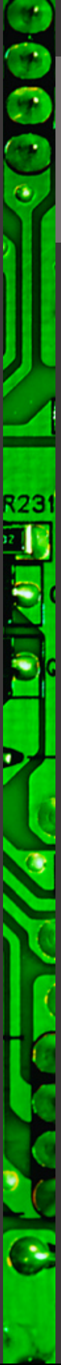
Are You Ready for the NERC CIP Supply Chain Standards?

InfraGard Power & Utilities Cross Sector Council – July 13 2020



YOUR GUIDE: PATRICK C MILLER

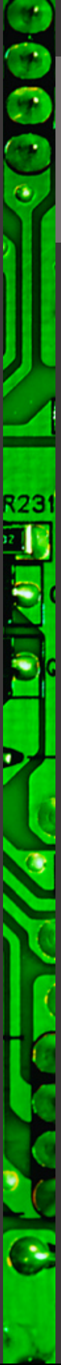
- Former utility staff (multiple utilities, telecommunications, water & energy)
- First NERC CIP auditor in the US
- Former WECC Manager of NERC CIP Compliance Audits & Investigations
- Drafter of sections of NERC UAS 1200, NERC CIP versions 1/2/3, and several CIP Interpretations, NERC SCWG contributor
- EnergySec Founder, Director and President Emeritus
- Former National Electric Sector Cybersecurity Organization Principal Investigator, US DOE
- Advisor to multiple industrial security product vendors
- Centro de Ciberseguridad Industrial (CCI) US Coordinator
- Managing Partner, Archer International
- GCIP, CISA, CRISC, CISSP, ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

WHY DO WE NEED CIP-013?

- 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 & 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 Glossary of Terms definition
- Was effective July 1, 2020; extended to October 1, 2020 due to COVID19
- Not required to renegotiate or abrogate existing contracts



STANDARD OVERVIEW

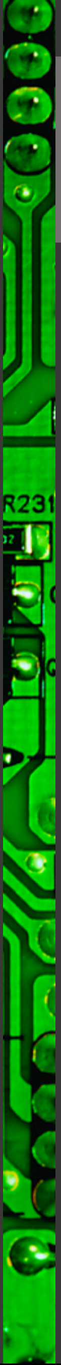
- R1: Plans and processes for:
  - Assessing pre-procurement cybersecurity risk
  - Notification by the vendor of vendor-identified incidents
  - Coordination of responses to vendor-identified incidents
  - Notification by vendors when remote/onsite access should be disabled
  - Disclosure by vendors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

GENERAL IMPACTS

- NERC [FERC] wants to mandate supply chain cybersecurity but has no jurisdiction over vendors
- CIP-013 regulates vendors by proxy, through the utilities, putting the compliance risk on the Registered Entity (utility)
- 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
- May or may not align with current procurement practices
- 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
- Expect direct and indirect costs to increase



STORIES FROM THE FIELD

- 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?
- How far down the rabbit hole to do you go?

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 into the sector, you must be this tall to ride the ride
- Expect direct and indirect costs to increase

COMPLIANCE & 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/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

- If you are totally lost, start with the ERO approved Implementation Guide
- Engage all potentially impacted business units and walk through requirements to understand full scope
- Review supply chain frameworks, learn lexicon so everyone can understand each other, intended goals and outcomes
    - Start anywhere, DNI NCSC SCRM, 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
- Set management expectations for cost increases

GAINING TRACTION

- 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 10/1/2020 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

- 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

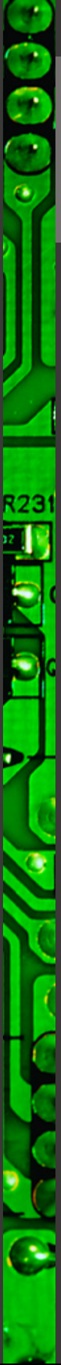
- Wait and see…
- "We're only going to do something when a contract is up for renewal…"
- What if there is no vendor?
  - eBay, Amazon, VAR/reseller, clearinghouse, contractor/subcontractor
- Do nothing isn't an option; some diligence is expected
- You will not be able to transfer all risk to the vendor
- 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 CIP standard, prepare internal SCRM team for responses
- Review and understand common framework/lexicon so both sides can understand each other, intended goals and outcomes
- Prepare answers against known SCRM 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

SCRM REGULATORY BIG PICTURE

- 10/18/18: FERC Order 850 directives
- 2/17/19: Senate Energy and Natural Resources Hearing; NERC CEO testifies
- 5/15/19: Executive Order 13873 – Securing the Information and Communications Technology and Services Supply Chain
- 5/17/19: NERC Report – Cyber Security Supply Chain Risks Staff Report and Recommended Actions
- 7/2/19: NERC Section 1600 Data Request
- 7/17/20: NERC Alert on EO 13873
- 5/1/20: Executive Order 13920 - Securing the United States Bulk-Power System
- 6/18/20 FERC Cybersecurity Incentives Policy White Paper
- 6/18/20 FERC NOI on Potential Enhancements to the CIP Standards
- 6/22/20: CIP-005-7, CIP-010-4, CIP-013-2 fail ballot (again)
- 7/8/20: NERC Alert on EO 13920
- 7/8/20: DOE RFI on Bulk-Power System Executive Order (13920)



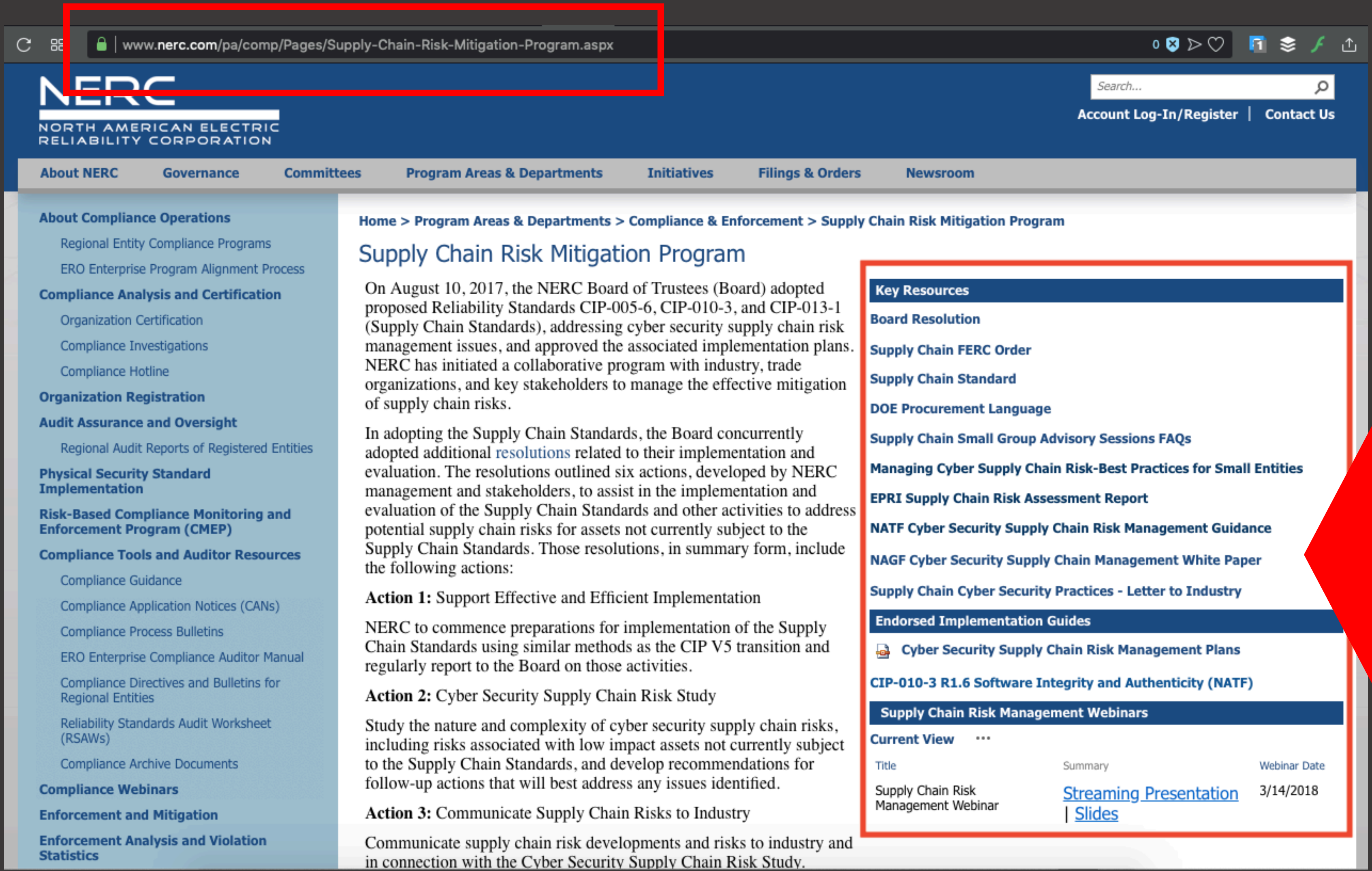
THE ROAD AHEAD FOR CIP-013

- The issue is not going away, will get more prescriptive
- Get started yesterday, it will take more time than you think
- Work together with the community on the questionnaire(s), responses, and terms & conditions; find common ground
- Expect CIP-013 to shift to low impact and more equipment
- Review existing processes for hooks, snags and contingencies
- Look for process improvement opportunities; include automation and controls
- This will be new to your auditors as well; Regions may differ in approach for a while
- Set expectations on cost and time impacts

THE ROAD AHEAD FOR SCRM

- Utilities are held to account, but vendors still have proxy risk
- Have some sympathy for each other, this is new to everyone
- Get executive sponsorship ASAP
- Review existing supply chain security frameworks; know the common lexicon so you can have meaningful conversations
- Be prepared to perform multiple asset reviews for overseers
- FERC vs. DOE regulatory authority
- Possible [future] alignment on a single approach/framework
- More Executive Orders are possible

CIP-013 RESOURCES



www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Search...

Account Log-In/Register | Contact Us

About NERC | Governance | Committees | Program Areas & Departments | Initiatives | Filings & Orders | Newsroom

- About Compliance Operations
  - Regional Entity Compliance Programs
  - ERO Enterprise Program Alignment Process
- Compliance Analysis and Certification
  - Organization Certification
  - Compliance Investigations
  - Compliance Hotline
- Organization Registration
- Audit Assurance and Oversight
  - Regional Audit Reports of Registered Entities
- Physical Security Standard Implementation
- Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
- Compliance Tools and Auditor Resources
  - Compliance Guidance
  - Compliance Application Notices (CANs)
  - Compliance Process Bulletins
  - ERO Enterprise Compliance Auditor Manual
  - Compliance Directives and Bulletins for Regional Entities
  - Reliability Standards Audit Worksheet (RSAWs)
  - Compliance Archive Documents
- Compliance Webinars
- Enforcement and Mitigation
- Enforcement Analysis and Violation Statistics

Home > Program Areas & Departments > Compliance & Enforcement > Supply Chain Risk Mitigation Program

Supply Chain Risk Mitigation Program

On August 10, 2017, the NERC Board of Trustees (Board) adopted proposed Reliability Standards CIP-005-6, CIP-010-3, and CIP-013-1 (Supply Chain Standards), addressing cyber security supply chain risk management issues, and approved the associated implementation plans. NERC has initiated a collaborative program with industry, trade organizations, and key stakeholders to manage the effective mitigation of supply chain risks.

In adopting the Supply Chain Standards, the Board concurrently adopted additional resolutions related to their implementation and evaluation. The resolutions outlined six actions, developed by NERC management and stakeholders, to assist in the implementation and evaluation of the Supply Chain Standards and other activities to address potential supply chain risks for assets not currently subject to the Supply Chain Standards. Those resolutions, in summary form, include the following actions:

Action 1: Support Effective and Efficient Implementation

NERC to commence preparations for implementation of the Supply Chain Standards using similar methods as the CIP V5 transition and regularly report to the Board on those activities.

Action 2: Cyber Security Supply Chain Risk Study

Study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards, and develop recommendations for follow-up actions that will best address any issues identified.

Action 3: Communicate Supply Chain Risks to Industry

Communicate supply chain risk developments and risks to industry and in connection with the Cyber Security Supply Chain Risk Study.

Key Resources

- Board Resolution
- Supply Chain FERC Order
- Supply Chain Standard
- DOE Procurement Language
- Supply Chain Small Group Advisory Sessions FAQs
- Managing Cyber Supply Chain Risk-Best Practices for Small Entities
- EPRI Supply Chain Risk Assessment Report
- NATF Cyber Security Supply Chain Risk Management Guidance
- NAGF Cyber Security Supply Chain Management White Paper
- Supply Chain Cyber Security Practices - Letter to Industry

Endorsed Implementation Guides

- Cyber Security Supply Chain Risk Management Plans
- CIP-010-3 R1.6 Software Integrity and Authenticity (NATF)

Supply Chain Risk Management Webinars

Current View ···

Title	Summary	Webinar Date
Supply Chain Risk Management Webinar	Streaming Presentation | Slides	3/14/2018

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

- DNI NCSC SCRM
- NIST CSF; SP800-161; CREATe
- IEC-62443
- BSI: BS ISO 28000:2007
- WCO SAFE
- SANS

ARCHER SERVICES

- Assessments, mock audits, program development
- NERC CIP, ES-C2M2, NIST CSF, IEC 62443
- Pre/during/post audit, mitigation, settlement
- 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

p.miller@archerint.com
@patrickcmiller
503.272.1414