TEXAS RE
Ensuring electric reliability for Texans

Ask Texas RE:

CIP-013-1: Supply Chain Risk Management

Kenath Carver

Director, Cybersecurity Outreach and CIP Compliance

CIP ERT – Level 1

Detail Tab or Request ID	Standard	Require-ment	Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet
Procurement	CIP-013		Provide a listing of each procurement during the audit period for high and/or medium impact BES Cyber Systems of vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s) on the Procurement tab. *Future use with CIP-013-2: Include procurements for EACMS and PACS associated with high and/or medium impact BES Cyber Systems.
CIP-013-R1-L1-01	CIP-013	R1	Provide each documented plan(s) that addresses the applicable requirement parts in CIP-013 R1.
CIP-013-R2-L1-01	CIP-013	R2	Provide a listing of vendors (persons, companies, or other organizations) with whom the responsible entity, or its affiliates, contract with to supply BES Cyber Systems and related services.
CIP-013-R3-L1-01	CIP-013	R3	Provide evidence that the documented plan(s) in CIP-013 R1 and its parts were reviewed and approved by the CIP Senior Manager or delegate(s) at least once every 15 calendar months during the audit period. Also provide evidence of the most recent review and approval performed prior to the audit period. Include the date of each review and the results, if any, of the review.

CIP ERT – Procurement Tab

		Procurement			Procurement Type			Procurement Dates				Sample Count:
Index	Unique ID	Vendor	BES Cyber System Impact Level	Description of Products or Services by Vendor or Vendor Transition(s)	Procurement for Vendor Products?	Procurement for Vendor Services?	Procurement resulting in Vendor Transition?	Identification & Assessment Start Date	Identification & Assessment End Dat	Procurement Start Date	Procurement End Date	Cyber Asset Classification *(future use)*
1												
2												
3												
4												

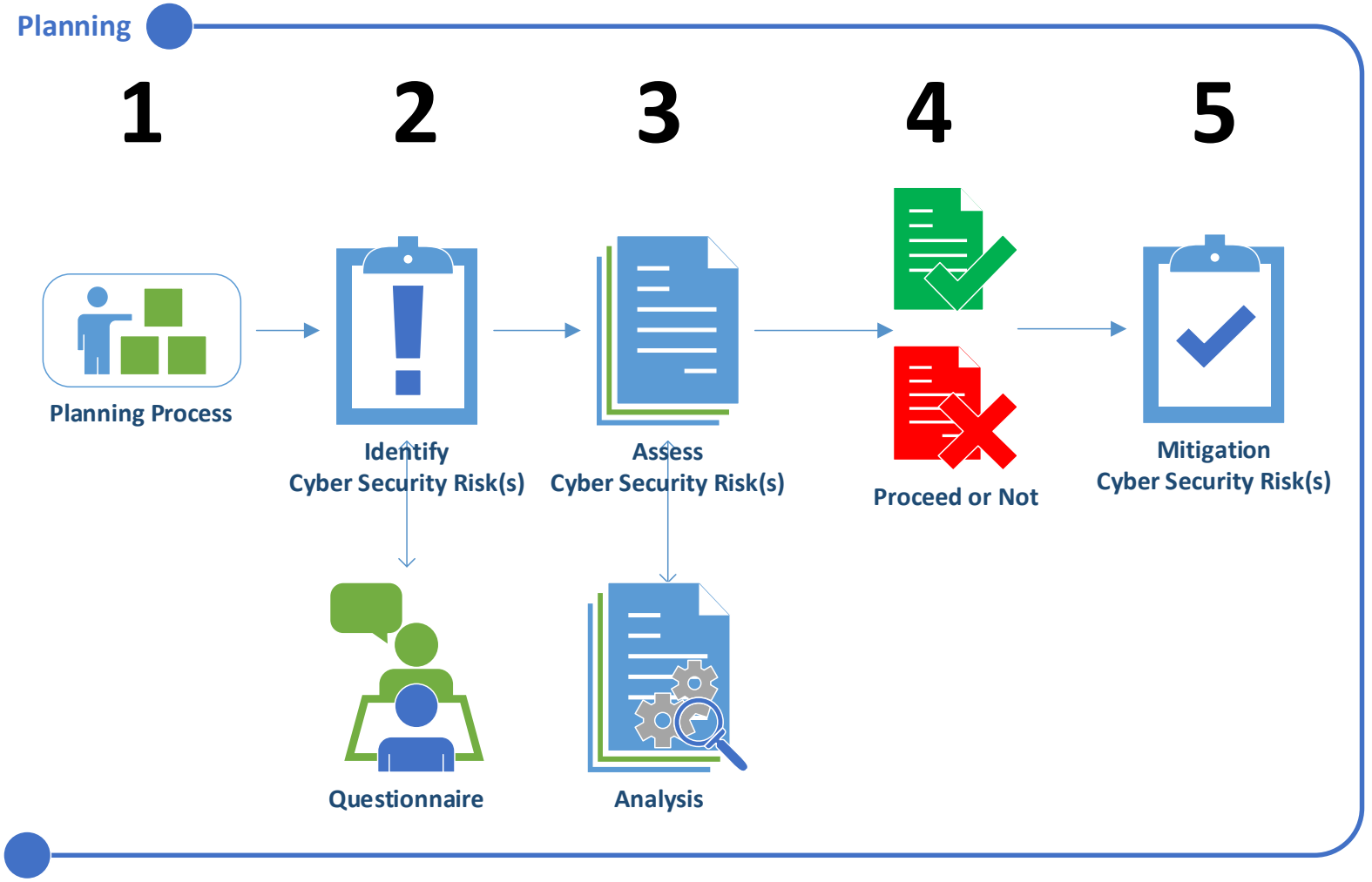
CIP ERT – CA Tab

Index	Cyber Asset ID	Date of Activation in a Production Environment, if Activated During the Audit Period	Date of Deactivation from a Production Environment, if Deactivated During the Audit Period
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

CIP ERT – Level 2

Request ID	Standard	Require-ment	Sample Set	Sample Set Source & Description	Sample Set Evidence Request
CIP-013-R2-L2-01	CIP-013	R2	Procurement-L2-01	Source Tab: Procurement Description: Sample of Unique IDs	For each Unique ID in Sample Set Procurement-L2-01, provide evidence of the identification and assessment of cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).
CIP-013-R2-L2-02	CIP-013	R2	Procurement-L2-01	Source Tab: Procurement Description: Sample of Unique IDs	For each Unique ID in Sample Set Procurement-L2-01, related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity, provide evidence of the implemented processes used in procuring that address the following, as applicable: 1. Notification by the vendor of vendor-identified incidents; 2. Coordination of responses to vendor-identified incidents; 3. Notification by vendors when remote or onsite access should no longer be granted to vendor representatives; 4. Disclosure by vendors of known vulnerabilities; 5. Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System; and 6. Coordination of controls for (i) vendor-initiated Interactive Remote Access, and (ii) system-to-system remote access with a vendor(s).

Evidence Outputs Part 1.1 Examples



CIP-013-1 R1 1.1 Audit Approach Examples

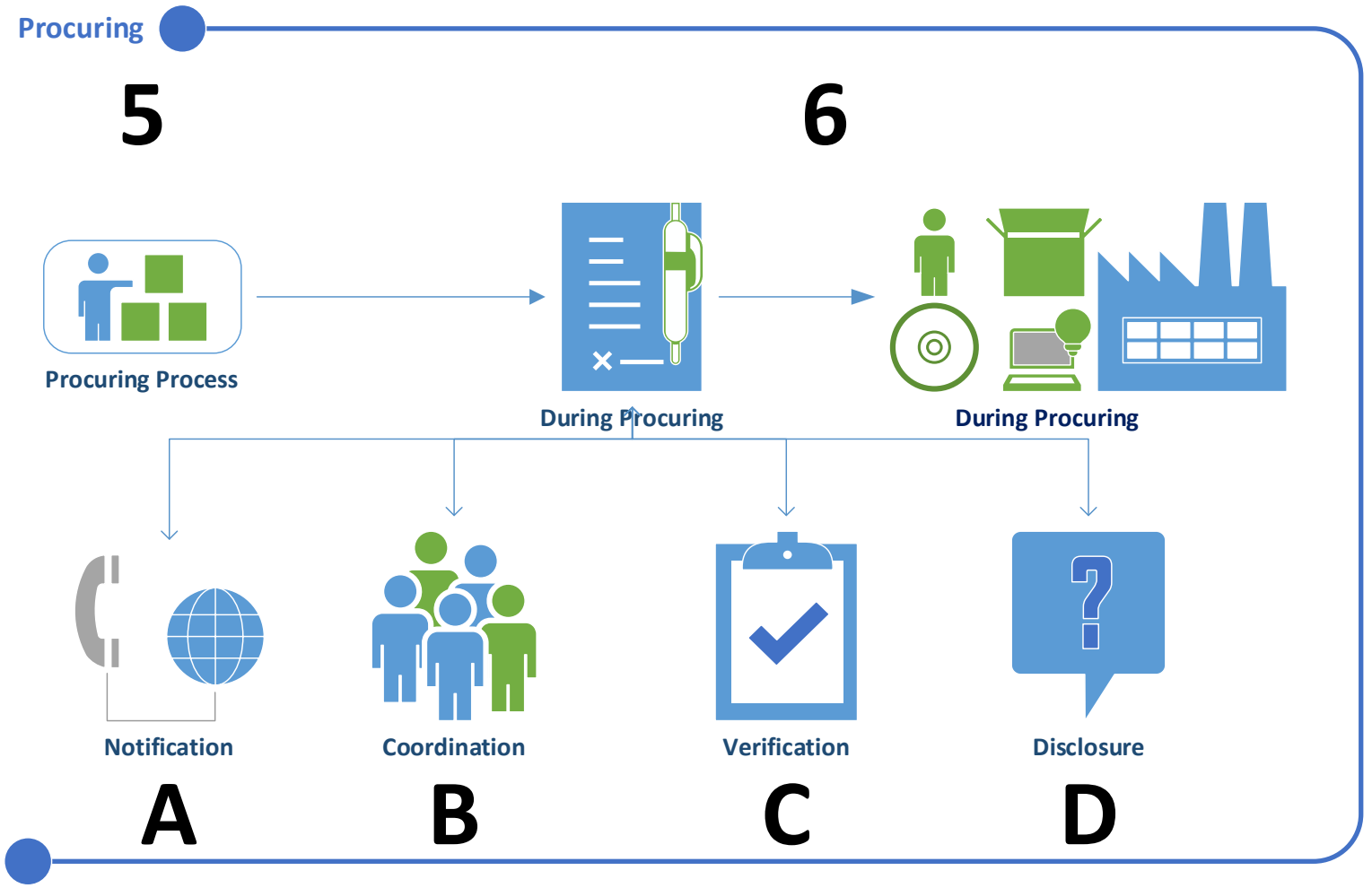
- Does the Entity Have Process(es)?
- How Does the Entity Define Vendor?
- How Does the Entity Address Procurements outside of the Normal Process(es)?
- Does the Process(es) Address How the Entity Will Identify and Assess Cyber Security Risk(s)?
- Does the Process(es) Address How the Entity Will Mitigate These Risks When Planning for BES Cyber Systems?

CIP-013-1 R1 1.1 and R2 Audit Approach Examples

Documentation

- BES Cyber Systems
- Vendor
- Products
- Services
- Dates
- Cyber Security Risk(s) Identified and Assessed
- Questionnaires & Analysis
- Cyber Security Risk(s) Mitigation
- Third-Party Services

Evidence Outputs Part 1.2 Examples



CIP-013-1 R1 1.2 Audit Approach Examples

- Does the Entity Have Process(es)?
- Does the Process(es) Address How the Entity Will Implement 1.2.1-1.2.6?
- In Lieu of Vendor Adherence, What Internal Controls Are Implemented?
- Does the Entity Continually Monitor Procurements after Procurement Is Complete?

CIP-013-1 R1 1.1 and R2 Audit Approach Examples

Documentation

- Dates
- Correspondence, Communications, etc.
  - Emails
  - Notification
  - Alerts
  - Logs
- Contracts, Agreements
- Internal Controls
- Third-Party Services

Outreach & Collaborations

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Industry Webinar Joint CCC/ERO Enterprise Webinar on Supply Chain

August 27, 2021 | 12:00 p.m. – 1:30 p.m. Eastern

Click here for: Join Webinar

The NERC Compliance and Certification Committee's Supply Chain Task Force (SCTF) has collaborated with the ERO Enterprise to address potential concerns with industry readiness for the enforcement of the CIP-013 Standards, Supply Chain Risk Management, and as an outreach opportunity to ensure industry remains informed and to support industry readiness. The NERC SCTF and the ERO Enterprise have been updating the Supply Chain Frequently Asked Questions for industry awareness and clarification of expectations. In addition, the SCTF has established a temporary email for submission of industry questions or requests where additional clarification is desired. The SCTF and the ERO Enterprise will be holding an informal webinar to discuss these items.

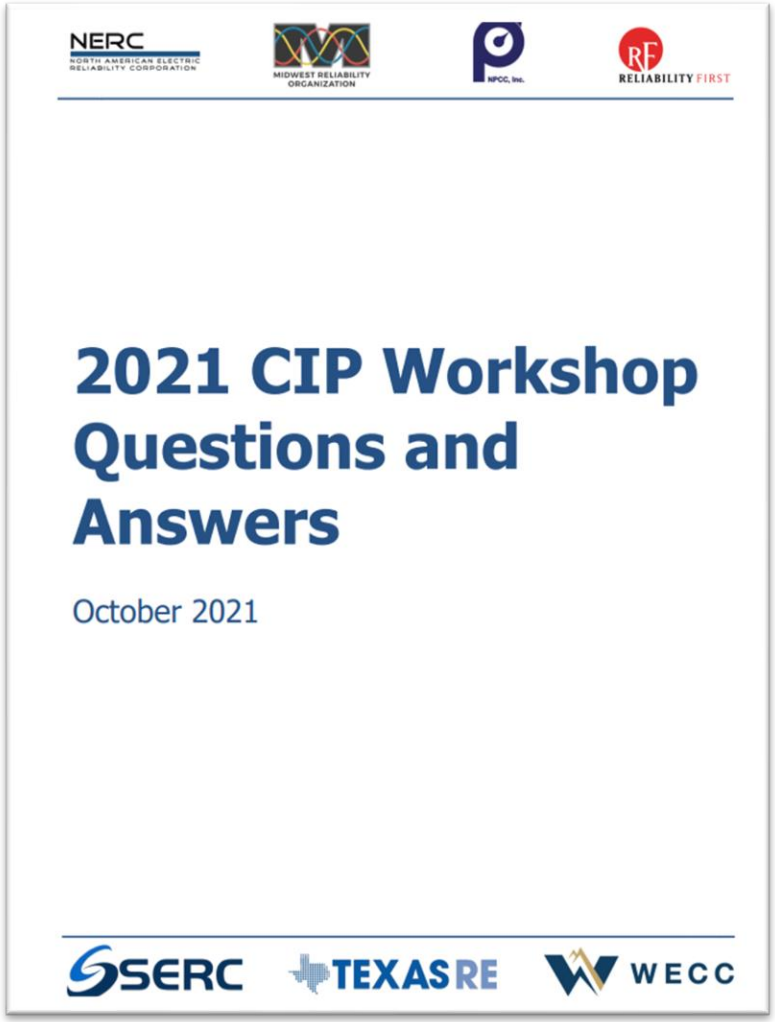
For more information or assistance, please contact Tiffany Whaley (via email) or at 404-290-2388.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
2560 | www.nerc.com

Joint CCC/ERO Enterprise Webinar

Outreach & Collaborations

Outreach & Collaborations



Individualized Collaborations

Help

TEXAS RE
Ensuring electric reliability for Texans