

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

CIP-002-4 through CIP-009-4 Technical Webinar

September 29, 2010

to ensure
the reliability of the
bulk power system

- Welcome and Opening Remarks – John Lim, Allen Mosher
- CSO706 Development Schedule Update – Phil Huff
- CIP-002-4 Revisions – John Lim
- Implementation Plan – Dave Revill
- Urgent Action SAR, CIP-005-4 – Jim Brenton
- Questions and Answers (All)
- Closing Remarks and Adjourn

- Provide
 - Context and background to CIP V4
 - Overview of Schedule and Milestones
 - Overview of CIP-002-4
 - Overview of Implementation Plan
 - Overview of CIP-005-4

Posted Documents – CIP V4 Standards

- CIP-002-4
 - Main revisions
- CIP-003-4, CIP-004-4, CIP-006-4, CIP-007-4, CIP-008-4, and CIP-009-4
 - Conforming changes
- Implementation Plan
- Reference (Guidance) Document
- Mapping Document
- VRF/VSL Analysis
- Summary Response to CIP-010 Attachment 2
 - “Consideration of Comments on Question 7”

- Separate Project (2010-15)
 - Urgent Action SAR
 - Urgent Action Revisions to Standard CIP-005-4

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security Order 706 Project 2008-06 – Draft Version 4 Industry Perspective

Allen Mosher – Chair, NERC Standards Committee

Technical Webinar for CIP-002 through CIP-009
Version 4

September 29, 2010

to ensure
the reliability of the
bulk power system

- NERC has established the completion of revised cyber-security standards as a Strategic Priority for 2010
- Broad support at the policy level:
 - NERC Executive Management
 - Standards Committee
 - NERC Board of Trustees
 - Industry Trade Association Coalition

- Cyber standards are part of a more comprehensive NERC infrastructure security program that includes:
 - Enhanced NERC situational awareness and communications capabilities
 - Development of a new set of recommendations to mitigate the Aurora vulnerability
 - Coordination by the ESCC with our government partners and other private sector industry segments
 - NERC Strategic Security Roadmap (posted for industry comment through October 1)

- New CIP standards are part of this defense in depth strategy to secure BES Assets and cyber-systems from unintentional failure and malicious acts
 - Common mode failure risks posed by deliberate cyber attacks present fundamentally different risks and different performance/behavior characteristics than the random events we plan for in n-1 contingency analysis studies
 - Current action will be judged based on perceived gaps and prior inactivity

- The industry has an opportunity to demonstrate the ERO Model works for cyber-security:
 - Use industry SMEs to develop reliability standards
 - Demonstrate industry consensus in support of: technical excellence, clarity, reasonable costs, enforceability, and responsiveness to regulatory concerns
- The alternative is a federal agency centric model:
 - President's Cyber-Security Initiative and agency programs
 - *Bi-partisan* Congressional support for action on cyber-security:
 - Energy Committees favor utility-sector specific approach (e.g., Grid Act)
 - Homeland Security Committees favor multi-sector approach
 - *No one favors doing nothing*

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security Order 706 Project 2008-06 – Draft Version 4 Development Schedule Update

Philip Huff – Arkansas Electric Cooperative
Corporation

Technical Webinar for CIP-002 through CIP-009
Version 4

September 29, 2010

to ensure
the reliability of the
bulk power system

Project Background

Incremental Progress

- Version 2 (Effective Apr 2010)
 - Addressed near-term directives
- Version 3 (Effective Oct 2010)
 - FERC directed changes
- Version 4
 - Impact thresholds replace risk-based assessment

Foundational Progress

- Concept Paper – July 2009
- CIP-010 Informal Posting – December 2009
- CIP-010 and 011 Informal Posting – May 2010
- Continued Drive to Consensus

CIP-002-4 Schedule



Remaining Project Schedule

- Address remaining 50+ FERC Directives in Order 706
- Improving the framework based on industry feedback
- Posting full package for formal comment in July 2011

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security Order 706 Project 2008-06 – Draft Version 4 CIP-002-4 Changes

John Lim – Consolidated Edison Co. of New York, Inc.

Technical Webinar for CIP-002 through CIP-009
Version 4

September 29, 2010

to ensure
the reliability of the
bulk power system

Scope: Identification of Critical Assets

- Non-uniform application of methodologies for identifying Critical Assets
 - Replace the Entity-defined Risk-Based Methodology requirement with a bright-line criteria
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

- Identification of Critical Assets
- Request for Data on Critical Assets
 - Identified currently
 - Categorized to High, Medium, Low
 - Currently identified Critical Assets
 - All BES assets
 - Criteria Different from Posted CIP002-4 Attachment 1
 - Data used as input for Drafting Team consideration
 - Excellent Industry Response: 647 responses

Critical Asset Identification — Each Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in *CIP-002-4 Attachment 1 – Critical Asset Criteria*. The Responsible Entity shall review this list at least annually, and update it as necessary.

Critical Cyber Asset Identification —..... For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes.....

- V3 qualifications still apply

Annual Approval — The senior manager or delegate(s) shall approve annually the list of Critical Assets and the list of Critical Cyber Assets.....

- No change in the requirement substance

- Criteria for Identification of Critical Assets (BES)
 - Bright-lines
- Generation
- Transmission
- Control Centers
- Anything else the Responsible Entity wants to include

- Plants with group of units = or > 1500 MW
 - Single unit or multiple unit plants
 - Critical Cyber Assets: Aggregate Impact
 - Nuclear Facilities evaluated based on bright line
- Required to run for reliability reasons
 - Designated by Transmission Planners
- Blackstart Resources
 - Designated by Transmission Operator in its restoration plan
 - Initial Plant for restoration – Glossary Term defined and used by EOP-005-2

- Reactive resources = or > 1000 MVARs
- Cranking Paths up to multiple path options
- Operating at = or > 500 KV
- Operating at = or > 300 KV with 3 other stations
- Facilities, if lost, etc., would violate IROLs
- FACTS, if lost, etc., would violate IROLs
- Loss of Critical Generation
- Nuclear Plant Interface Requirements (NPIRs)
- SPS/RAS, if lost, etc., would result in IROLs

Primary and Backup

- Performing the functional obligations of RC, BA, TOP
 - Refer to Reference Document for delegated functions (TOs)
- Generation Control = or > 1500 MW in a single interconnection

And...

Any additional assets that the
Responsible Entity deems
appropriate to include

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cyber Security Order 706 Project 2008-06 – Draft Version 4 Implementation Plan

David S. Revill – Georgia Transmission Corporation

Technical Webinar for CIP-002 through CIP-009
Version 4

September 29, 2010

to ensure
the reliability of the
bulk power system

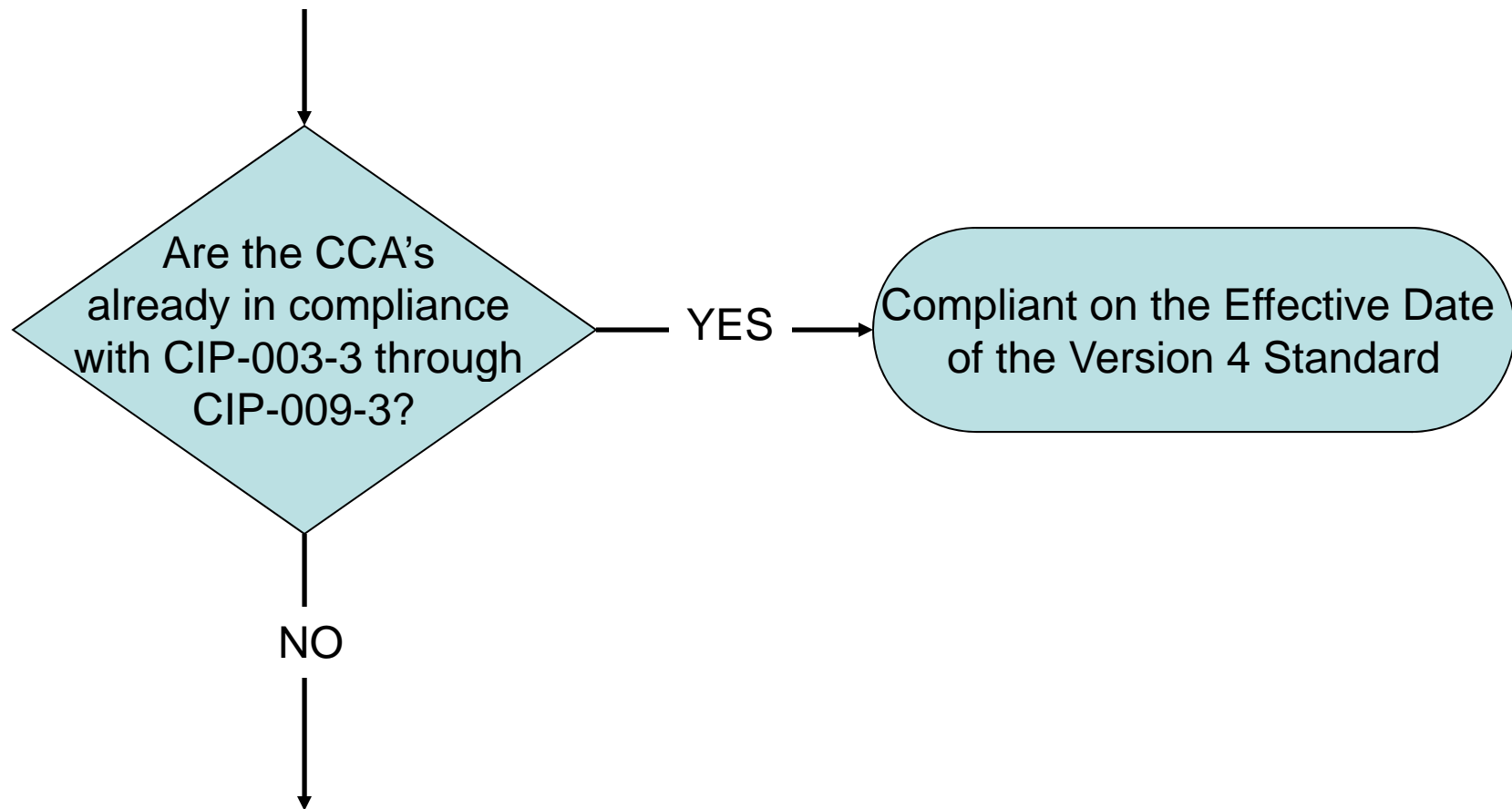
- Two Implementation Plans are included for Version 4
 - “Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4”
 - Lays out the implementation plan framework and refers the Entity to the “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities” if needed
 - Separate compliance milestone for CIP-002-4 vs. other standards
 - “Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities”
 - Only conforming changes from the Version 2 & 3 plans

- Compliance should be reached with CIP-002-4 on the Effective Date of the standard
 - The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after Board of Trustees (BOT) adoption in those jurisdictions where regulatory approval is not required)
 - [Minimum of 6 months following FERC approval]

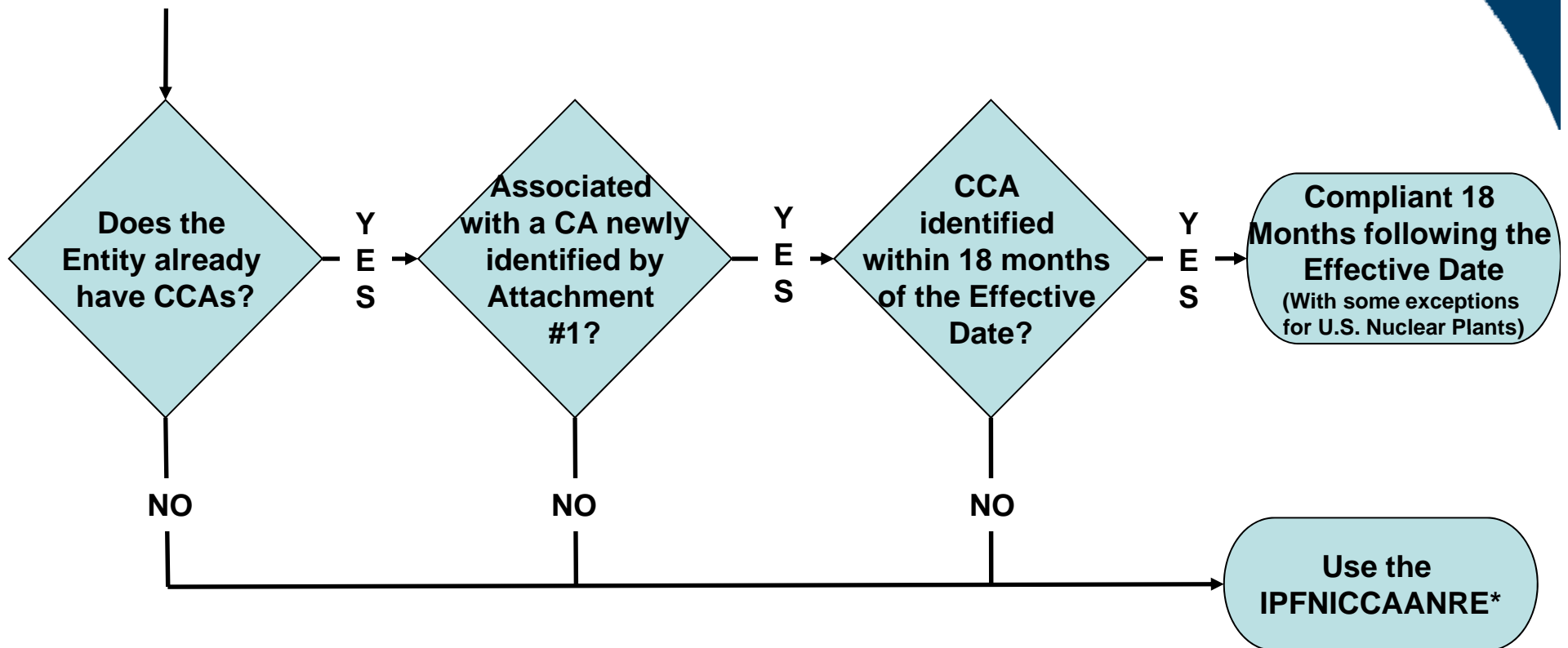
Implementation Plan – CIP-003-4 through CIP-009-4

- Critical Cyber Assets already in Compliance with CIP-003-3 through CIP-009-3
- Critical Cyber Assets associated with Critical Assets Newly Identified by CIP-002-4
- All Other Critical Cyber Assets

Critical Cyber Assets Already in Compliance with CIP-003-3 through CIP-009-3



Critical Cyber Assets associated with Critical Assets Newly Identified by CIP-002-4

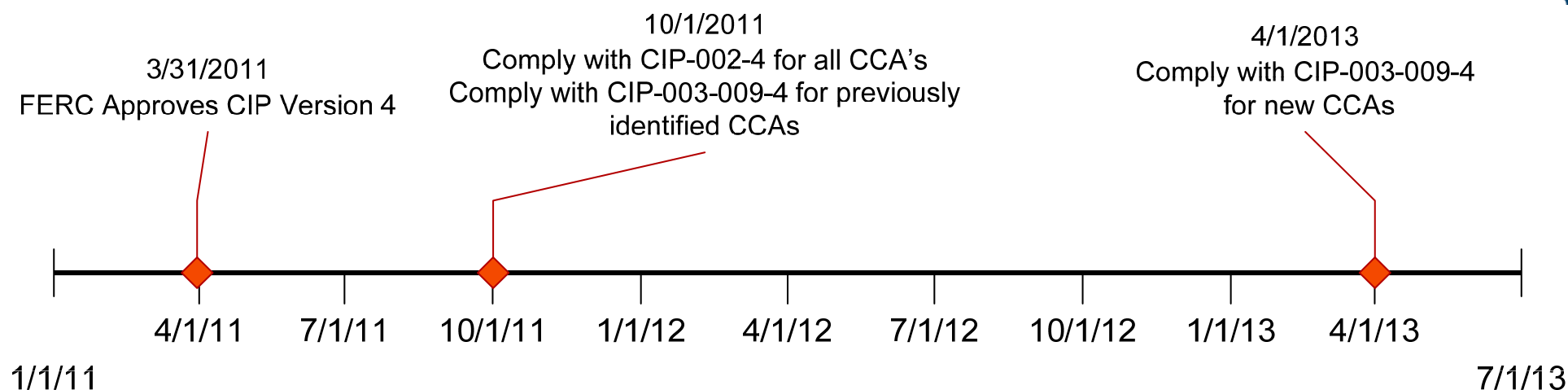


*IPFNICCAANRE - *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities*

Critical Cyber Assets associated with U.S. Nuclear Plants Newly Identified by CIP-002-4

- The 18 month implementation window is slightly modified for U.S. Nuclear Plants in recognition of their unique operating environment.
- Compliant the latter of
 - (i) 18 months following the Effective Date of CIP-002-4 R2
 - or
 - (ii) 6 months following completion of the first refueling outage beyond 18 months from the Effective Date of CIP-002-4 for those requirements requiring a refueling outage.
- Consistent with the approach used in the Version 3 Implementation Plan for U.S. Nuclear Plants

Implementation Timeline



All dates included in the timeline are purely speculative and are for example purposes only.

Implementation Plan – Summary

- **CIP-002-4**
 - Compliant by the Effective Date of CIP-002-4 (Approximately 6 months following FERC approval)
- **Critical Cyber Assets Already in Compliance with CIP-003-3 through CIP-009-3**
 - Compliant by the Effective Date (Approximately 6 months following FERC approval)
- **Critical Cyber Assets associated with Critical Assets Newly Identified by CIP-002-4**
 - Compliant with CIP-003-4 through CIP-009-4 18 months following the Effective Date (or approximately 24 months following FERC approval)
- **All Other Critical Cyber Assets**
 - Reference the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* for your specific compliance schedule
 - Newly Registered Entities have 24 months to be compliant with CIP-002-4 through CIP-009-4

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Urgent Action SAR and CIP-005-4 Remote Access

Jim Brenton – Electric Reliability Council of Texas

Technical Webinar for CIP-002 through CIP-009
Version 4

September 29, 2010

to ensure
the reliability of the
bulk power system

- Background
- Standards Modifications
- Reference Document
- Schedule

- Urgent Action Process initiated by Mike Assante in response to new intelligence received from DOE, DHS and FBI concerning vulnerabilities in VPN implementations
- Use Urgent Action Process
 - Submit SAR and Standard concurrently
 - Does not require a full drafting team
 - Does not require posting for comments

Urgent Action CIP-005-4

- Changes restricted to CIP-005
 - “Simplifies” development and balloting
 - Add requirements for Cyber Assets used to remotely connect to CCAs for the purpose of support and maintenance
 - Complements and does not conflict with CAN-005
- Guidance Document
- Schedule to complete for concurrent approval and filing of CIP-002-4 with regulators at the end of the year

Reference (Guidance) Document

- Executive Summary
- Background
- Use Cases
- Remote Access Concepts
- Case Studies
- References & Bibliography

- Pre-ballot posting and formation of ballot pool closed on 9/17/2010
- Balloting started on 9/17/2010 for 10 days
- Likely withdraw CIP-005-4 in response to ballot comments – modify and re-post for initial ballot
- Schedule to complete for concurrent approval and filing of CIP-002-4 with regulators at the end of the year



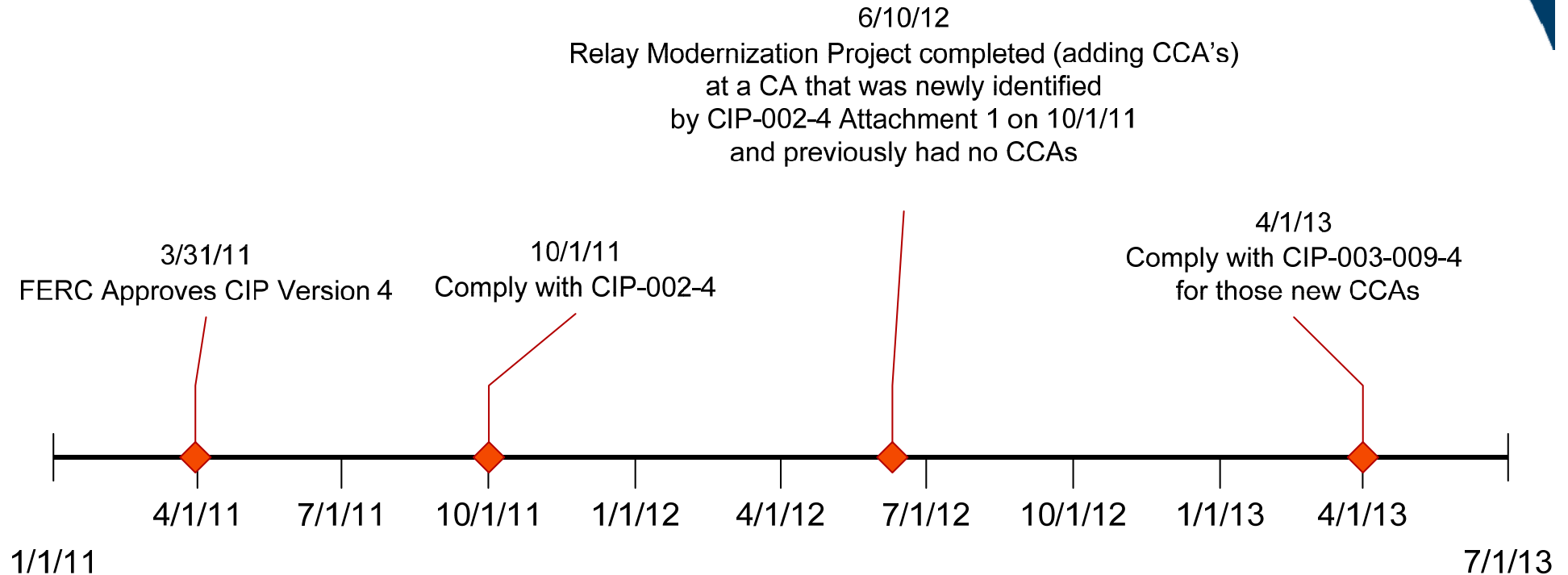
*Questions
and
Answers*

Closing and Adjourn

- Register for the Ballot Pool
- Provide Constructive Comments
- Offer alternative language where possible

Thank you.

Example of CCA Identification within the 18 months following the Effective Date



Example of CA Identification within the 18 months following the Effective Date

