

Draft CIP Standards Version 5

Project 2008-06 Cyber Security Order 706 Standards Drafting Team
April 10, 2012

RELIABILITY | ACCOUNTABILITY



Opening Remarks – John Lim, Consolidated Edison, Chair

Version 5 Overview – Philip Huff, AECC, Vice Chair

Version 5, Highlights of Draft 2 – John Lim, Consolidated Edison; David Revill, Georgia Transmission Corporation; and Jay Cribb, Southern Company

Comment and Ballot Process – Steven Noess, NERC and Jay Cribb, Southern Company

Questions and Answers – Moderated by Steven Noess, NERC



CIP Version 5 Overview

Comparative Table

Version 4	Version 5
42 requirements; 113 parts	37 requirements; 148 Parts
No contextual information	Includes background, rationale, and guidelines and Technical Basis
Measures on high level requirement only	Measures for each requirement, including parts
14 requirements with Technical Feasibility Exception (TFE) triggering language	12 requirements with TFE triggering language
Undefined periodic terms	Clear periodic requirements: initial requirements in Implementation Plan
Many binary Violation Severity Levels (VSLs)	More gradated VSLs

Advantages of Version 5



Flexibility

Builds on Experience

Systems Approach

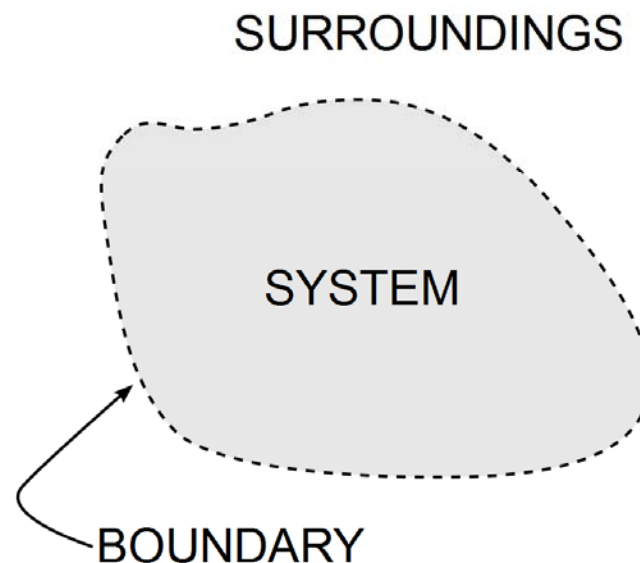
Results-based Standards

- Addresses the remainder of 60 directives in FERC Order No. 706
- Closes the continuous development cycle for CIP standards
- Allows industry to better implement long-term security solutions and audit programs

- Focuses on the reliability and security result
- Eliminates unnecessary documentation requirements
- Identifies examples of evidence
- Provides guidance and context alongside each requirement



- Cyber Assets function together as a complex system
- Identify the system and apply requirements to the whole rather than the part

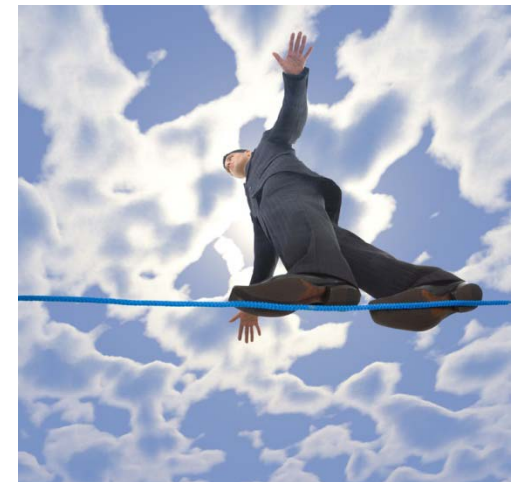



- Systems performing a Bulk Electric System (BES) function receive an appropriate level of protection
 - Systems are no longer “in or out”
- Impact and connectivity inform applicability
- Non-technology specific
- More appropriate use of TFE process
- Framework for establishing a culture of security

- Informed by and responsive to implementation and audit lessons from Versions 1 through 3
- Industry has progressed with better, alternative ways to meet a requirement objective
- Cyber risk and the tools to mitigate risk have changed



- Demonstrates clear accountability for CIP, yet...
- Balances the need to be both:
 - **Specific** enough to objectively demonstrate compliance and
 - **Broad** enough to allow effective risk mitigation
- **Specific** in *when* and *what* to achieve but **broad** in *how* to get there





CIP Version 5 – Highlights of Draft 2 Changes

- Applicability – Section 4
 - Distribution Provider/LSE
 - UVLS/UFLS
 - Distribution Provider
 - Cranking Path Elements

- Facilities-based approach
 - Identify High Impact and Medium Impact Facilities, Systems, and Equipment
 - Identify and categorize associated BES Cyber Systems and BES Cyber Assets
 - Attachment 1 criteria closer to Version 4 language
- BES Reliability Operating Services – No longer used
- Sixty days for update due to BES change

- Restoration Facilities, Systems, and equipment
 - Blackstart Resources
 - Cranking Paths
- Concerns on overall effect on BES restoration resources
 - NERC Operating Committee/Planning Committee discussion (March meetings)
- No longer in Medium Impact criteria
 - In scope
 - Default to Low Impact

- **BES Cyber Asset**

“A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, Systems, or equipment; which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, Systems and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)”

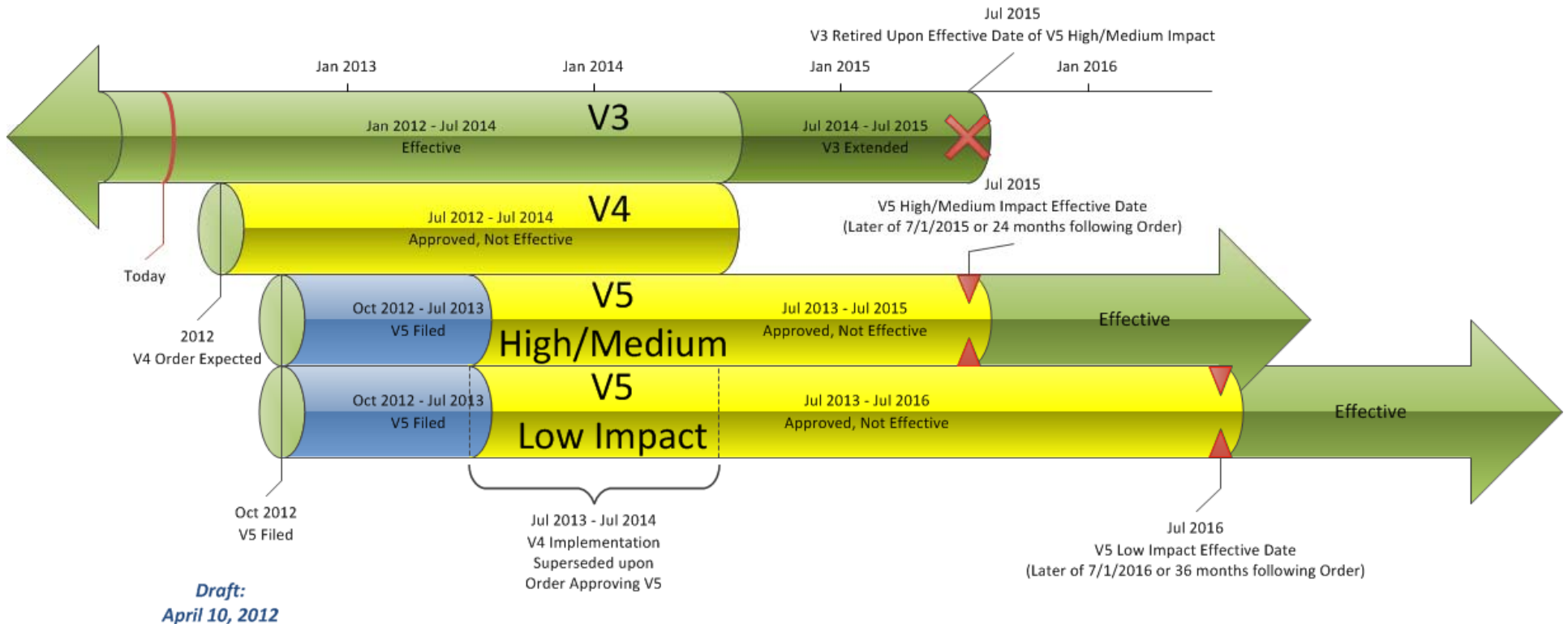
- BES Cyber System
 - “One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.”
- BES Reliability Operating Services
 - Removed as a NERC Glossary Term and from references in the requirements or other definitions
 - Moved as guidance to Guidelines and Technical Basis

- Control Center
 - “One or more facilities hosting operating personnel that monitor and control the BES in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations.”

- Dispersed requirements were hard to find and identify
 - “All Responsible Entity” requirements also applied to Low Impact
- Removed all Low Impact requirements from CIP-004 though CIP-011
- Now only a single requirement (CIP-003 R2) – Low Impact Policy
 - 2.1 Cyber security awareness;
 - 2.2 Physical access control;
 - 2.3 Electronic access control; and
 - 2.4 Incident response to a BES Cyber Security Incident.
 - An inventory, list, or discrete identification of BES Cyber Systems is not required.

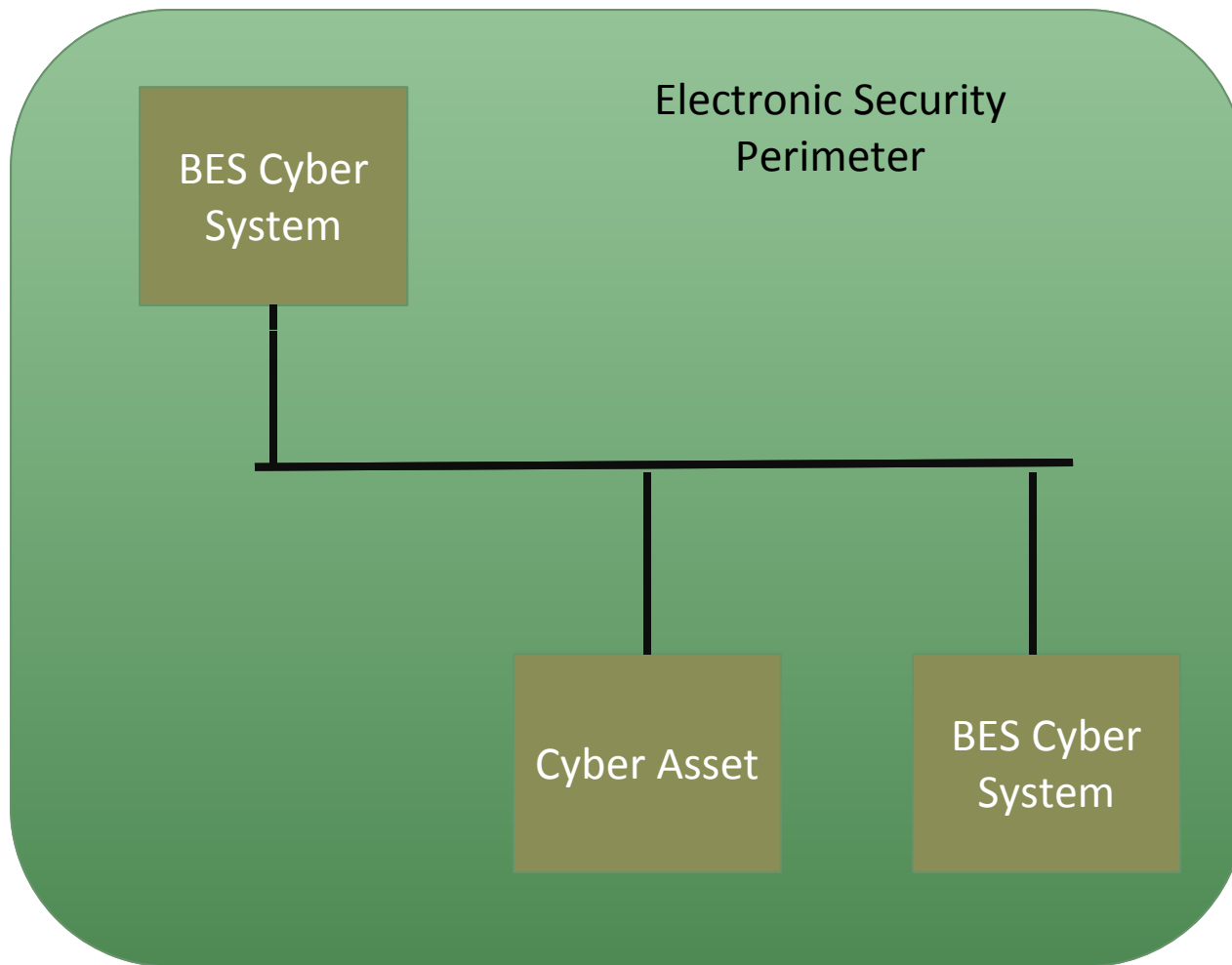
- Modified timing language in the standards
 - ~~“initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months”~~
- Initial performance clarified in Implementation Plan
 - On or before the Effective Date
 - Within X calendar days/months/years of the Effective Date

Proposed Implementation Plan for Version 5 of CIP Cyber Security Standards
(Graphic for illustrative purposes only; dates are estimates only and based on assumptions.
There is no way to know or anticipate when FERC may take action on pending matters.)



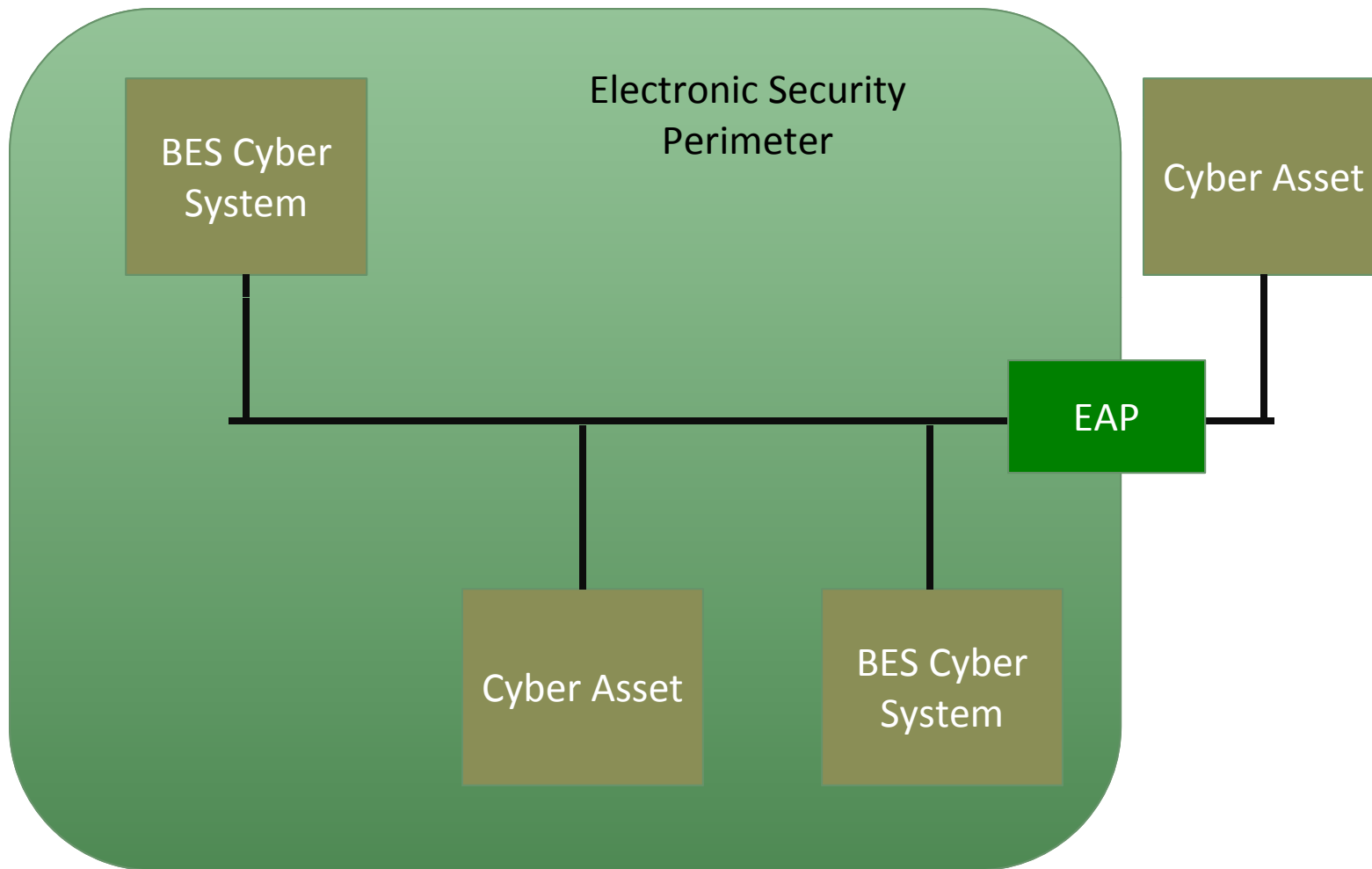
- Electronic Security Perimeter (ESP)
 - “The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.”
- Protected Cyber Asset (PCA)
 - “A Cyber Asset connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same ESP (a Cyber Asset is not a Protected Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a Cyber Asset within an ESP or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes).”

ESPs - High Watermarking

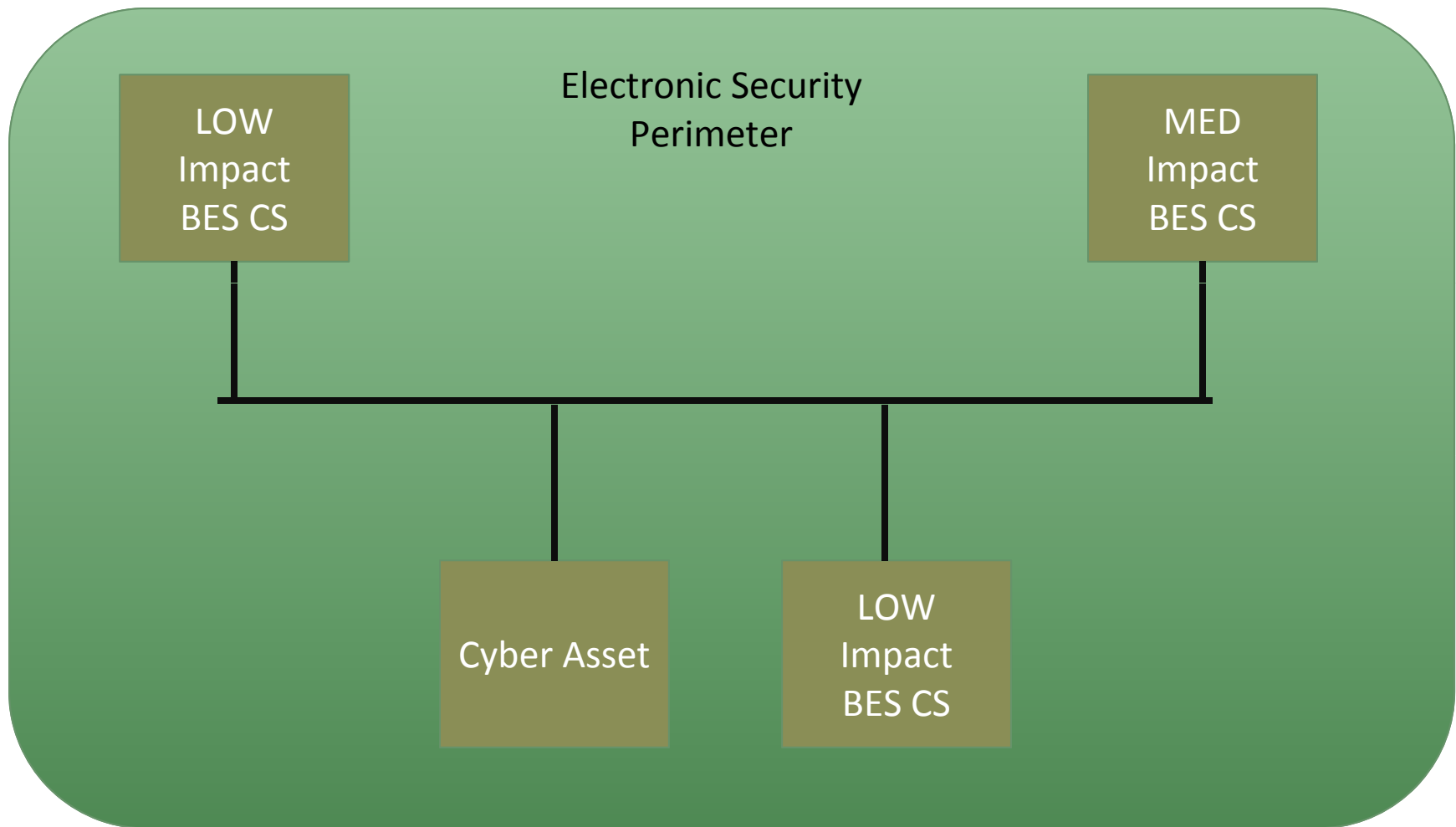


No External
Routable
Connectivity

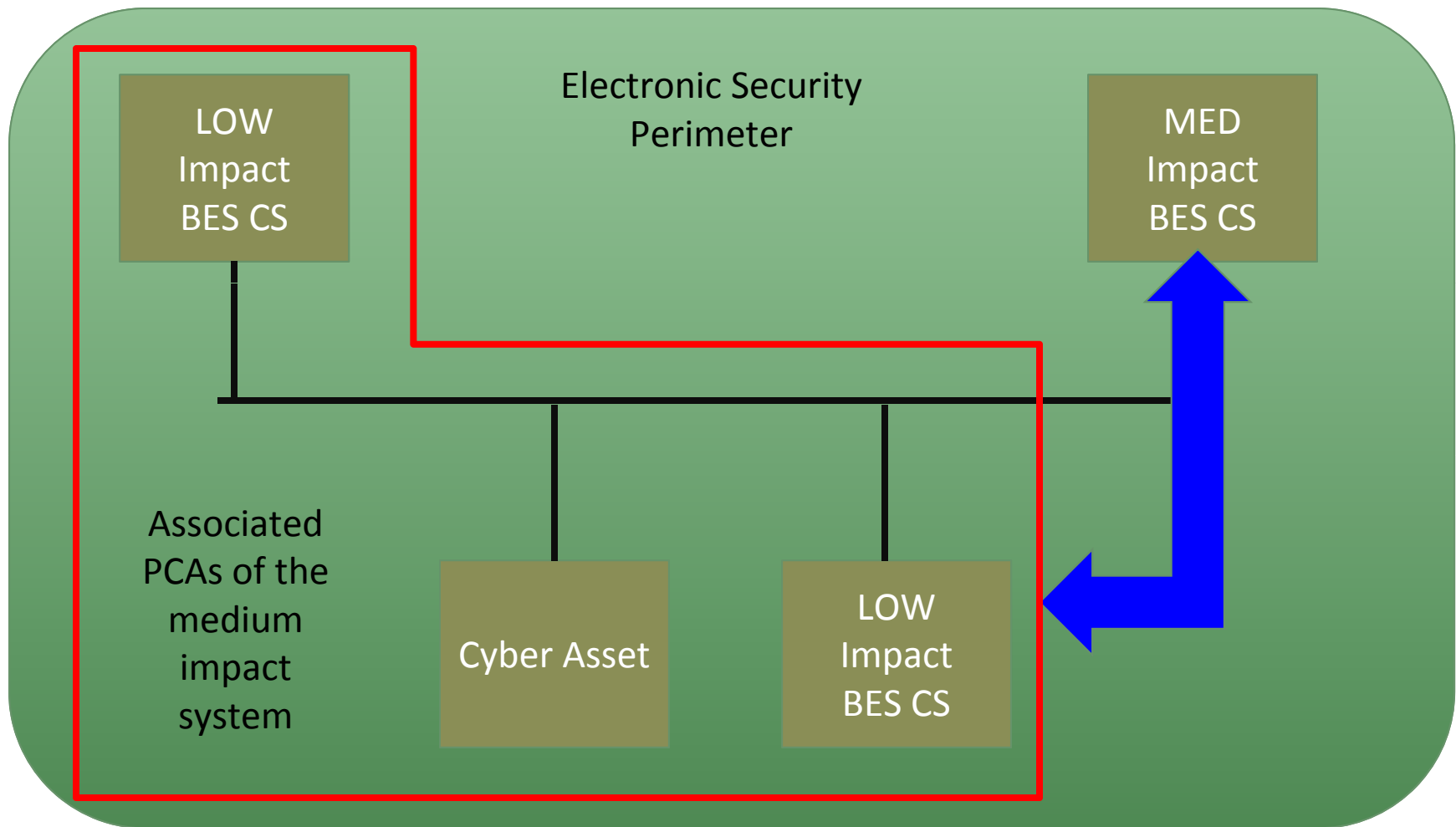
ESPs - High Watermarking



ESPs - High Watermarking



ESPs - High Watermarking



- All High and Medium Impact BES Cyber Systems
 - “Define operational or procedural controls to restrict physical access”
 - This includes standalone and serial connected BES Cyber Assets
- Additional items for Medium Impact BES Cyber Systems with External Routable Connectivity and High Impact BES Cyber Systems
 - Control, monitor, and log access to Physical Security Perimeters
 - Allow access to only individuals who have authorized unescorted physical access
 - Visitor control program, maintenance, and testing

- “Physical Security Perimeter” term replaces “Defined Physical Boundary”
- “Transient Cyber Asset” deleted
- “External Connectivity” deleted

- VSLs modified to include more granularity and gradation
 - Reduction in binary/severe nature
 - Gradated timeframes
 - Gradated percent of assets in violation



Comment and Ballot Process

Stakeholder Consensus Process

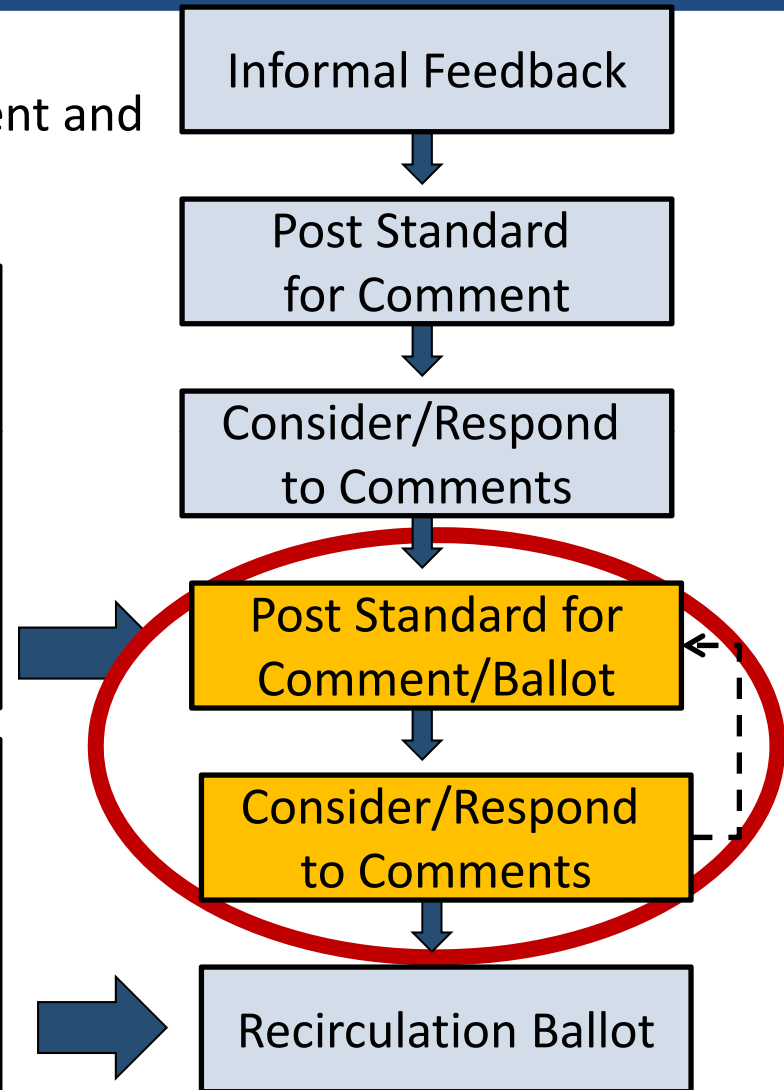
CIP Version 5 posted for 40-day formal comment and simultaneous 10-day successive ballot period

New/Successive Ballot:

At this step, the standard is either “new” or significantly changed from the last version posted for comment/ballot. The ballot record starts with no votes and no comments.

Recirculation Ballot:

At this step, there have been no significant changes to the standard from the last ballot. The ballot record starts with all votes and comments from the previous ballot.



Comment and Ballot Period

- April 12, 2012 through May 21, 2012
 - Formal 40-day comment period
- May 11, 2012 through May 21, 2012
 - Twelve Successive Ballots open
 - Ten Standards
 - Definitions
 - Implementation Plan



Navigating Stakeholder Input Toward Consensus

- Stakeholder feedback is essential
- Almost 2000 pages of comments
- Very constructive comments during last posting
- Drafting team considered all viewpoints



- Ballot Comments
 - Submit through “checkbox form” – not within ballot
 - No need to submit same comment more than once
- Comments on proposed standards
 - Submit through electronic form
 - Be brief
 - Focus on question asked
 - Indicating agreement with others is preferred over copying the comments (e.g., “ABC agrees with XYZ’s comments”)

- Unofficial comment form
 - Provided to assist comment development
 - Divided into four forms (A through D)
 - Formatting will not transfer from unofficial form to official form (web-based)
- Warning included on comment form:



VERY IMPORTANT:

Please note that **the official comment form does not retain formatting** (even if it appears to transfer formatting when you copy from the unofficial Word version of the form into the official electronic comment form). If you enter extra carriage returns, bullets, automated numbering, symbols, bolding, italics, or any other formatting, that formatting will not be retained when you submit your comments. Therefore, if you would like to separate portions of your comment by idea, e.g., the drafting team requests that each distinct idea in the same comment block be prefaced with (1), (2), etc., instead of using formatting such as extra carriage returns, bullets, automated numbering, bolding, or italics.

5. CIP-009-5 R1 states “Each Responsible Entity shall have one or more documented recovery plans that collectively include each of the applicable items in *CIP-009-5 Table R1 – Recovery Plan Specifications*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R1?

Yes

No

6. CIP-009-5 R2 states “Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable items in *CIP-009-5 Table R2 – Recovery Plan Implementation and Testing*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R2?

Yes

No

7. CIP-009-5 R3 states “Each Responsible Entity shall maintain each of its recovery plans in accordance with each of the applicable items in *CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication*.” The requirement then proceeds to define the requirement parts in the table. Do you agree with the proposed Requirement R3?

Yes

No

8. CIP-009-5: If you disagree with the changes made to CIP-009-5 since the last formal comment period, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Comments:

- Issues and responses for each individual requirement
- Effective feedback
 - Specific to question
 - Provided proposed change/rationale
- Less effective feedback
 - Repeating comment multiple times/responses to entire standard in every question
 - No reference to where suggested change should occur
 - Non-technology agnostic requirements that can't be applied to all Cyber Assets in a mandatory and enforceable environment.

- Please submit your questions via the ReadyTalk chat window
- Moderator and point of contact – Steven Noess, NERC
 - steven.noess@nerc.net
- Key dates:
 - April 12, 2012 through May 21, 2012 – Formal Comment Period
 - May 11, 2012 through May 21, 2012 – Ballots Open
- Slides and recording of this webinar will be posted to the NERC website (usually within three business days)