



RELIABILITY & SECURITY

Oversight Monthly Update

March 21, 2024, 2:00 p.m. MT



Reliability & Security Oversight Monthly Update

March 21, 2024

Mailee Cook, Training and
Outreach Specialist

WECC Industry Subject Matter Expert (ISME) Application Now Available

Apply Today

[HTTPS://WWW.WECC.ORG/RELIABILITY/ISME%20APPLICATION.PDF](https://www.wecc.org/reliability/isme%20application.pdf)



Enforcement ***FUNDAMENTALS***

March 25, 2024

RELIABILITY & SECURITY

Workshop - Salt Lake City, UT



March 26–27, 2024



RELIABILITY IN THE WEST

A DISCUSSION SERIES



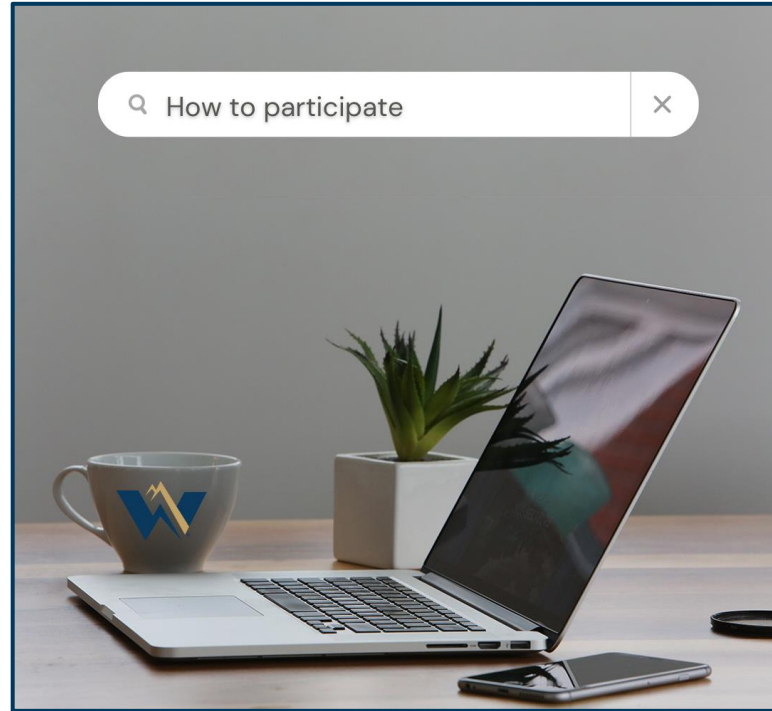
Antitrust Policy

- All WECC meetings are conducted in accordance with the WECC Antitrust Policy and the NERC Antitrust Compliance Guidelines
- All participants must comply with the policy and guidelines
- This meeting is public—confidential or proprietary information should not be discussed in open session

Antitrust Policy

- This webinar is being recorded and will be posted publicly
- By participating, you give your consent for your name, voice, image, and likeness to be included in that recording
- WECC strives to ensure the information presented today is accurate and reflects the views of WECC
- However, all interpretations and positions are subject to change
- If you have any questions, please contact WECC's legal counsel

Participating



Send questions via chat to WECC Meetings
Use the “raise hand” feature

Agenda

- Standards Update
 - Steve Rueckert, Director of Standards, WECC
- Evidence Request Tool V8.1
 - Monica Vela, Cybersecurity Auditor, WECC
- CIP-012 Link Identification
 - Mike Krum, Cybersecurity Auditor, WECC
 - Tom Williams, Entity Monitoring Manager, WECC



R&SO Standards Update

March 21, 2024

Steve Rueckert
Director of Standards

Items Covered

- Current WECC Activities
- Current NERC Activities

Current WECC Projects

- WECC-0142 Retire BAL-002-WECC
 - In abeyance; WSC may terminate
- WECC-0153 Interchange Consolidation Criterion
 - Consolidation of 11 WECC INT Criteria into a single document
 - Drafting complete
 - Will be presented to the WSC with a request to ballot
- WECC-0154 VAR-001-5 Five-year Review
 - Drafting team recommends no changes
 - Informational filing with NERC

WECC Approval Items

- WECC-0147 BAL-004-WECC-3 ATEC
 - Five-year review
 - Minor, non substantive revisions
 - WECC BOD unanimously approved at the March 13, 2024, BOD meeting
 - Will be forwarded to NERC with a request to file with FERC
- WECC-0150 PRC-001-WECC-CRT-3 Governor Droop
 - Five-year review
 - Clarifications to Facilities, Background, and Overview section to address IBR
 - WECC BOD unanimously approved at the March 13, 2024, BOD meeting
 - Will become effective October 1, 2024

NERC Activities

- NERC has roughly 24 active or new projects
- Prioritized as high, medium, or low
 - Projects with FERC-mandated completion dates or NERC BOT directed dates are prioritized as high
- Low and medium projects may not be addressed until 2025 or 2026
- See prioritization on the NERC Standards Under Development page at <https://www.nerc.com/pa/Stand/Pages/Standards-Under-Development.aspx>

Recent NERC Ballots

- Project 2022-03 Energy Assurance with Energy-Constrained Resources
 - Received a weighted 6.08% approval
 - WECC voted negative with comments
 - DT will review comments
- Project 2023-03 Internal Network Security Monitoring
 - Ballot closed March 18, 2024
 - WECC voted affirmative

NERC Events

- NERC SC meeting March 20, 2024
 - Four Action Items
 - Agenda packed; available at:
[https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC Meeeting Agenda March 20 2024.pdf](https://www.nerc.com/comm/SC/Agenda%20Highlights%20and%20Minutes/SC_Meeeting_Agenda_March_20_2024.pdf)
- Project 2023-01 IBR Event Reporting
 - Informal comment period closing March 27, 2024
- Project 2020-06 Verification of Models and Data for Generators Inverter-based Resource-related Definitions
 - Formal comment period and ballot closing April 8, 2024



www.wecc.org



Evidence Request Tool

V8.1

March 21, 2024


Monica Vela

Cybersecurity Auditor

Agenda

- Wait, there's a new ERT version?
- Who and When about ERT updates
- ERT tabs
 - Level 1 tab
 - Level 2 tab
 - TCA and RM tabs
 - BCSI tab
 - Personnel tab
 - Procurement tab

Wait, There's a New ERT Version?



NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

[Account Log-In/Register](#) | [Contact Us](#)

[About NERC](#)
[Career Opportunities](#)
[Governance](#)
[Committees](#)
[Program Areas & Departments](#)
[Standards](#)
[Initiatives](#)
[Reports](#)
[Files](#)

One-Stop Shop (Compliance Monitoring & Enforcement Program)

- Align and Secure Evidence Locker
- Compliance Assurance
- Compliance Guidance
- Compliance Investigations
- Compliance Analysis and Certification
- Compliance Hotline
- ERO Enterprise Program Alignment Process
- Regional Audit Reports of Registered Entities
- Risk-Based Compliance Monitoring and Enforcement Program (CMEP)
- Organization Registration and Organization Certification
- Organization Certification
- Enforcement and Mitigation
- CMEP and Vegetation Reports
- Reliability Standards Audit Worksheet (RSAWs)
- Centralized Organization Registration ERO System (CORES) Technology Project

Home > Program Areas & Departments > Compliance & Enforcement > One-Stop Shop (Compliance Monitoring & Enforcement Program)

One-Stop Shop (Compliance Monitoring & Enforcement Program)

The One-Stop Shop provides a consolidated and sortable listing of the pages located on the left navigation and commonly used documents related to the Compliance Monitoring and Enforcement Program (CMEP).

[ERO Enterprise Guidance: Potential Noncompliance Related to Coronavirus Impacts](#) (May 10, 2021)

[COVID-19 Logging Spreadsheet - Template](#) (May 28, 2020)

[COVID-19 ORC and CMEP Frequently Asked Questions](#) (Updated June 25, 2020)

[FERC, NERC Provide Industry Guidance to Ensure Grid Reliability Amid Potential Coronavirus Impacts](#)

One-Stop-Shop (CMEP, Compliance, and Enforcement) - Active

Documents	Year	Category	Date
Compliance (38)			
CIP ERT & User Guide (3)			
CIP Evidence Request Tool Master v8.1	2024	CIP ERT & User Guide	2/8/2024
CIP Evidence Request Tool Release Notes v8.1	2024	CIP ERT & User Guide	2/8/2024
CIP Evidence Request Tool User Guide v8.1	2024	CIP ERT & User Guide	2/8/2024

Who and When about ERT Updates

- Starting with July audits
- The ERO Enterprise implements major versions annually
 - NERC and Regional Entities such as WECC participate
- NERC Security Working Group (SWG)
 - Industry group
 - Comments and feedback

Level 1 Tab

- Due Date column was hidden—RFI due dates in Align
- Creation of SEL Reference ID is automated

	A	B	C	D	F
1					
2	Detail Tab or Request ID ▼	Standard ▼	Requirement ▼	Initial Evidence Request Required in RSAW and NERC Evidence Request Spreadsheet ▼	SEL Reference ID
20	CIP-002-R1-L1-01	CIP-002-5.1a	R1	Provide the process that was implemented to identify each of the high impact and medium impact BES Cyber Systems, and each asset containing a low impact BES Cyber System. Additionally, provide evidence of the implementation of that process.	,CIP-002-R1-L1-01 CIP-002-5.1a R1

Level 1 Tab

- Updated references from CIP-004-6 and CIP-011-2 to new versions
- Added requests for clarity purposes
 - CIP-008-6: Provide each documented Cybersecurity Incident Response Plan(s) that collectively include each of the requirement parts...
 - CIP-009-6: Provide each documented recovery plan(s) that collectively include each of the requirement parts...
 - CIP-005-R2-L1-04: Provide configuration files for each EAP used for IRA sessions or active vendor remote access sessions.
 - BCSI worksheet description: list of BCSI **groupings** for provisioned access

Level 2 Tab

- Creation of SEL Reference ID is automated

	F	G	I
1	ENTIAL		
2	Sample Set Evidence Request	Sample Set Index Numbers & Data	SEL Reference ID
3	For each BES asset containing a low impact BES Cyber System in Sample Set BES-Assets-L2-01, provide evidence that physical security controls were implemented to control physical access, based on need as determined by entity, to: 1. The asset or the locations of the low impact BES Cyber Systems within the asset; and 2. The Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.	N/A	,CIP-003-R2-L2-01, CIP-003-8 R2

Level 2 Tab

- Request added to CIP-012-R1-L2-01
 - Implementation of security protections

- References to CIP-004-6 and CIP-011-2
 - CIP-004-R6-L2-02
 - CIP-011-R1-L2-01
 - Designated storage locations

Sample Set Evidence Request
For each BES Asset in Sample Set BES-Assets-L2-04, for Real-time Assessment and Real-time monitoring data being transmitted between Control Centers, provide the following evidence: 1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification; 2. Identification of where the Responsible Entity applied security protection for transmitting; 3. Implementation of security protection; and 4. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

Sample Set Evidence Request
For each terminated individual in Sample Set Personnel-L2-06, provide evidence that the individual's access to BCSI was revoked by the end of the next calendar day following the effective date of the termination action.
For each BCSI grouping in Sample Set BCSI-L2-01, provide evidence how the BCSI is protected and securely handled to mitigate risks of compromising confidentiality.

TCA and RM Tabs

- Were changes made during the audit period?
 - Changes in vulnerability management, malicious code detection, or other management processes.

Transient Cyber Assets Managed by the Responsible Entity or by a Party Other Than the Responsible Entity								Sample Count:
Index	TCA ID	TCA Management Typ	Description of Use	Managed by	Asset ID Where Used	Connected at Asset with High/Medium Impact BCS	Connected at Asset with Low Impact BCS	Were changes made during audit period?
1								
2								

Removable Media						Sample Count:
Index	Removable Media ID	Asset ID Where Used	Connected at Asset with High/Medium Impact BCS	Connected at Asset with Low Impact BCS	Description of Use	Were changes made during audit period?
1						
2						

BCSI Tab

BES Cyber System Information Storage Locations				Sample Count:
Index ▼	Designated Storage Location ▼	Impact Rating ▼	Storage Type ▼	
1				
2				

BES Cyber System Information Protection					Sample Count:
Index ▼	BCSI Groupings and Description ▼	Description of Protection Method ▼	BCSI Type ▼	Impact Rating ▼	Were changes made during audit period? ▼
1					
2					

BCSI Tab

	A	B	C	D	E	F	G	H
1			CONFIDENTIAL					or use by Region
2		BES Cyber System Information Protection					Sample Count: 0	
3	Index	BCSI Groupings and Description	Description of Protection Method	BCSI Type	Impact Rating	Were changes made during audit period?	BCSI-L2-01	Random Sampling Process
4	1							
5	2							
6	3							
7	4							
8	5							
9	6							
10	7							
11	8							
12	9							
13	10							
14	11							
15	12							
16	13							
17	14							
18	15							
19	16							
20	17							
21	18							
22	19							

BCSI Type

- Physical
- Electronic - On Premises
- Electronic - Off Premises

Impact Rating

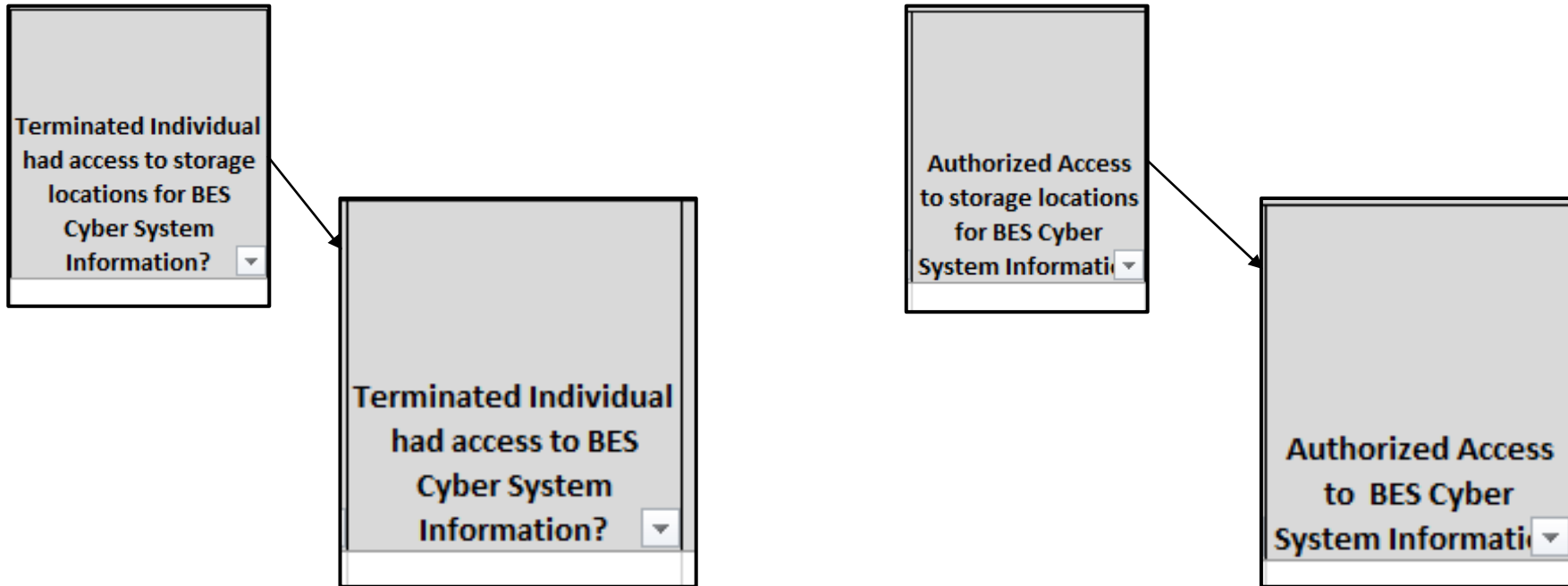
- High
- Medium with ERC
- Medium without ERC

Were changes made during audit period?

- TRUE

Personnel Tab

- “Storage locations” removed



Procurement Tab

- Columns removed
 - Identification & Assessment Start Date
 - Identification & Assessment End Date



Electric Reliability and Security for the West

www.wecc.org



CIP-012 Link Identification

March 21, 2024

Mike Krum, Cybersecurity
Auditory, WECC

Tom Williams, Entity Monitoring
Manager, WECC

Agenda

- CIP-012 functional applicability
- What is Real-time Assessment and Real-time monitoring data (RTA/RTM)?
- Key concepts for CIP-012 link identification
 - Control Centers and associated data centers
 - Entity communication scenarios
 - Alignment with IRO-010 and TOP-003 Standards
 - Joint responsibility
 - Link or control failure and CIP Exceptional Circumstances
- A suggested process for CIP-012 link identification

Functional Applicability

CIP-012 Functional Applicability

4. Applicability:

4.1. Functional Entities: The requirements in this standard apply to the following functional entities, referred to as “Responsible Entities,” that own or operate a Control Center.

4.1.1. Balancing Authority

4.1.2. Generator Operator

4.1.3. Generator Owner

4.1.4. Reliability Coordinator

4.1.5. Transmission Operator

4.1.6. Transmission Owner

CIP-012 is applicable to GO/GOP-only entities, even low impact.

What Is Real-time?

What Is a Real-time Assessment?

What Is Real-time monitoring?

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- 1.1.** Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;
- 1.2.** Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and
- 1.3.** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

What Is Real-time?

- “Present time as opposed to future time. (From Interconnection Reliability Operating Limits standard.)” [*NERC Glossary of Terms*](#)
- The concept of real-time refers to coordination of independent clocks over wide areas to ensure safety, security, and resilience in power systems.
- The “Interconnection Reliability Operating Limits standard” refers to directives in FERC Order No. 693.

Home > Program Areas & Departments > Standards > Archived Reliability Standards Under Development

Archived Reliability Standards Under Development

Projects - Closed
2006-01 System Personnel Training
2006-02 Assess Transmission Future Needs and Develop Transmission Plans
2006-03 System Restoration and Blackstart - EOP-001, EOP-005, EOP-006
2006-04 Back-up Facilities - EOP-008
2006-06 Reliability Coordination - COP-001, COM-002, IRO-001
2006-07 ATC/TTC/AFC and CBM/TRM Revisions
2006-08 Reliability Coordination - Transmission Loading Relief
2007-01 Underfrequency Load Shedding - EOP-003, PRC-006
2007-02 Operating Personnel Communication Protocols - COM-002
2007-03 Real-time Transmission Operations - TOP-001, TOP-002, TOP-003, TOP-004, TOP-005, TOP-006, TOP-007, TOP-008, PER-001
2007-04 Certifying System Operators
2007-05 Balancing Authority Controls
2007-06 System Protection Coordination - PRC-027, Retirement of PRC-001
2007-06.2 Phase 2 of System Protection Coordination - PER-006-1, Retirement of PRC-001
2007-07 Vegetation Management
2007-09 Generator Verification - MOD-025, MOD-026, MOD-027, PRC-024
2007-11 Disturbance Monitoring - PRC-002
2007-12 Frequency Response - BAL-003
2007-14 Coordinate Interchange - Timing Table
2007-17 Protection System Maintenance and Testing - PRC-005
2007-17.2 Protection System Maintenance and Testing - Phase 2 (Reclosing Relays) - PRC-005
2007-17.3 (PRC-005-X) Protection System Maintenance and Testing Phase 3 (Sudden Pressure Relays) - PRC-005
2007-17.4 PRC-005 FERC Order No. 693 Directive - PRC-005 (Maintenance of supervisory devices associated with automatic reclosing)
2020 Periodic Review Standing Review Team - Standards Grading
2021 Periodic Review Standing Review Team - Standards Grading
2022 Periodic Review Standing Review Team - Standards Grading
2018 Bulk Electric System Definition Reference
CIP Standards Efficiency Review
Cost Effectiveness Pilot - TPL-001
Cost Effective Analysis Process (CEAP) for NERC ERO Standards
Order 754
Operate Within Interconnection Reliability Operating Limits
Revisions to the NERC Standards Processes Manual
Standards Efficiency Review
Standard Processes Manual 2010
Standards Processes Manual Revisions to Implement SPIG Recommendations 2013
Technical Rationale for Reliability Standards

Reliability Standards

- One Stop Shop
- US Reliability Standards
- Complete Set of Reliability Standards
- VRF VSL Matrix
- Functional Model
- US Effective Date Status Functional Applicability
- Glossary of Terms

Balloting & Commenting

Reliability Standards Under Development

- Drafting Team Vacancies
- Project Tracking Spreadsheet
- Projected Posting Schedule
- Regional Standards Development
- Reliability Standards Development Plan
- Requests for Interpretations (RFIs)
- Standard Authorization Requests (SARs)

Archived Reliability Standards Under Development

Standards Committee

Webinars

Workshops

Resources

Home > Program Areas & Departments > Standards > Operate Within Interconnection Reliability Operating Limits

Operate Within Interconnection Reliability Operating Limits

Related Files

Status:

Approved by the NERC Board of Trustees on October 17, 2008 and is pending FERC approval.

Purpose/Industry Need:

The purpose of this standard is to prevent instability, uncontrolled separation or cascading outages that adversely impact the reliability of the bulk transmission system.

Draft	Action	Dates	Results	Consideration of Comments
<p>IRO-008-IRO-010</p> <p>EOP-001, IRO-002, IRO-004, IRO-005, TOP-003, TOP-005, TOP-006 Clean Redline to last approval and posting</p> <p>Implementation Plan Clean Redline to last posting</p> <p>FERC Directives in Order 693 Addressed in IROL Implementation Plan</p>	Pending FERC Approval			
<p>IRO-008-IRO-010</p> <p>EOP-001, IRO-002, IRO-004, IRO-005, TOP-003, TOP-005, TOP-006 Clean Redline to last approval and posting</p> <p>Implementation Plan Clean Redline to last posting</p> <p>FERC Directives in Order 693 Addressed in IROL Implementation Plan</p>	<p>Recirculation Ballot</p> <p>Info>></p>	8/12/2008 - 8/21/2008 (closed)	<p>Summary>></p> <p>Full Record: IRO-008-1</p> <p>IRO-009-1</p> <p>IRO-010-1</p>	
<p>Draft 10 Standards IRO-008-010</p> <p>IRO-008-IRO-010 Clean Redline to last posting</p> <p>EOP-001, IRO-002, IRO-004, IRO-005, TOP-003, TOP-005, TOP-006 Clean Redline to last approval</p> <p>Implementation Plan Clean Redline to last posting</p> <p>FERC Directives in Order 693 Addressed in IROL Implementation Plan</p>	<p>Ballot Window</p> <p>Info>></p>	7/21/2008 - 7/30/2008 (closed)	<p>Summary>></p> <p>IRO-008-1 Full Record>> Comments Received>></p> <p>IRO-009-1 Full Record>> Comments Received>></p> <p>IRO-010-1 Full Record>> Comments Received>></p>	<p>IRO-008-1 Consideration of Comments>></p> <p>IRO-009-1 Consideration of Comments>></p> <p>IRO-010-1 Consideration of Ballot Comments>></p>
	Pre-ballot Review Info>>	6/20/2008 - 7/21/2008 (closed)		

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

(Docket No. RM06-16-000; Order No. 693)

Mandatory Reliability Standards for the Bulk-Power System

(Issued March 16, 2007)

AGENCY: Federal Energy Regulatory Commission, DOE.

ACTION: Final Rule.

SUMMARY: Pursuant to section 215 of the Federal Power Act (FPA), the Commission approves 83 of 107 proposed Reliability Standards, six of the eight proposed regional differences, and the Glossary of Terms Used in Reliability Standards developed by the North American Electric Reliability Corporation (NERC), which the Commission has certified as the Electric Reliability Organization (ERO) responsible for developing and enforcing mandatory Reliability Standards. Those Reliability Standards meet the requirements of section 215 of the FPA and Part 39 of the Commission's regulations. However, although we believe it is in the public interest to make these Reliability Standards mandatory and enforceable, we also find that much work remains to be done. Specifically, we believe that many of these Reliability Standards require significant improvement to address, among other things, the recommendations of the Blackout Report. Therefore, pursuant to section 215(d)(5), we require the ERO to submit significant improvements to 56 of the 83 Reliability Standards that are being approved as mandatory and enforceable. The remaining 24 Reliability Standards will remain pending at the Commission until further information is provided.

The Final Rule adds a new part to the Commission's regulations, which states that this part applies to all users, owners and operators of the Bulk-Power System within the United States (other than Alaska or Hawaii) and requires that each Reliability Standard identify the subset of users, owners and operators to which that particular Reliability Standard applies. The new regulations also require that each Reliability Standard that is approved by the Commission will be maintained on the ERO's Internet website for public inspection.

NOTE: The following appendices will not be published in the Code of Federal Regulations.

Appendix A
Disposition of Standards,
Glossary and Regional Differences

Reliability Standard	Title	Proposed Disposition
BAL-001-0	Real Power Balancing Control Performance	Approve
BAL-002-0	Disturbance Control Performance	Approve; direct modification
BAL-003-0	Frequency Response and Bias	Approve; direct modification
BAL-004-0	Time Error Correction	Approve; direct modification
BAL-005-0	Automatic Generation Control	Approve; direct modification
BAL-006-1	Inadvertent Interchange	Approve; direct modification
CIP-001-1	Sabotage Reporting	Approve; direct modification
COM-001-1	Telecommunications	Approve; direct modification
COM-002-2	Communications and Coordination	Approve; direct modification
EOP-001-0	Emergency Operations Planning	Approve; direct modification
EOP-002-2	Capacity and Energy Emergencies	Approve; direct modification
EOP-003-1	Load Shedding Plans	Approve; direct modification
EOP-004-1	Disturbance Reporting	Approve; direct modification
EOP-005-1	System Restoration Plans	Approve; direct modification
EOP-006-1	Reliability Coordination - System Restoration	Approve; direct modification
EOP-007-0	Establish, Maintain, and Document a Regional Blackstart Capability Plan	Pending
EOP-008-0	Plans for Loss of Control Center Functionality	Approve; direct modification
EOP-009-0	Documentation of Blackstart Generating Unit Test Results	Approve
FAC-001-0	Facility Connection Requirements	Approve
FAC-002-0	Coordination of Plans for New Facilities	Approve; direct modification
FAC-003-1	Transmission Vegetation Management Program	Approve; direct modification
FAC-004-0	Methodologies for Determining Electrical Facility Ratings	Withdrawn
FAC-005-0	Electrical Facility Ratings for System Modeling	Withdrawn
FAC-008-1	Facility Ratings Methodology	Approve; direct modification
FAC-009-1	Establish and Communicate Facility Ratings	Approve
FAC-012-1	Transfer Capabilities Methodology	Pending

Relevant Definitions Proposed in 2008

Term	Proposed Definition	In NERC GOT
Real-time	Present time as opposed to future time.	Yes
Real-time Assessment	An examination of existing and expected system conditions, conducted by collecting and reviewing immediately available data.	Yes (but much longer)
Real-time Data	Real-time measured values, state estimator values derived from the measured values, or other calculated values derived from the measured values—may include directly monitored data, inter-utility data exchange (e.g., Interconnection Control Area Communication Protocol or SCADA Data), and manually collected data.	No
Real-time Monitoring	The act of scanning data and drawing conclusions about what the data indicates.	No

[Definitions posted with ballot of Operate within Interconnection Reliability Operating Limits Standard](#)

Real-time Assessment

- “An evaluation of system conditions using Real-time data to assess existing (pre-Contingency) and potential (post-Contingency) operating conditions. The assessment shall reflect applicable inputs including, but not limited to load; generation output levels; known Protection System and Remedial Action Scheme status or degradation, functions, and limitations; Transmission outages; generator outages; Interchange; Facility Ratings; and identified phase angle and equipment limitations. (Real-time Assessment may be provided through internal systems or through third-party services.)” [*NERC Glossary of Terms*](#)

Operate Within Interconnection Reliability Operating Limits Standard

These definitions will be posted and balloted along with the standard, but will not be restated in the standard. Instead, they will be included in a separate “Definitions” section containing definitions relevant to all standards that NERC develops.

Definitions

Bulk Electric System: A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and bulk transmission system.

Cascading Outages: The uncontrolled successive loss of system elements triggered by an incident at any location.

Generator Owner: The entity that owns the generator.

Instability: The inability of the transmission system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances.

Interconnection Reliability Operating Limit: A system operating limit which, if exceeded, could lead to instability, uncontrolled separation, or cascading outages that adversely impact the reliability of the bulk transmission system.

Interconnection Reliability Operating Limits Standard: An instrument of transmission

generation outages, and equipment limitations.

Real-time: Present time as opposed to future time.

Real-time Assessment: An examination of existing and expected system conditions, conducted by collecting and reviewing immediately available data.

Real-time Data: Real-time measured values, state estimator values derived from the measured values, or other calculated values derived from the measured values — may include directly monitored data, Inter-utility data exchange (e.g., Interconnection Control Area Communication Protocol or SCADA Data), and manually collected data.

Real-time Monitoring: The act of scanning data and drawing conclusions about what the data indicates.

Alignment with TOP-003 and IRO-010 Standards

What Types of Data Are Applicable?

The phrase “Real-time Assessment and Real-time monitoring data” comes from the IRO-010 and TOP-003 Standards

“Each [Reliability Coordinator / Transmission Operator] shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments.”

Such data would typically include Real-time data exchanged with a Reliability Coordinator, Balancing Authority, or with your backup / alternate / secondary Control Center

CIP-012-1 Technical Rationale

Alignment with IRO and TOP standards

The SDT recognized the FERC reference to additional Reliability Standards and the responsibilities to protect the applicable data in accordance with [NERC Reliability Standards TOP-003 and IRO-010](#). The SDT used these references to drive the identification of sensitive BES data and chose to base the CIP-012-1 requirements on the Real-time data

² [NIST Special Publication 800-53A, Revision 4](#), page B-3

³ [NIST Special Publication 800-53A, Revision 4](#), page B-6

Requirement R1

specification elements in these standards. This approach provides consistent scoping of identified data, and does not require each entity to devise its own list or inventory of this data. Many entities are required to provide this data under agreements executed with their RC, BA or TOP. [Data requiring protection in CIP-012-1 consists of a subset of data that is identified by the RC, BA, and TOP in the TOP-003 and IRO-010 data specification standards, limited to Real-time Assessment data and Real-time monitoring data.](#) CIP-012-1 excludes other data typically transferred between Control Centers such as Operational Planning Analysis data, weather data, market data, and other data that is not used by the RC, BA, and TOP to perform Real-time reliability assessments and analysis identified in TOP-003 and IRO-010. The SDT determined that Operational Planning Analysis data, if rendered unavailable, degraded, or misused, would not adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise as detailed in CIP-002- 5.1a. The SDT notes that there may be special instances during which Real-time Assessment or Real-time monitoring data is not identified by the RC, BA, or TOP. This would include data that may be exchanged between a Responsible Entity's primary and backup Control Center.

Evidence of RTA/RTM Analysis

- Auditors expect to see your entity's analysis of RTA/RTM data
- A common evidence artifact for inter-entity transmission of RTA/RTM is an annotated TOP-003 data specification
- The CIP-012 plan, or a related document, should include the RTA/RTM analysis
 - Functional applicability should drive whether your entity has a CIP-012 plan, even if your entity does not have a Control Center that communicates with another Control Center
 - The conclusion of the CIP-012 plan might be that your entity does not communicate RTA/RTM to another Control Center

Control Centers Associated Data Centers Entity Communication Scenarios

Control Centers and Associated Data Centers

- The definition of Control Center in the NERC Glossary of Terms is among four pages of definitions that came out of Project 2008-06 for version 5 of the CIP Standards related to FERC Order No. 791
- The network link between a Control Center and a geographically separate associated data center could also be applicable to CIP-012

October 26, 2012

Page 1 of 4

CIP Exceptional Circumstance

A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

CIP Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011.

Control Center

One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.

Cyber Assets

Programmable electronic devices, and communication networks including the

CIP-002 and Real-time—or is it real-time?

Real-time Operations

One characteristic of the BES Cyber Asset is a real-time scoping characteristic. The time horizon that is significant for BES Cyber Systems and BES Cyber Assets subject to the application of these Version 5 CIP Cyber Security Standards is defined as that which is material to real-time operations for the reliable operation of the BES. To provide a better defined time horizon than “Real-time,” BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise. This time window must not include in its consideration the activation of redundant BES Cyber Assets or BES Cyber Systems: from the cyber security standpoint, redundancy does not mitigate cyber security vulnerabilities.

CIP-012 Communication Scenarios

- Intra-Entity
 - Control Centers are owned or operated by a single entity
- Inter-Entity
 - Control Centers are owned or operated by different entities
 - Over a private network
 - Over a third-party network
- Inter-Regional
 - Control Centers are in different NERC Regions over any network

Keys to CIP-012 Link Identification

- Identification of Control Centers (yours and others')
- Identification of RTA/RTM
- Identification of network links transmitting RTA/RTM
 - WECC has seen CIP-012 controls in three main areas:
 - Link encryption (data in motion)
 - Physical controls (PSPs or PSP-like rooms)
 - Logical controls (monitor, detect, alert, and respond to potential compromises of the confidentiality and integrity of RTA/RTM)
 - WECC has not seen at audit use of the Secure ICCP protocol ([IEC TS 62351-4](#))

Joint Responsibility

- For inter-entity communication between Control Centers, each entity is responsible for the part of the link it can control
- A third party providing network transport among entities does not release entities of responsibility for documenting R1.3
- A contract or MOU with “the other side” is not required

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

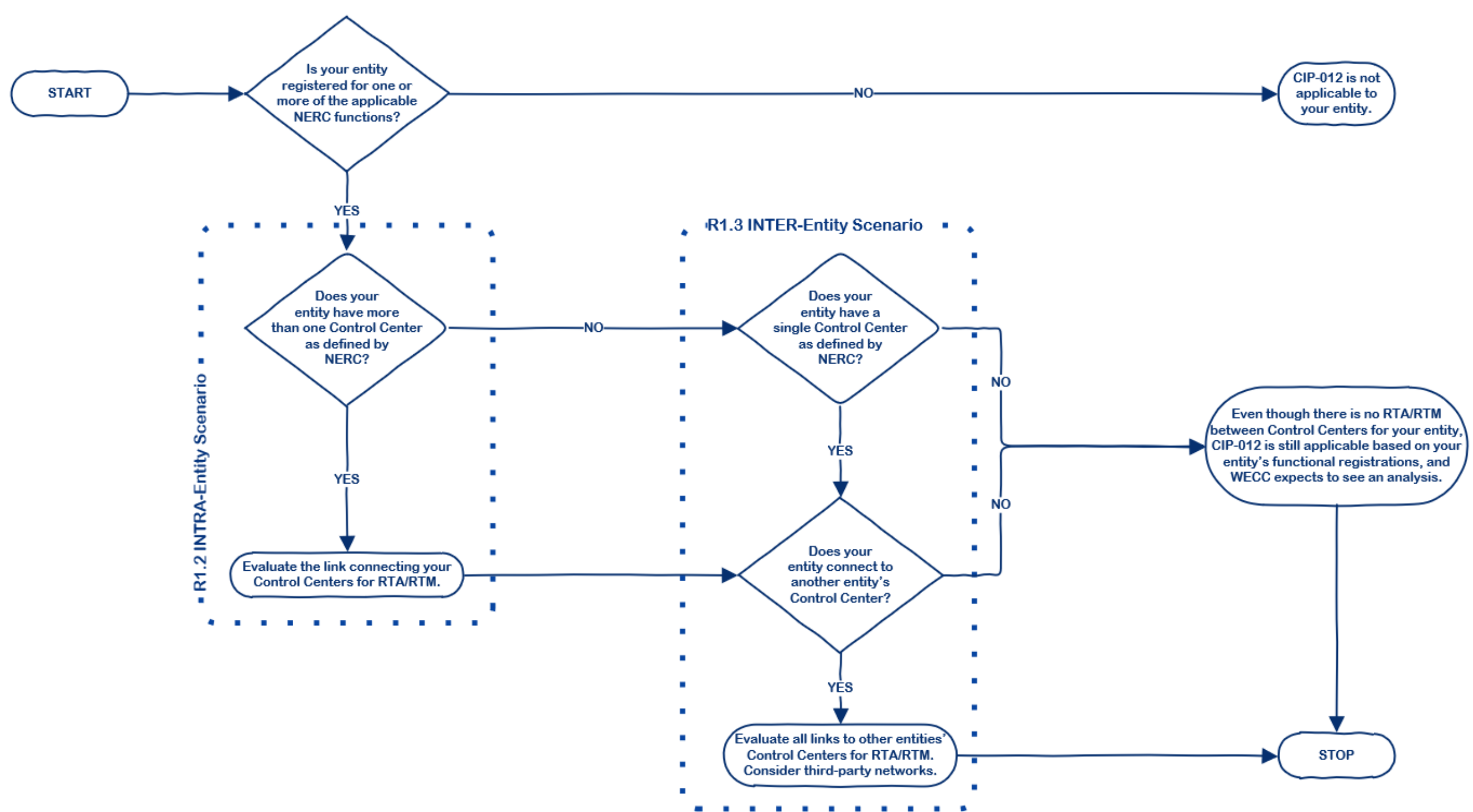
CIP Exceptional Circumstance

- Also defined in Project 2008-06, a CIP Exceptional Circumstance is “a situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.”

CIP Exceptional Circumstance and CIP-012

- How could a CIP Exceptional Circumstance apply to CIP-012?
 - Failure of a control that your entity's plan requires to meet the security objective of CIP-012
 - For example, if your entity's CIP-012 plan documents link encryption as a required control, and link encryption were to fail due to hardware, software, or equipment failure, your entity could declare a CIP Exceptional Circumstance
- Therefore, identification of your entity's CIP-012 links is a prerequisite for monitoring, which is a prerequisite for being alerted about a "link down" status or "encryption failed" status that could trigger a CIP Exceptional Circumstance

Suggested Process for CIP-012 Link Identification





Electric Reliability and Security for the West

www.wecc.org



RELIABILITY & SECURITY

Oversight Monthly Update

April 18, 2024, 2:00 p.m. MT



Follow and engage!
@weccreliability