go back to 2001, when our founding partners crossed paths at a large electric utility in the Pacific Northwest. At that time, cybersecurity was new to many in the energy sector and operational technology resilience was becoming more important than ever. Security and resilience were receiving increased attention from executive management, government officials, and other interested parties.

Critical infrastructure and industrial security has matured greatly since then. Today Archer delivers unrivaled strategic and tactical advice in, but not limited to, cyber security, physical security, regulatory compliance, government affairs, witness preparation, disaster recovery, continuity of operations, emergency management, information technology, industrial controls systems, and training.

Archer's headquarters are in Portland, Oregon and our Canadian branch is based in Vancouver, BC. We have global reach through business partnerships in Europe and South America.

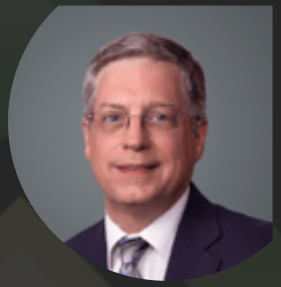
Find out more at https://archerint.com/

@patrickcmiller

Patrick Miller

Managing Partner, Archer

- Former electric utility security staff for multiple organizations
- Former NERC CIP Standards/Interpretations Drafting Team member
- Former WECC Regional CIP Manager of Audits and Investigations
- Founder, President Emeritus and Director of EnergySec
- US Coordinator for International Industrial Cybersecurity Center (CCI)



Steve Reed

Senior Consultant, Archer

- Over 30-year CIA career as an Information Security and Communications Officer
- Former security engineer for U.S. Army's Distributed Common Ground System (DCGS-A)
- Provides security assessments and penetration testing for a variety of clientele with a heavy focus on NERC CIP
- Certified Ethical Hacker
- Certified Penetration Tester

@tnvolsfan29

Steven Briggs

Senior Program Manager I&C Systems Generation Cybersecurity, Tennessee Valley Authority

- Member on the NERC CIPC Supply Chain Working Group & Control System Security Working Group
- Information System Security Officer for TVA's Coal, Gas, and Hydro Cybersecurity and Compliance
- Working with Agency Working Group to develop internal policy and compliance controls for CIP-013

Why Do We Need It?

- Supply chain has always been a known weakness
- History of adversary use of supply chain vulnerabilities
  - Warfare
  - Nation-State Espionage
  - Industrial Espionage/Sabotage
- What if bad things are embedded in the power system?
- Growing mandate in most government agencies/sectors
- Becoming standard risk management practice, time for the electric sector to catch up; FERC Order 850

Who, What and When…

- NERC Registered Entities (with CIP applicability)
- Functions: BA, DP, GO, GOP, RC, TOP, TO
  - Some qualifiers for DP function, all BES Facilities for others
- Applicable: Only high and medium impact BES Cyber Systems
  - No low impact - yet
  - No PACS, EACMS or PCAs - yet
  - No ERC exclusion – also see GoT definition
- Effective July 1, 2020
- Not required to renegotiate or abrogate existing contracts

Standard Overview

- R1: Plans and processes for:
  - Assessing pre-procurement cybersecurity risk
  - Notification by the vendor of vendor-identified incidents
  - Coordination of responses to vendor-identified incidents
  - Notification by vendors when remote/onsite access should disabled
  - Disclosure by vendors of known vulnerabilities
  - Verification of software integrity and authenticity
  - Coordination vendor interactive & system-to-system remote access
- R2: Implementation of the plan
- R3: Senior Management Approval of plan 15 calendar months

General Impacts

- NERC [FERC] wants to mandate supply chain cybersecurity but has no jurisdiction on supply chain vendors
- CIP-013 regulates vendors by proxy, through the utilities, putting the compliance risk on the Registered Entity
- Intended to create a dialog about security between both parties
- May lead to standardization on what utilities can/can't buy
- May change cybersecurity practices from vendors
- Comes with administrative overhead and cost for everyone

Utility Impacts

- May need to establish new contract language and procedures for hardware, software, firmware *and services*
- Incident response process(es): notification, coordination
- Process for vendor physical access revocation notification/action
- Assess vendor products and their ability to support
- Respond to vendor-issued vulnerability notices
- Change updating/patching/installation process(es)
- Controls on vendor-initiated remote/system-to-system access
- Yes, costs will go up, both direct and indirect

Field Implementation Observations

- Internal relationships are usually challenged and stretched
- Voluntelling, Teflon, finger-pointing and selective memory
- Reinforce senior management buy-in to keep on track
- Draw out your processes (process flow diagrams) to fully understand the mechanics
- Hunt for gaps and needed controls
- What does evidence look like for an audit?
- Who will be your SME for the audit?

Vendor Impacts

- Customers may be seeking new contract language, T&Cs
- Incident response process(es): notification, coordination
- Access notification and action
- Secure development lifecycle and internal security practice
- Responsible/coordinated vulnerability notices and release
- Verification of software integrity and authenticity
- Controls on vendor-initiated remote access
- To sell to the sector, you must be this tall to ride the ride
- Costs will go up both direct and indirect

Compliance and Market Maturity

- Some utilities/vendors/auditors are more advanced than others
- Expect some interesting behavior from everyone
- The more complex the software or hardware is, the more cumbersome the change/growth process
- The more complex and large the utility, the more cumbersome the change/growth process
- Both sides (utility & vendor) have responsibility and risk
- Collaborative posture and openness are best for everyone
- Not everything can fit your mold; be flexible

Getting Started - Utilities

- If you are totally lost, start with the ERO approved Implementation Guide
- Engage all potentially impacted business units and walk through requirements with to understand full scope
- Review supply chain frameworks, learn lexicon so everyone can understand each other, intended goals and outcomes
  - Some existing options exist, e.g. NIST SP-800-161, IEC 62443
  - Don't worry about picking the wrong one, they're all "Legos"
- Prepare and issue questionnaires for vendors – be sensible, normalize, standardize, you are not a snowflake
- Brace management for cost increases

Gaining Traction – Utilities

- Start with a list of all BCAs and associated software and firmware inventories (from baselines required in CIP-010)
- Build a list of all vendors, for hardware, software and services for your BES Cyber Assets/Systems
- Determine contract/source for each:
  - Hardware
  - Software
  - Firmware
- Review contracts for each vendor
  - Contract renewal date; how close is it to 7/1/2020 deadline?
  - Understand your change timelines, renewals; build tracker/notifications
  - Terms and conditions
  - Look for conflicting clauses, insert new language
  - May need to involve legal

Building Momentum - Utilities

- Add time to operational efforts, projects
  - Purchases, to allow for new discussions
  - Implementation, to allow for software validation before patching/updates
  - Incident response, when vendor notifies you of an issue
- Establish software validation methods
- Prioritize all process development work for R1.2
- Engage staff to draft plan and associated processes:
  - Procurement
  - Legal
  - Operations
  - IT

Pitfalls - Utilities

- "We're only going to do something when a contract is up for renewal…"
- What if there is no vendor?
  - eBay, Amazon, VAR/reseller, clearinghouse, contractor/subcontractor
- Do nothing isn't an option
  - What does diligence look like?
- Don't forget about the companion standards CIP-005-6 and CIP-010-3
- Implement early (at least 1Q) to test your program and controls

Recommendations For Vendors

- Review the new standard, understand it, don't hide from it
- Review and understand common framework/lexicon so both sides can understand each other, intended goals and outcomes
- Prepare answers against known frameworks, let your utilities know which one you chose
- Stand up an internal CERT, with all associated processes
- Establish method for communicating personnel access changes
- Establish software validation and publication methods
- Minimize remote/system access needs and choose secure options
- Seek outside assistance in validating your understanding
- Be open to discussion with customers
- Brace management for cost increases

Regulatory Machinery in Motion

- Order 850 directives
  - Inclusion of EACMS
  - Study certain categories of assets not currently subject to the Supply Chain Standards
- NERC issued report: Cyber Security Supply Chain Risks Staff Report and Recommended Actions May 17, 2019 recommends the following for H/M impact
  - Include EAMCS excluding monitoring and logging
  - PACSs that provide physical access control (excluding alarming and logging)
  - Conduct further study inclusion of low impact BES Cyber Systems with ERC by **issuing a Request for Data or Information pursuant to Section 1600**
  - Guideline to assist entities with evaluating PCAs on a case-by-case basis
- If you have H/M impact, go ahead and apply it to L (it's coming)
- If you only have L impact, it's coming your way too
- NERC reports to FERC who reports to multiple paths upstream

The Road Ahead for Everyone

- This issue is not going away and will not decrease; get on board
- Get started yesterday; it will take all of the implementation window to meet the compliance deadline
- Work together on the questionnaire/responses as well as the terms & conditions; find common ground
- Review existing processes for hooks, snags and contingencies
- Look for process improvement opportunities; include automation and controls
- Set expectations on cost and time impacts

The Road Ahead for Everyone

- Utilities are held to account but both parties have skin in the game
- Have some sympathy for each other, this is new to everyone
- Work together instead of against each other, you're in the same boat
- Get executive sponsorship for this initiative, and get in early so you can drive through changes sooner than later; expect the unexpected
- Read existing supply chain security frameworks out there; know the common lexicon so you can have meaningful conversations
- If it's too confusing, difficult or if you hit a stale-mate ask for help from a third party
- This will be new to your auditors as well; Regions may differ in approach for a while

CIP-013 Resources

CIP-013 Resources

- ERO Enterprise-Endorsed Implementation Guidance
  - CIP-013-1-R1-R2-R3 Implementation Guidance
- Proposed Implementation Guidance
  - CIP-013-1 R1 R2 Supply Chain Management (NATF)
- Various draft and non-ERO-endorsed guidance
  - All Regions have given workshops, webinars and guidance
  - EEI – [Draft] Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk
  - Lew Folkerth, Tom Alrich and various pundits
- **Depending on your utility, your mileage may vary**

Supply Chain Security Frameworks

- IEC-62443
- BSI: BS ISO 28000:2007
- NIST CSF; SP800-161; CREATe
- WCO SAFE
- DHS ICS-CERT, National Strategy
- SANS

Archer Services

- Assessments, mock audits and program development
- CIP, ICE/IRA, ES-C2M2, NIST CSF
- Live audit and settlement support
- Asset Inventory for plants and substations
- Internal controls design and testing
- Incident response and recovery exercises
- Security technology architecture and integration
- Supply chain security, ICS lab testing
- Cybersecurity training and awareness programs
- Physical security assessments
- Project management
- Executive/Board security briefing

Question 1

By access do you mean interactive remote access and system to system access? What about access to BCSI?

- CIP-013 1.2.6 has considerations for both interactive remote access and system to system remote access, but BCSI is not specifically mentioned.
- For the NERC CIP Medium and High asset-related BCSI, the company should have an established CIP-011 protection plan for BCSI. The requirements should already be included in contracts to ensure appropriate information protection with your vendors.

Question 2

As a vendor, are we to impose the cyber requirements from the customer down to, say, Microsoft? Oracle?

- Vendors aren't bound to the standard, but they are tied to their customers - who are bound to it. The upstream supply chain for the vendor gets very complicated. At a minimum, cover your own software/hardware/firmware - but where you're using outside components, diligence around that security will be key. For example, are you updating any embedded open source or other commercial components when they are updated?
- Supporting information on third party components and applications that are patched or supported independently of your product should be understood by the customer. The patch source locations and verification methods would be beneficial to supply as part of the requested CIP-013 information. For third party components such as open source code or other elements that are controlled by updates/patches to your product are the vendors responsibility to account for and should be understood by the customer. As known vulnerabilities in these third party products are identified and disclosed there should be an understanding of your product lifecycle on the impact and expectation to receive patches that incorporate remediation's to third party vulnerabilities. The CIPC working group is working on supporting guidance around product provenance and integrity verification that should help provide some considerations and best practices on how to handle these situations.

Question 3

Discuss relationship between CIP13 R1.2.4 and CIP 10 Vulnerability Assessments

- In the High CIP space the entity already is doing the implementation assessment. This should support your CIP-013 process and be one of the elements used to identify, account for, and mitigate risk of assets/applications brought into your CIP environment. For other assets/applications that are brought into your entities CIP space this process could be used to account for risk that are outside of the contract space. These assessments need to be tailored to the risk level the product poses and in line with your entities established risk tolerance level that is documented in your CIP-013 plan.

Question 4

How should utilities handle vendors who won't "play" (i.e. incomplete or unanswered risk questionnaires, or non-agreement of T&C)? In some cases, the field of vendors and service providers is relatively small.

- Derive a process. Don't make the request too cumbersome for the vendor, and create limited questions. You're still responsible for internal mitigation.
- In CIP-013 R2 Note the entity is not responsible for the vendors adherence to the contract. As long as the entity is accounting for the process they went through with the vendor to apply the CIP-013 risk plan and account for the controls then by everything known today that should be sufficient. The entity is still responsible for their BES Cyber Systems security and their impacts to the BES. If the vendor can't/won't supply mitigations or controls then the entity may need to implement their own controls. Lack of responses should also be reflected in the evaluation of risk if you are competing vendors. The entity also wants to make sure that they are asking questions of the vendor that they are actually going to use to meet compliance or determine effectiveness of security controls. The CIPC working group is working on supporting guidance around supply chain lifecycle to support these questions.

Question 5

Aren't the T&Cs of the contracts beyond the scope of the standard?

- Completed contracts are, the standard terms and conditions that you can use to meet CIP-013 requirements are not and I would plan to use this as a key piece of evidence

Question 6

You made reference to insurance. Most GL or E&O does not cover 1st and 3rd party damages...thoughts on requiring cyber insurance as a formal requirement in SLAs and other legally binding agreements?

- I wouldn't go there yet. It's still a bit in question.
- I am not sure how this would help to support CIP-013 compliance. I would not look at making this a requirement unless it is an already established practice at your entity, where the increase in cost and complexity of the contract negotiations are known or expected.

Question 7

In the greater DC area, NIST hosts the software assurance and cyber suppl chain forum hosted by MITRE. Great session for understanding concepts that are already adopted by Gov Contractors to DOD and DHS.

- This is a great group. DHS and other government entities are working on similar efforts for government supply chain security. There were a number of their resources listed in the slides, and on the NERC Supply chain page.

Question 8

Would you still go thru Amazon or other 3rd parties to purchase items once CIP-013 goes into effect? Seems like part of this purpose is to assess the vendor and so this may be tricky when trying to stay compliant.

- Short answer is “not unless you don’t have better option.” The risk still falls on you, if you don’t use an appropriate vendor.
- Sometimes there are no other choices when you are dealing with legacy equipment that the vendor no longer provides, but to go to Ebay. These should be one off cases, but something that needs to be accounted for in the plan. You will have to work with 3rd parties with some vendors that do not directly sell to consumers.
- If you are not using a direct contract for the product/service that you are brining into your BES environment then the CIP-013 responsibilities fall to the entity to account for. In the entities plan these should have associated risk scores and process control steps to prevent non-evaluated equipment from entering into your BES space that has not been validated and associated requirements accounted for.

Question 9

If your procurement process has to go through company approved resellers, should a utility develop "best effort" processes specific to the vendors to address applicable requirements. i.e. monitor feeds and/or correspondence for vulnerabilities that can feed your internal VA/IR programs, vendor language regarding their Supply Chain and QA methodologies, etc.?

- You definitely need some awareness of threats and incidents to feed your programs. I would include anything that supports CIP-013 as part of the plan.
- Additionally CIP-013 R1.1 instills the responsibility on the entity to ensure the plan remains effective over the life of the product/service that is procured. This can be done by simple communication with the vendor contract representatives to update the entity on any planned for or executed changes with the support model of the product/service. This is standard practice amongst several vendors to publish information on transition to new companies, updates to product support, or end of life of support. As part of the 15 month review by the CIP senior manager this can be an element that is included in that report or documentation to account for the completed/approved review of the risk plan.