2019 | THE ACADEMY

Legal & Regulatory Conference

PARTNER SPONSOR

GRIDLIANCE

NERC CIP-013-1 Cyber Supply Chain Risk Management Standard Implementation

Andrew F. Neuman

Assistant General Counsel

October 17, 2019

NYPA Background

- NYPA is a corporate municipal instrumentality and a political subdivision of the State of New York and operating pursuant to Title 1 of Article 5 of the New York Public Authorities Law
- NYPA is the largest state owned utility in the United States and operates 16 electricity generating facilities and more than 1,400 circuit-miles of transmission lines
- In recognition of its rigorous asset management practices, NYPA became the first electric utility in North America to receive ISO 55001 certification (September 2019)
- NYPA's power supply customers include the City of New York, the Metropolitan Transportation Authority, the Port Authority of New York, munis, co-ops and economic development customers statewide
- As a Generator Operator/Owner and Transmission Owner, NYPA is a "Responsible Entity" for purposes of CIP-013

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority

New York Laws, Regulations & Cyber Policies

- **New York Public Authorities Law § 2879:**

  "Every public authority . . . shall adopt by resolution comprehensive guidelines which detail the corporation's operative policy and instructions regarding the use, awarding, monitoring and reporting of procurement contracts."

- **New York State Technology Law § 201 - Internet Security & Privacy Act**

- **New York State General Business Law § 899-aa - Notification of Unauthorized Acquisition of Private Information**

- **NYPA Appendix P:** Procurement Requirements – Information Security Requirements for Vendors & External Partners

- **NY Public Officers Law §87 - New York Freedom of Information Law ("FOIL")**

- **Sole Source Procurements, Pre-qualified Selection, M/WBE Requirements, External Audits**

Transmission & Generation Assets and CIP Program Overview

CIP-013 Cyber Security Risk Management Plans Apply to High & Medium Impact BES Cyber Systems

Generation Statistics and Measures	
No. of Generators (including pump-storage units)	60
Installed Capacity (ICAP) (Summer 2017) (MW)	5,844

Transmission Statistics and Measures	
765 kV Transmission Lines (miles)	155
345 kV Transmission Lines (miles)	928
230 kV Transmission Lines (miles)	338
115 kV Transmission Lines (miles)	35
Bulk Electric System Stations (No.)	29

NYPA's CIP Program	
#Applicable Facilities:	**61**
# High Impact:	2
# Medium Impact:	24
# Low Impact:	35
# BES Cyber Systems:	**1,049**
# High Impact:	10
# Medium Impact:	491
# Low Impact:	548
# BES Cyber Assets:	**2,301**
# High Impact:	117
# Medium Impact:	963
# Low Impact:	1,221

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority

Overview of NYPA's organization and complex third-party landscape

8 Business Units

30 Departments

2,000+ Employees

~ 3,500 *Active Vendors* ***At Any Given Point***

Over 70,000 ***Items Currently in*** *Warehouse Inventory*

Approx. 50,000 *Line Items Requisitioned* ***Over the Last Year***

Over 20,000 *Contracts* ***Per Year***

Over 10,000 *Credit Card Transactions* ***Per Year***

NERC CIP Scope

< 200 *CIP Vendors* ***At Any Given Point***

< 5,000 ***CIP Items Currently in*** *Warehouse Inventory*

< 400 *CIP Related Contracts* ***Per Year***

NEW YORK STATE OF OPPORTUNITY. NY Power Authority

The procurement process presents risk and opportunities to be addressed within NYPA's CIP-013 solutions

Below is a simplified view of NYPAs procurement process

Competitive Bidding Process

Need Identification				Sourcing					Contract Management			Supplier Relationship and Performance Management	
IT/ Site/ Project Management (UOPP)	Need Identified	Inventory / On site due diligence	Purchase Requisition Submission	Sourcing Strategy	Solicitation	Bid Receipt, Handling, and Opening	Bid Evaluations	Bid Award	Initiation	Negotiation	Administration	Supplier Performance Monitoring	Supplier Continuous Improvement

CIP-013's new requirements will have broad impacts across many functions and regions:

Cross-Functional Team

- **Cyber Security**
- **Strategic Supply Management**
- Operations Technology
- Engineering (PCE and OCS)
- Physical Security

- Project Management
- Information Technology
- Legal and Internal Audit
- Corporate Ethics and Compliance
- HR/Training/Change Management
- Enterprise Risk Management

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority

CIP-013 Key Risks and Challenges

- Timeline to implement controls prior to enforcement is short
- SSM and supply processes have not previously been part of CIP program
- Organizational staffing to support comprehensive cyber assessment activities
- Suppliers not used to meeting CIP-013 related controls
- Internal stakeholder adoption of new/modified compliance processes
- Need for procurement standardization for vendors/vendor certification
- Small Purchase Risks & Limits on “piggy-backing” on other NY State contracts
- Costs to NYPA customers and NY State ratepayers

Where to Begin?

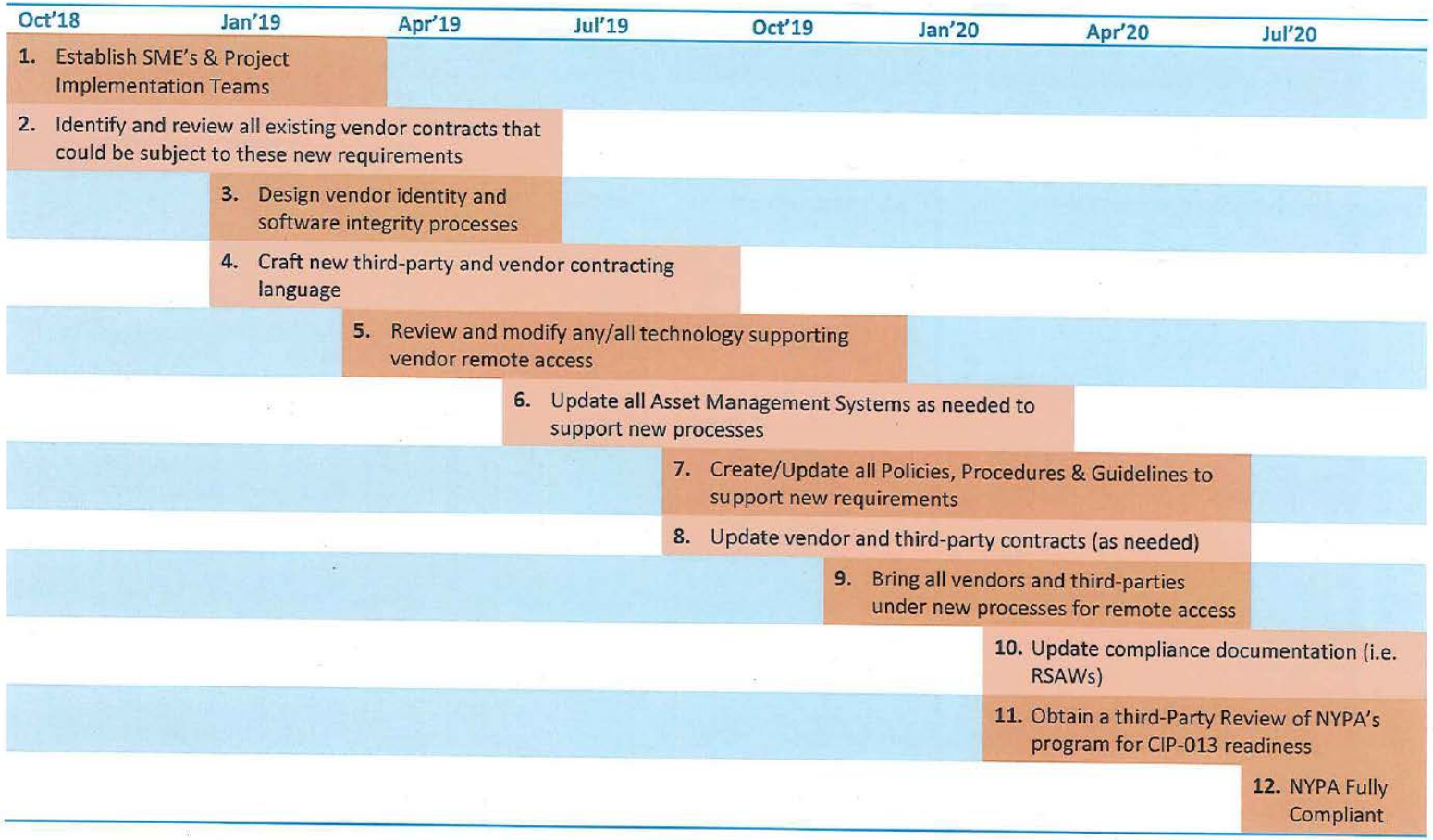
- NYPA is in the process of holistically revamping supply chain risk management processes across various points of the vendor management lifecycle.

- Project Phases for CIP-013 Implementation Include:

  - Initial Project Planning
  - Contract Analysis & Review
  - Development of “New” contracting language
  - Create Process for Vendor Verification
  - Identify Changes to Remote Access Process
  - Coordinate Alignment of all Documentation to Meet Audit Requirements

Appendix B: One Possible High-Level Project Plan

The following next steps and associated timeline are recommended in order for NYPA to ensure compliance with the new CIP Supply Chain requirements:



NEW YORK STATE OF OPPORTUNITY. NY Power Authority

CIP-013 Supply Process Requirements and Potential Solutions

Requirements

R1 A supply chain risk management plan defined which requires use of key contractual terms and addresses key supply situations for high and medium BES Cyber Systems

- Supplier incident notification
- Supplier response support
- Supplier remote access
- Supplier vulnerability disclosures
- Authenticity/integrity of supplied patches

R2 Proof of implementation/operation of the plan such that applicable items and services purchased for use in the BES and their suppliers can be shown to have been selected and procured according to the terms of the plan in R1 prior to use

R3 Proper delegation of annual review, approval and maintenance of the plan provided in R1

Potential Solutions

- Procurement Checklists to determine if the vendors must follow new CIP-013 Supply processes
- Contract T&C's along with new and updated policies and procedures to implement the Cyber Supply Chain Risk
- Management Plan and modifications to remote access and patch management processes
- Use of tools to automate the risk and vendor monitoring processes
- Use of cross-functional teams for the management of risks associated with potential CIP-013 vendors

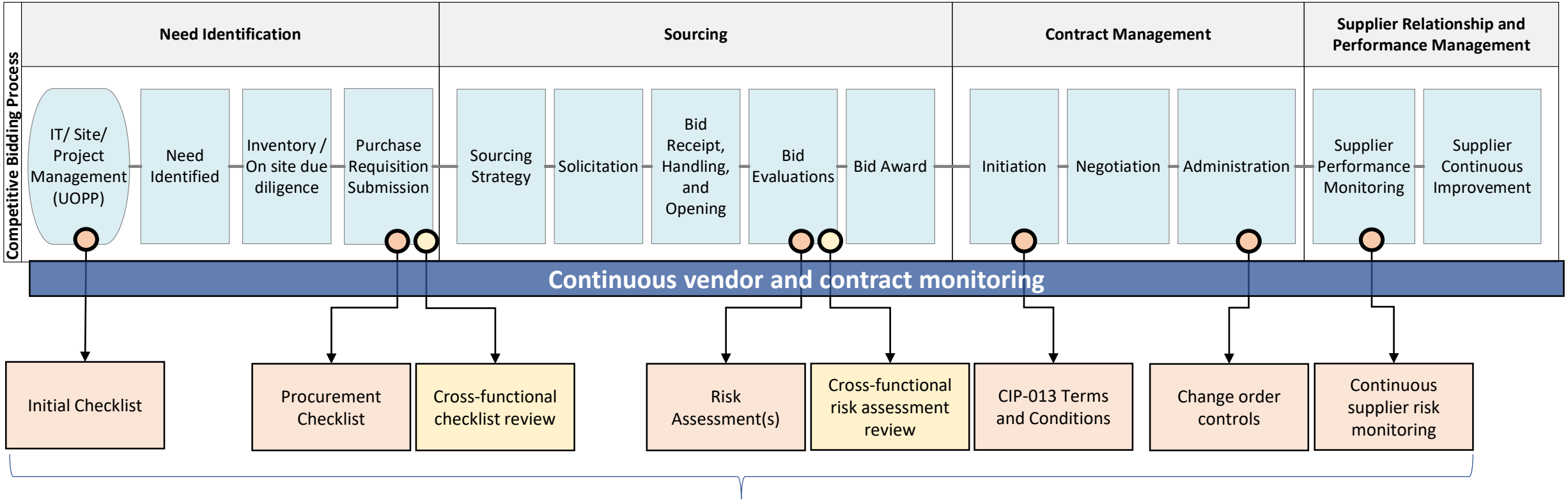
- Documentation of requirements as provided in CIP-013 R1.1
- Implementation and management of processes and tools to ensure requirements are in operation according to the terms of plan in R1

- Review and approval of plan and implementation of continuous monitoring tools or processes to ensure R1 is managed and maintained

What's been done to date

- Developed detailed project plan, initiated project baseline activities including the review of CIP-013 compliance requirements and engaged relevant stakeholders in Procurement, Cyber and Business unit
- Conducted current supply side process assessment with SSM, Cyber and business unit; developed high-level future supply side flows for procurement processes
- Reviewed vendor contracts for CIP-013 coverage across BES procurement channels
- Developed an Inherent Risk Questionnaire to enable identification of potential risks associated with vendor engagement
- Completed initial analysis of T&C's and NYPA Cyber 'Appendix P' for CIP-013 coverage
- Reviewed possible technology solutions that can assist and automate compliance processes

Example "New" Procurement Processes and Controls



The new Cyber Supply Chain Risk Management Plan could govern the above processes and controls

Above is an example only: NYPA is developing controls beyond those outlined for these in other procurement situations

Legend: Process Step | Compliance Control | Internal Control

NEW YORK STATE OF OPPORTUNITY. NY Power Authority

In Conclusion . . .

- It is not business as usual
- Everyone has a role in supporting strong compliance
- Ensuring deadlines are met without severely disrupting operations
- Pressing for the necessary organizational change these CIP requirements present
- Getting external feedback through sessions like today
- Collaborating with peers to solve industry-wide compliance challenges