NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

# Industry Webinar

Project 2018-02 Modifications to CIP-008
Cyber Security Incident Reporting

November 16, 2018

RELIABILITY | ACCOUNTABILITY

# Agenda

- Presenters
  - Standard Drafting Team

| | |
|---|---|
| Chair, Dave Rosenthal, MISO | Vice Chair, Kristine Martz, Exelon |
| Member, Sharon Koller, ATC | Member, Tony Hall, LG&E |

  - NERC Staff - Alison Oswald
- Administrative Items
- Project 2018-02 Status
- Industry Areas of Concerns and Modifications
- Implementation Guidance Example
- Next Steps
- Questions and Answers

# NERC Antitrust

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

# NERC Public Disclaimer

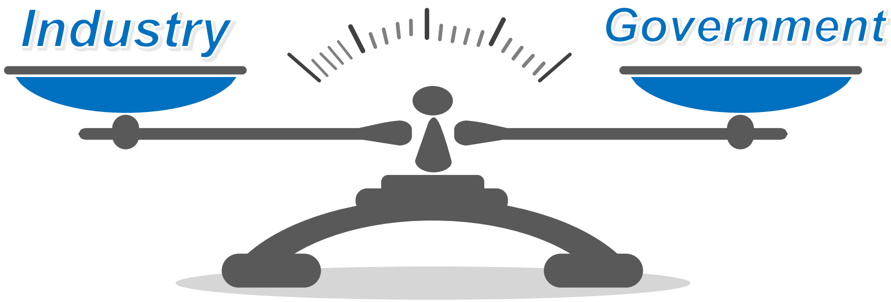
- Public Announcement
  - Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.
- Presentation Material
  - Information used herein is used for presentation purposes and may not reflect the actual work of the official posted materials
- For the official record
  - This presentation is not a part of the official project record
  - Comments must be submitted during the formal posting

# Status of Project 2018-02

- This is the second posting
  - 15-day comment period
  - 10-day ballot period (November 20 – 29, 2018)
- CIP-008-6 addresses:
  - FERC Order 848
- Team reviewed all industry comments and adjust approach
- Team is providing draft Implementation Guidance and Technical Rationale
  - This will help with understanding the approach/challenges

# Chair Remarks

- Team Theme:



- Team Goal:

*Deliver a* ***quality*** *product that will meet the directives in the FERC Order No. 848 while striking a* ***balance*** *between industry and government that will be industry approved before the NERC board meeting in February 2019*

---

- Ballot comments fell into 7 Areas of concern
- Team developed a strong outreach approach to help test our new approach
- Implemented changes that provide better alignment from a “balance” perspective
- Developed supporting documentation that will help everyone understand our approach

# CIP-008-6: Team Review

- **Ballot comments fell into 7 Areas of concern:**
  1. Attachment 1 (Removing it from the standard)
  2. Notification timeframe changes & Reporting requirements
  3. Updated definitions to provide clarity and better scope management
  4. PSP concerns have been addressed
  5. Clarity around definition of attempts
  6. Addressed concerns regarding scope as it relates to EACMS's and the five functions
  7. Addressed concerns regarding Implementation plan timing
- **Remember the Spirit of the order:**
  - Voluntarily sharing of information beyond reporting requirements does not introduce compliance risk and is encouraged.
  - Even if a cyber related issue does not escalate to the RCSI definition, the entity is still encouraged to share.

# Attachment 1

- **Industry Comments:**
  - Concerns over requiring the use of Attachment 1, the methods for submittal, alignment with existing forms such as OE-417, and reporting to multiple agencies

- **SDT Response:**
  - **The SDT removed the obligation to use Attachment 1** within the proposed CIP-008 R4, and moved it to draft Implementation Guidance. In addition, the SDT removed the requirement that prescribed the methods of notification
  - The SDT worked with E-ISAC and ICS-CERT's successor, the National Cybersecurity and Communications Integration Center (NCCIC), to review options
  - FERC Order 848 directly mentions that the OE-417 form does not meet the intention of the order. The proposed modifications to CIP-008 do not impact obligations to report under EOP-004
    - **Note:** E-ISAC launch of their Cyber Automated Information Sharing System (CAISS), developed in collaboration with E-ISAC members and designed to provide machine-to-machine cyber threat information sharing.

# Notification & Reporting Timeframes

- **Industry Comments:**
  - Concerns related to modifying the proposed initial notification and update timeframes due to the increase in scope of reporting.

- **SDT Response:**
  - The SDT adopted commenters proposal to **increase the timeline for reporting updates from 5 to 7 calendar days,** elected to keep the 1 hour initial reporting timeframe for Reportable Cyber Security Incidents, and end of next calendar day initial reporting for attempts to compromise
  - The Clock for initial notification starts when the Registered Entity determines the Cyber Security Incident is reportable
  - Entities are only obligated to initially notify the agencies of the attributes that are known upon determination
  - Entities determine the process for investigating, including the process for closing the investigation.  It is not the intention of the SDT to require continuous updates, but the team encourages the sharing of information as it is known.

# Definitions

- **Industry Comments:**
  - Commenters asked for clarity in the definitions for attempts to compromise, how BES Cyber Assets (BCAs) are included and the potential for consolidating definitions

- **SDT Response:**
  - The SDT determined the **definition for Reportable Attempted Cyber Security Incident is not needed**, and altered the approach to incorporate “attempts to compromise” into the requirement language for the Responsible Entity to establish criteria and follows their process to determine an attempt.
  - The SDT modified the definition of Reportable Cyber Security Incident to specifically include BES Cyber Systems that perform one or more reliability task of a functional entity.

# Physical Security Perimeters (PSPs)

- **Industry Comments:**
  - Commenters expressed confusion on how the standard relates to Physical Security Perimeters (PSP) and in some instances requested the removal of PSP from the Cyber Security Incident definition.
- **SDT Response:**
  - The SDT elected to keep PSPs in Cyber Security Incident definition based on previous FERC Order 706 which directed the SDT to consider breaches that occurred through cyber or physical means.
  - **The intention is not for PSP breaches alone to be considered Cyber Security Incidents.**
  - If a cyber component is identified via an investigation of a physical breach, the regional entities CIP-008 processes should be activated to determine classification, response, and reportability.

# Attempts

- **Industry Comments:**
  - Commenters requested a definition for "attempts," or for the SDT to provide clear examples within Implementation Guidance to aid the industry
- **SDT Response:**
  - The SDT modified the requirement language to link the Registered Entity's processes to identify, classify and respond under CIP-008 R1, Part 1.1, its process to define attempts and to determine reportability under CIP-008 R1, Part 1.2.
  - It is to Industry's benefit to provide the **Responsible Entity with the ability to define attempts in accordance with their existing frameworks** based on system architecture and their "normal".
  - The SDT has includes examples in the posted draft Implementation Guidance.

# Five Functions of an EACMS

- **Industry Comments:**
  - Concerns that the inclusion of the five functions modified the definition of Electronic Access or Monitoring Control Systems (EACMS) and either narrowed or broadened the scope of the proposed modifications to definitions.

- **SDT Response:**
  - **The SDT elected to remove the five functions of an EACMS that were identified in the FERC Order from all proposed and modified definitions.**
  - Through outreach it was determined that that functions were not included in the order to change the scope of the EACMS definition, but to justify the inclusion of EACMS in the scope of CIP-008.
  - The definition and applicability column are aligned to eliminate confusion regarding asset classification vs. the function(s) of a device.
  - The SDT understands regional discrepancies on EACMS definitions, and refers the entity to relay concerns to NERC.

# Implementation Timeline

- **Industry Comments:**
  - Concerns that a 12-month implementation plan is not sufficient to accommodate the increased workload associated with increased reporting requirements

- **SDT Response:**
  - **The SDT increased the proposed implementation plan from 12-months to 18-months.**
  - The SDT was compelled to make the modification based on comments related to:
    - The impact on small business entities;
    - The time required to modify compliance documentation;
    - The time required to develop and deploy enhanced end-user training;
    - Alignment with existing CIP-008 requirements (15 month test cycle); and
    - Consideration to resources and potential network architecture modifications

# Information Protection

- **Industry Comments:**
  - Concern over information protection once information is submitted to E-ISAC and NCCIC, and Freedom of Information Act (FOIA) requests

- **SDT Response:**
  - The SDT submitted comments related to Information Protection to the E-ISAC and NCCIC, and received the following information in response:
    - **Both organizations have multiple ways to secure submitted information** including a secure portal, and encrypted e-mail (PGP)
    - DHS will not attribute any information to an entity, but may incorporate non-attributable and anonymized information into publicly available products
    - Data submitted to DHS is stored with other sensitive incident reporting data received an triaged from various public and private sector entities
    - DHS has successfully exempted similar information from FOIA in the past under exemptions *(see Consideration of Comments for detailed responses from DHS)*

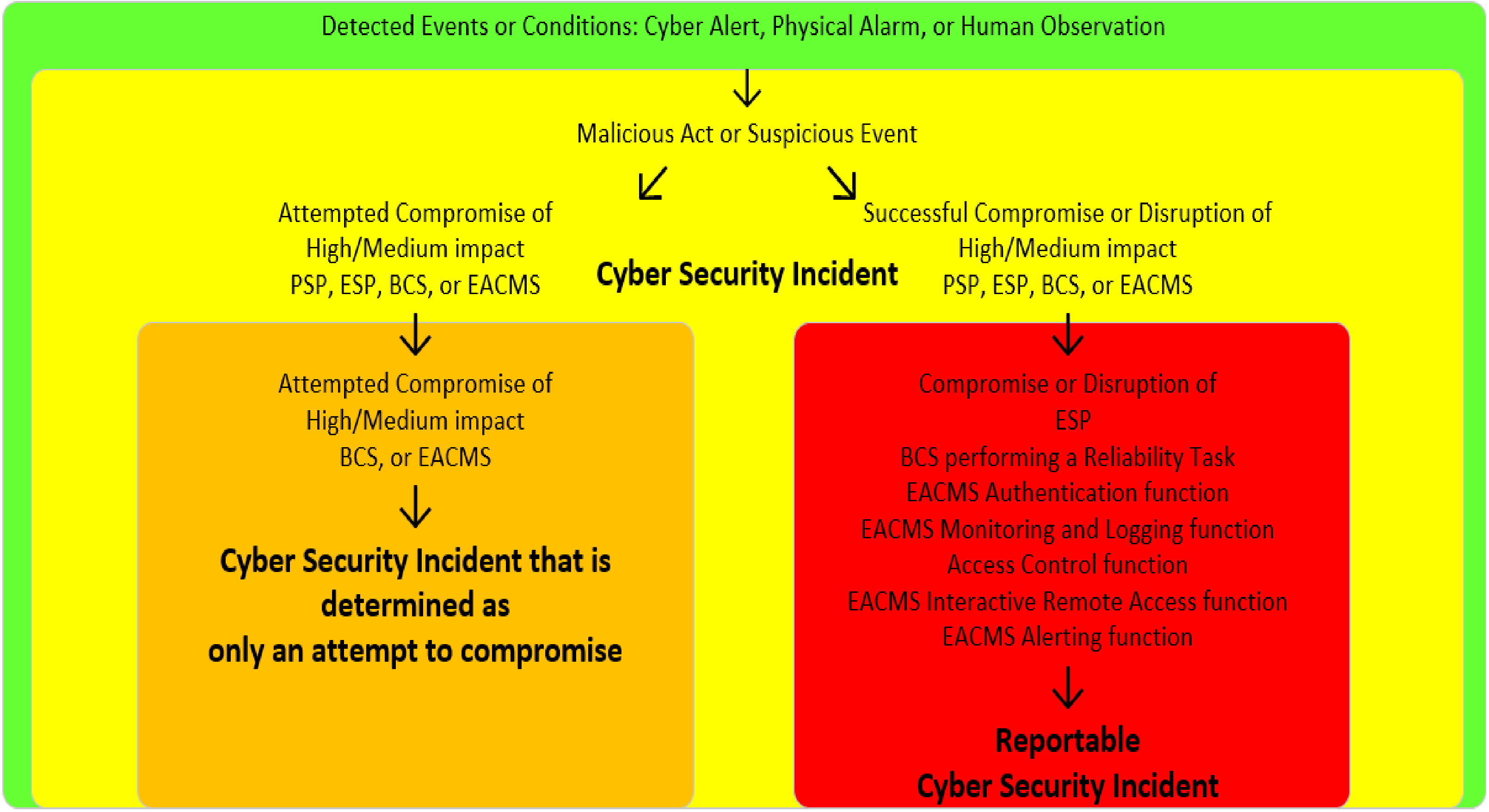
# Technical Rational & Implementation Guidance

- **Industry Comments:**
  - Industry requested Implementation Guidance to understand how Responsible Entities could meet compliance with the proposed modifications

- **SDT Response:**
  - Implementation Guidance has not yet gone through the formal approval process
  - **The SDT has posted both draft Technical Rationale and Implementation Guidance** for consideration because the team believes that it is an important element of the overall standards development process
  - The draft Implementation Guidance includes an explanation of the relationship between the proposed definitions, ways that a Registered Entity may choose to define attempts, decision tree models, methods for reporting, practical examples, and other information to support the implementation of the proposed modifications
  - The draft Technical Rationale has also been posted for review, and outlines the SDT’s positions

# Implementation Guidance Example

- **Relationship between definitions and requirement language:**



Detected Events or Conditions: Cyber Alert, Physical Alarm, or Human Observation

↓

Malicious Act or Suspicious Event

↙ ↘

Attempted Compromise of
High/Medium impact
PSP, ESP, BCS, or EACMS

**Cyber Security Incident**

Successful Compromise or Disruption of
High/Medium impact
PSP, ESP, BCS, or EACMS

↓

Attempted Compromise of
High/Medium impact
BCS, or EACMS

↓

**Cyber Security Incident that is determined as only an attempt to compromise**

↓

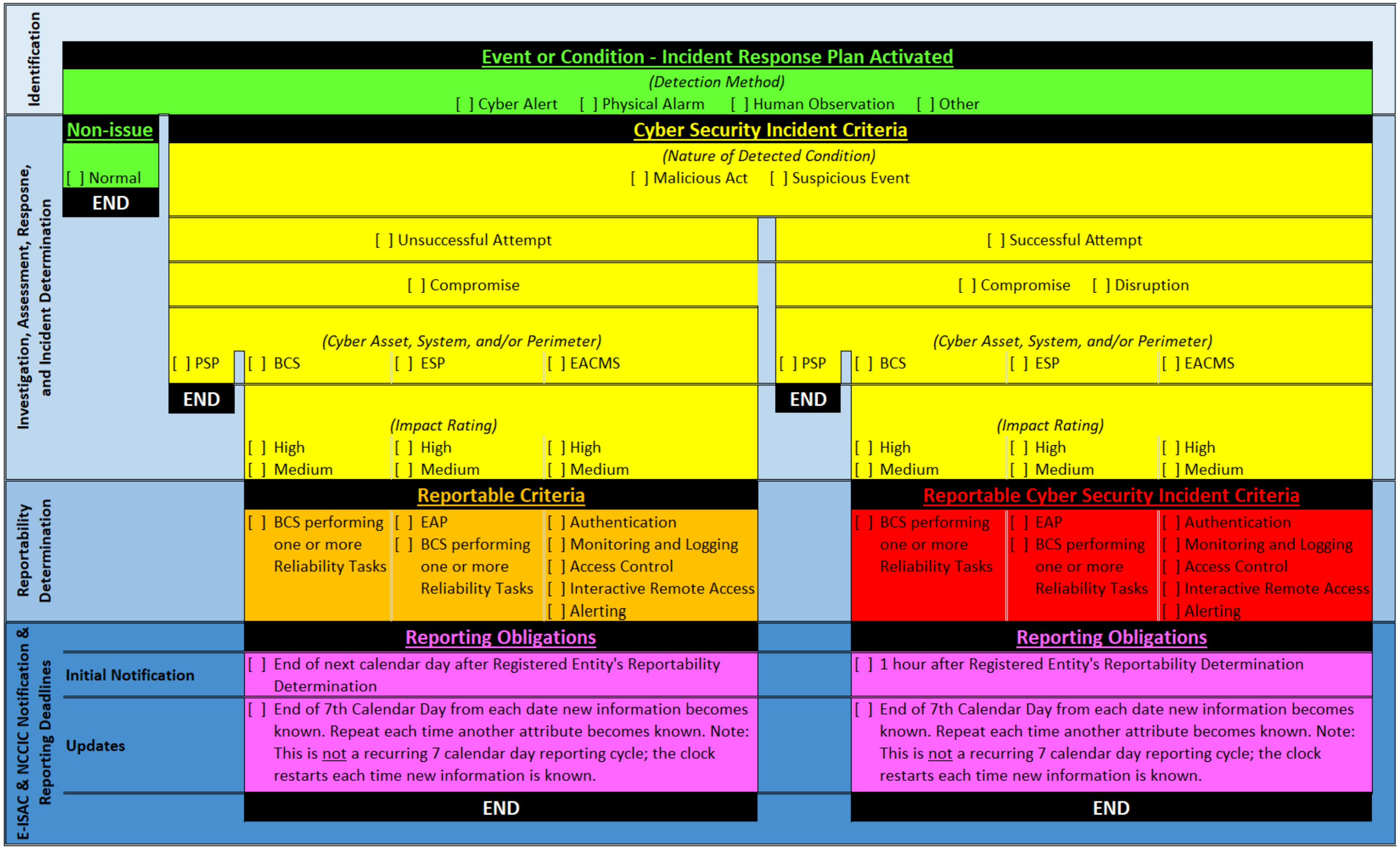
Compromise or Disruption of
ESP
BCS performing a Reliability Task
EACMS Authentication function
EACMS Monitoring and Logging function
Access Control function
EACMS Interactive Remote Access function
EACMS Alerting function

↓

**Reportable Cyber Security Incident**

# Implementation Guidance Example (cont'd)

- **Example Decision Tree Model:**



Identification

**Event or Condition - Incident Response Plan Activated**

*(Detection Method)*

[ ] Cyber Alert [ ] Physical Alarm [ ] Human Observation [ ] Other

Investigation, Assessment, Resposne, and Incident Determination

**Non-issue**

[ ] Normal

END

**Cyber Security Incident Criteria**

*(Nature of Detected Condition)*

[ ] Malicious Act [ ] Suspicious Event

[ ] Unsuccessful Attempt

[ ] Compromise

*(Cyber Asset, System, and/or Perimeter)*

[ ] PSP — END

[ ] BCS [ ] ESP [ ] EACMS

*(Impact Rating)*

[ ] High [ ] High [ ] High

[ ] Medium [ ] Medium [ ] Medium

[ ] Successful Attempt

[ ] Compromise [ ] Disruption

*(Cyber Asset, System, and/or Perimeter)*

[ ] PSP — END

[ ] BCS [ ] ESP [ ] EACMS

*(Impact Rating)*

[ ] High [ ] High [ ] High

[ ] Medium [ ] Medium [ ] Medium

Reportability Determination

**Reportable Criteria**

[ ] BCS performing one or more Reliability Tasks

[ ] EAP

[ ] BCS performing one or more Reliability Tasks

[ ] Authentication

[ ] Monitoring and Logging

[ ] Access Control

[ ] Interactive Remote Access

[ ] Alerting

**Reportable Cyber Security Incident Criteria**

[ ] BCS performing one or more Reliability Tasks

[ ] EAP

[ ] BCS performing one or more Reliability Tasks

[ ] Authentication

[ ] Monitoring and Logging

[ ] Access Control

[ ] Interactive Remote Access

[ ] Alerting

E-ISAC & NCCIC Notification & Reporting Deadlines

**Reporting Obligations**

**Initial Notification**: [ ] End of next calendar day after Registered Entity's Reportability Determination

**Updates**: [ ] End of 7th Calendar Day from each date new information becomes known. Repeat each time another attribute becomes known. Note: This is not a recurring 7 calendar day reporting cycle; the clock restarts each time new information is known.

END

**Reporting Obligations**

**Initial Notification**: [ ] 1 hour after Registered Entity's Reportability Determination

**Updates**: [ ] End of 7th Calendar Day from each date new information becomes known. Repeat each time another attribute becomes known. Note: This is not a recurring 7 calendar day reporting cycle; the clock restarts each time new information is known.

END

*Where 'Calendar Day' is used, the 'end' of the day = 11:59 PM local time of that day.

** Where 'Determination' is used, this refers to the Registered Entity's Determination.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Implementation Guidance Example (cont'd)

- **Examples of varied events and conditional factors from draft Implementation Guidance:**

| Event | Normal or Benign | Malicious / Confirmed Suspicious |
|---|---|---|
| **Detected malware** | • A corporate machine infected by a known Enterprise Windows-specific vulnerability is scanning all local hosts including a non-Windows-based EACMS or Windows-based EACMS or BCS and is determined by the Registered Entity to be an SMB exploit applicable to only Windows-based machines. | • An infected corporate machine is scanning all local hosts including an EACMS or BCS for well-known ports and determined to be a suspicious event by the Registered Entity. (**Cyber Security Incident pursuant to CIP-008-6 R1.1 determination**) |
| | | • An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**) |
| | | • An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and has attempted to gain unauthorized access to the EACMS or BCS. (**determination of only an attempt to compromise one or more systems identified in the "Applicable Systems" column for CIP-008-6 R1.2**) |
| | | • An infected corporate machine is scanning all local hosts including an EACMS or BCS for specific known ICS ports and exploited/compromised specified ICS ports that perform command and control functions of a BCS. (**Reportable Cyber Security Incident pursuant to CIP-008-6 R1.2 determination**) |

Normal

Investigate

Report as only an attempt to compromise

Report as successful compromise

# Summary of Changes

- Definitions
  - *Removed five EACMS functions*
  - *Removed reportable attempted cyber security incident*
  - *Developed Implementation Guidance for Attempts*
- Requirement Language
  - Attachment 1 – *Removed, 'how' is up to each entity*
  - Notification Methods – *Removed, 'how' is up to each entity*
  - Timelines – *Adjusted from 5 calendar days to 7 for 'Updates'*
  - PSP – *Struck unneeded and confusing language*
  - Attempt - *Added criteria for entity to define*
- VSLs – Reduction in Severity
- Implementation Plan – changed from 12 to 18 months

# Documents for 2nd Posting

CIP-008-6 documents available during the 2nd Posting:

- 2nd Proposed Draft standard including Definitions (Clean and Redline)
- Updated Implementation Plan
- VRF/VSL Justification
- Technical Rationale
- Consideration of, and Response to, Comments
- Implementation Guidance

# Next Steps

- Comment period
  - Project 2018-02 page
  - 15-Day Comment – November 15 – 29, 2018
  - 10-Day Ballot – November 20 - 29, 2018
- Respond to Comments
  - December 2018
- Point of contact
  - Alison Oswald, Senior Standards Developer
  - Alison.oswald@nerc.net or call 404-446-9669
- Webinar Posting
  - 48-72 hours
  - Standards Bulletin

# Q & A Objectives

- Informal Discussion
  - Via the Q&A feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions as possible
  - Webinar and chat comments are not a part of the official project record

# Questions and Answers

# Webinar has ended – Thank You