NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-014 Initial Compliance Monitoring Plan

Steven Noess, Director of Compliance Assurance
Compliance Committee Meeting
November 4, 2015

RELIABILITY | ACCOUNTABILITY




ERO to Monitor Implementation

- **Number of assets critical under the standard**
- **Defining characteristics of the assets identified as critical**
- Scope of security plans
- Timelines for implementing security and resiliency measures
- **Industry's progress in implementing the standard**

2016 Compliance Monitoring

- Assessing and supporting effective implementation
- 2016 Focus to confirm:
  - Registered entities the Reliability Standard is applicable to
  - Whether applicable registered entities performed a required risk assessment to determine whether they have critical facilities, and
  - Whether the registered entities identified critical facilities
- Includes analysis to understand:
  - Why certain stations or substations are identified
  - Why certain stations or substations were not identified
  - What are the defining characteristics of critical stations and substations
  - Qualifications of third party reviewers and how they ensure effective verification

Timing and Approach: Identifying Critical Facilities

- ERO Enterprise-wide self-certification for CIP-014 requirements for identification of critical assets
  - Conducted by each Regional Entity
  - Offsite activity
  - Supports monitoring of effective implementation
  - Tailored and limited:
    - Is the standard applicable?
    - If so, did the registered entity complete the risk assessment/verification requirements?
    - Did the risk assessment result in critical assets?
    - If so, how many?
    - Was notice to a Transmission Operator required for a primary control center?

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Timing and Approach: Identifying Critical Facilities

- Self-certification timing
  - November 2015: Communicated in CMEP Implementation Plan
  - March 15, 2016: Notice to all TOs, including request for answers to the limited questions
  - May 1, 2016: Information due from all TOs
- FERC Audits in 2016
  - In coordination with the ERO Enterprise
  - Minimize duplication of efforts
- Additional compliance monitoring activities for selected registered entities based on risk and follow-on analysis

Timing and Approach: Security Plans

- Transition to assessing Security Plans (R5)
  - Q3/Q4 2016 and 2017
  - Informed by understanding of critical facility identification
- Informal Registered Entity site visits to share progress
  - Already underway: NERC and Regional Entity coordination
  - Focused on security plan effectiveness

Industry's Progress: Early Indications

- Remarkable progress
- Physical security plans focused on mitigating risks from specific threats
- Commitment to purpose of the standard very encouraging to the ERO Enterprise
- Coordination and outreach from 2015 to inform 2016 approach
  - Regional Entity workshops
  - Collaboration with industry groups on guidance as necessary
  - Critical Infrastructure Protection Committee working groups
  - Webinars

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

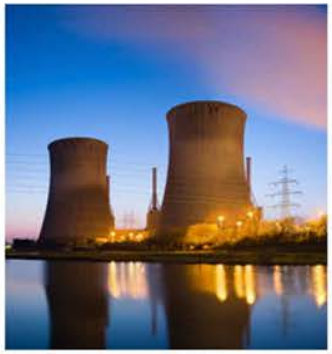
CIP V5 Initial Compliance Monitoring Plan

Steven Noess, Director of Compliance Assurance

Compliance Committee Meeting

November 4, 2015

RELIABILITY | ACCOUNTABILITY

Background

- Enforcement date (High and Medium Impact): April 1, 2016
  - Risk-based compliance monitoring plan for 2016 for High and Medium Impact requirements
  - Concerted outreach on Low Impact requirements for 2017 and 2018

CIP V5 Activities in 2015

- Small Group Advisory Sessions
  - 6 sessions completed in 2015
  - Evaluating lessons to apply to Low Impact in 2016
- Security Reliability Program (SRP) meetings
  - 12 SRPs complete or scheduled for completion in 2015 (including 4 regional workshops impacting several registered entities)
- CIP Workshops and Curriculum
  - Includes calendar of outreach activities from all Regions
  - Archived presentations and webinar recordings
- Reliability Standard Audit Worksheets completed
- Guidance documents posted for comment
  - Lessons Learned and FAQs
  - Section 11 status under Standard Processes Manual

Progress on CIP V5 Transition Program

- Over 45 Lessons Learned & FAQs have been posted for industry comment
- Consensus via the Section 11 Process
- All topics from July 1 way forward meeting addressed and drafts posted:
  - Programmable Electronic Device
  - Impact rating for generation interconnection facilities
  - Third-party notifications for certain impact rating criteria
  - Network devices and external routable connectivity
  - Functional obligations of Control Centers

2016 Compliance Monitoring Approach

- Confirm effective CIP-002 identifications based on impact rating criteria (high and medium focus)
- Focused Audits in 2016
  - ROP required 3-year audits for RC, BA, and TOPs
  - Coordination with FERC on certain audits
- Risk-based approach to timing and scope

Highlights

Risk-Based approach to timing and scope

3-year audits scheduled for 2016

FERC coordination

CIP-002 Identifications: the **foundation**

Goals of 2016 approach

- Understand program effectiveness and support transition
  - Registered entity approaches
  - Program and general controls discussions
  - Limited sampling or testing for effectiveness based on risk
- Identify successes and challenges
- Tailored to appropriate risks

All Registered Entities Subject to CIP Standards

- ERO Enterprise-wide self-certification for CIP-002 identifications
  - Conducted by each region
  - Offsite activity
  - Supports understanding of continent-wide identifications and progress under CIP-002
  - Tailored and limited:
    - Straightforward table format
    - Number and type of assets with corresponding high, medium, and low impact rating criteria
  - Timing
    - November 2015: Communicated in CMEP Implementation Plan
    - February 1, 2016: Notice to all applicable entities, including the table accompanying the self-certification
    - May 1, 2016: Information due from all entities

2016 Audits and Spot Checks

- Scheduled audits based on ROP requirements (3-year entities)
- Tailored scope
  - Based on risk (identified in 2016 CMEP Implementation Plan (IP))
    - CIP-002 R1 and R2
    - CIP-005 R1 and R2
    - CIP-006 R1, R2 and R3
    - CIP-007 R1, R2, R3 and R5
  - Informed by Inherent Risk Assessment
- FERC Led Audits
  - In coordination with the ERO Enterprise
  - Minimize duplication of efforts
- Additional compliance monitoring activities for selected registered entities based on risk and follow-on analysis

Transition to 2017 Compliance Monitoring Approach

- Risk-based and considers the type of entity (Type 1, 2 or 3)
- 2016 activities support identification of entity-specific risk

Type 1 "New High and Medium"	Type 2 "Limited V3-V5 Scope Change"	Type 3 "Large Entity with High, Med, Low"	Type 4 "Small Entity w/Low"
Control Centers Substations Generation	Primarily Control Centers	Control Centers Substations Generation	Small Substation & Gen Mix
No V3 compliance history	Significant V3 History	Significant V3 History	No V3 Compliance History
<40 Entities	<50 Entities	<50 Entities	>1000 Entities

Low Impact Requirements

- Effective in 2017 and 2018
- Outreach informed by 2015 transition program and 2016 compliance monitoring activities, focused on Type 4 registered entities and risk
  - Small Group Advisory Sessions
  - Workshops, webinars, and other education
  - Coordination with trades

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Enforcement Metrics, Risk, and Reliability

Terry Bilke, Midcontinent Independent System Operator, Inc.
Sonia Mendonça, VP of Enforcement and Deputy General Counsel
Compliance Committee Meeting
November 4, 2015

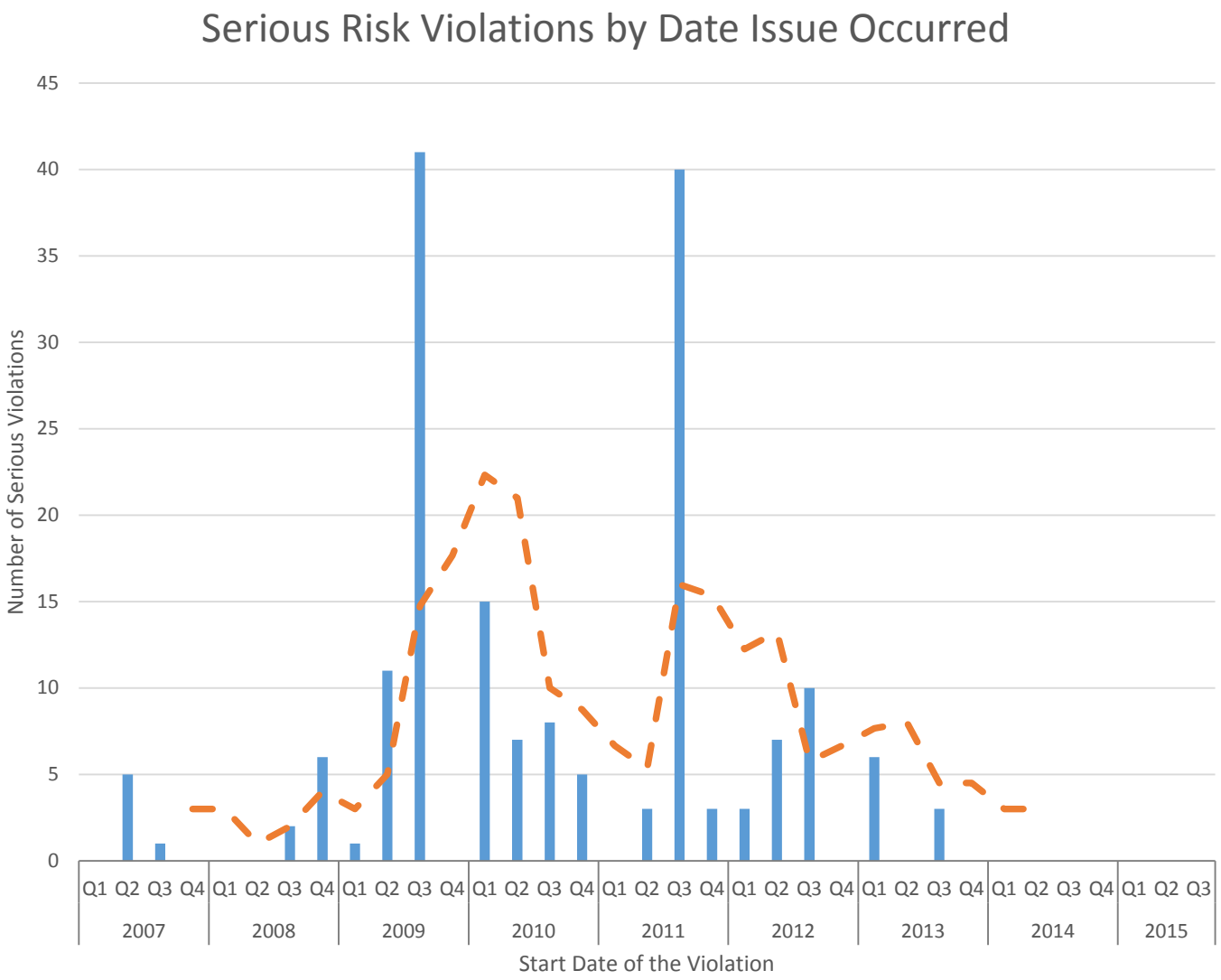
RELIABILITY | ACCOUNTABILITY




RISC Request

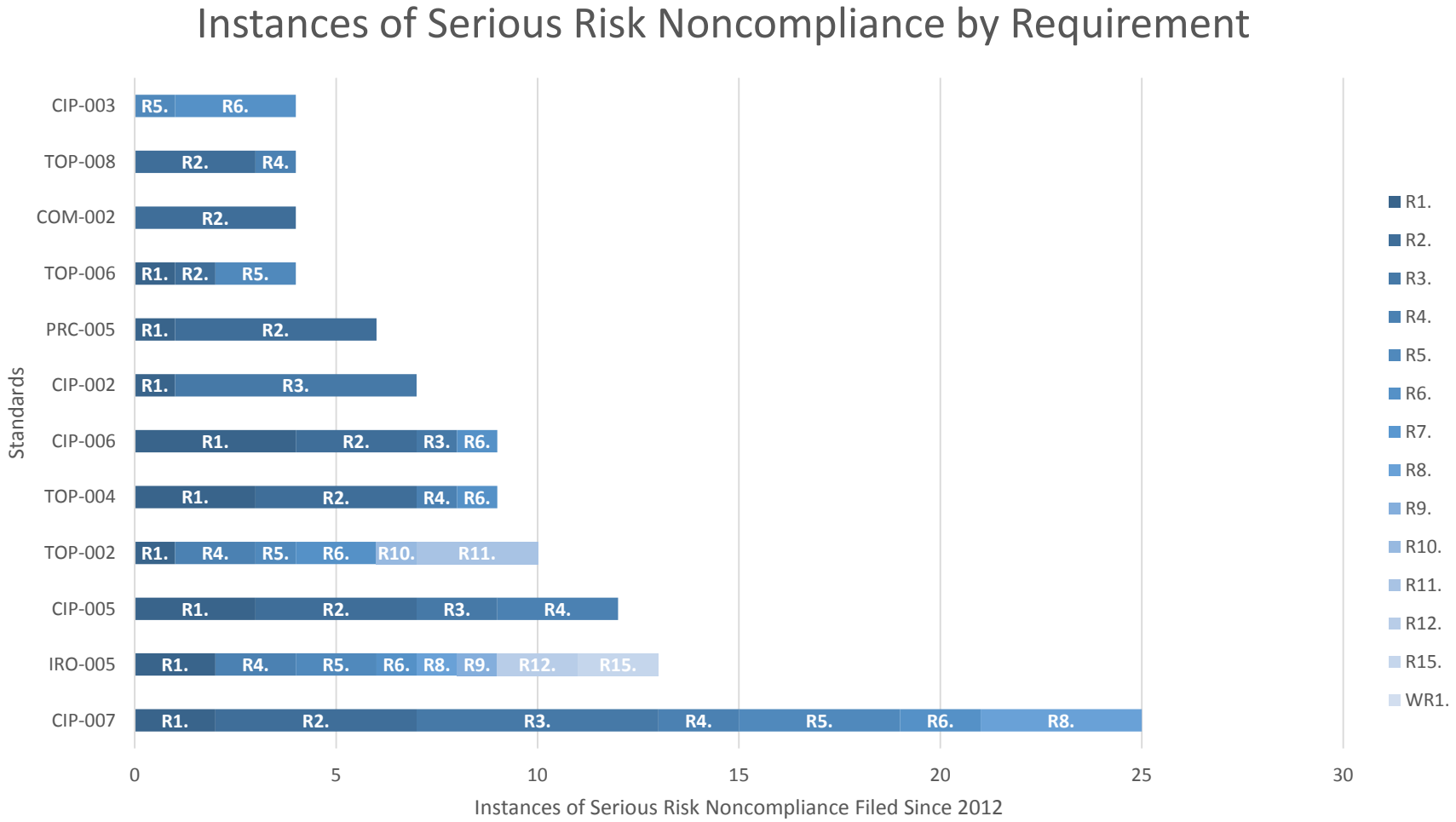
- NERC RISC asked the CCC for input on managing reliability risk by leveraging compliance data
- CCC-led team developed 2 high-level metrics
  - CP-1 (Count of Serious Risk Violations by quarter of occurrence)
  - CP-2 (Count of “Impactful” Violations by quarter of occurrence)

CP-1 (Serious Risk Violations by Quarter)

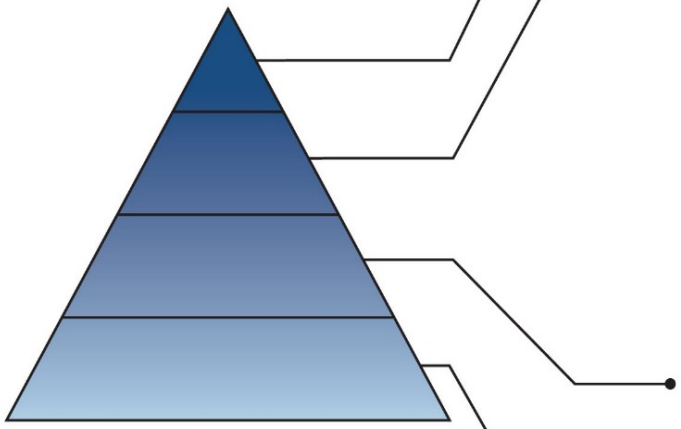


About 3% of the 5,000+ violations processed since 2012 were deemed Serious Risk

Top Serious Risk Violations



CP-2 Data Collection



There was a violation or PV **and** it led to:

Tier 3: Major BES Disturbances

- Caused or contributed to a major BES disturbance

Tier 2: Moderate Impact

- IROL exceeded
- BES limit (non-IROL SOL, frequency, voltage, or ACE) exceeded for > 30 minutes
- BES facilities tripped unexpectedly
- Emergency action taken (e.g., reconfiguration, load shed) to mitigate or prevent the impact of the violation
- Equipment damage
- Major (> 50%) loss of visibility, control, state estimation, or contigency analysis for over 30 minutes

Tier 1: Minor Impact

- Observations similar to those in in tier 2 but of lesser magnitude
- Loss of ability to monitor cybersecurity intrusions

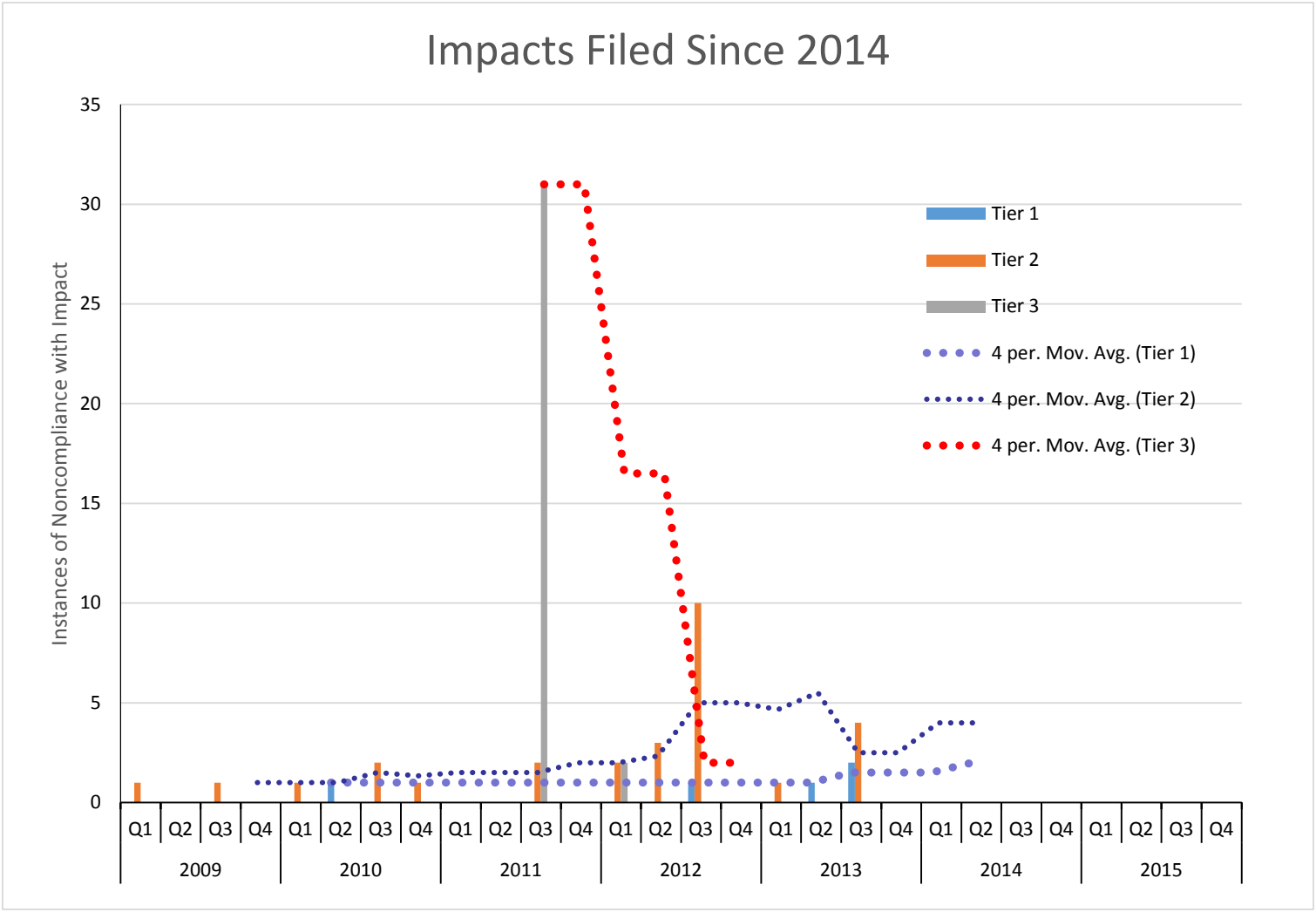
Tier 0: No Impact

- No observed impact

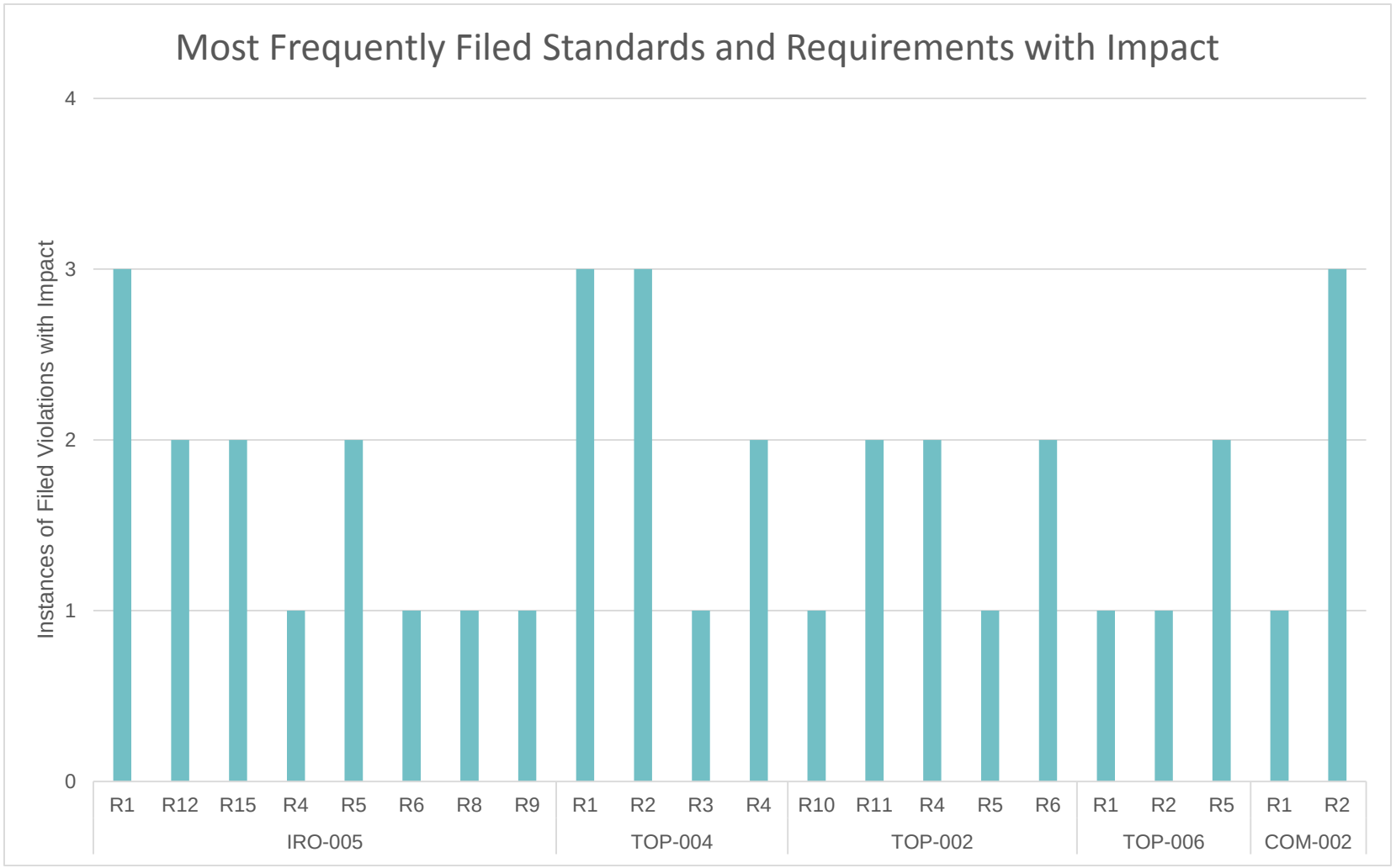
To reduce the # and magnitude of these

Find and Fix these

Violations with Impact



Impactful Requirements



Recommendations (NERC)

- Establish the CP-1 and CP-2 data streams and associated “Top 20” lists and share root causes and lessons learned
- Metrics to be considered in future RISC reports
- Use the CP-1 and CP-2 data as input to the CMEP Implementation Plan’s Risk Elements and Focus Areas
- Establish goals and approaches to encourage a culture of self-detection, self-correction, and self-reporting

Recommendations (Registered Entities)

- Consider the “Top 20” lists as focus areas for the development of internal controls
  - Serious Risk (CP-1) Requirements
  - Impactful Requirements (CP-2)
  - Most violated Requirements
- Pursue self-logging capability and aggressively self-inspect and self-correct
- Capture underlying causes and actions taken to correct compliance exceptions

Thanks to Team Members

- Aaron Hornick (NERC)
- Barb Kedrowski (NERC CCC)
- Ed Kichline (NERC)
- Gizelle Wray (NERC)
- Heide Caswell (NERC PAS)
- Howard Gugel (NERC)
- James Stanton (NERC CCC)
- Margaret Pate (NERC)
- Matthew Varghese (NERC)
- Melinda Montgomery (NERC PAS)
- Michael DeLoach (NERC CCC)
- Paul Kure (NERC PAS)
- Peter Raia (NERC)
- Stanley Kopman (NPCC)
- Terry Bilke (NERC CCC)

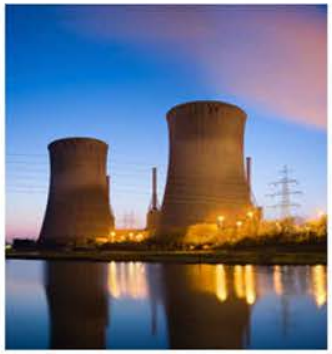
Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Implementation of the Risk-Based Compliance Monitoring and Enforcement Program

Lane Lanford, President and CEO, Texas Reliability Entity, Inc.
Steven Noess, Director of Compliance Assurance, NERC
Sonia Mendonça, Vice President of Enforcement and Deputy General Counsel
Compliance Committee Meeting
November 4, 2015

RELIABILITY | ACCOUNTABILITY

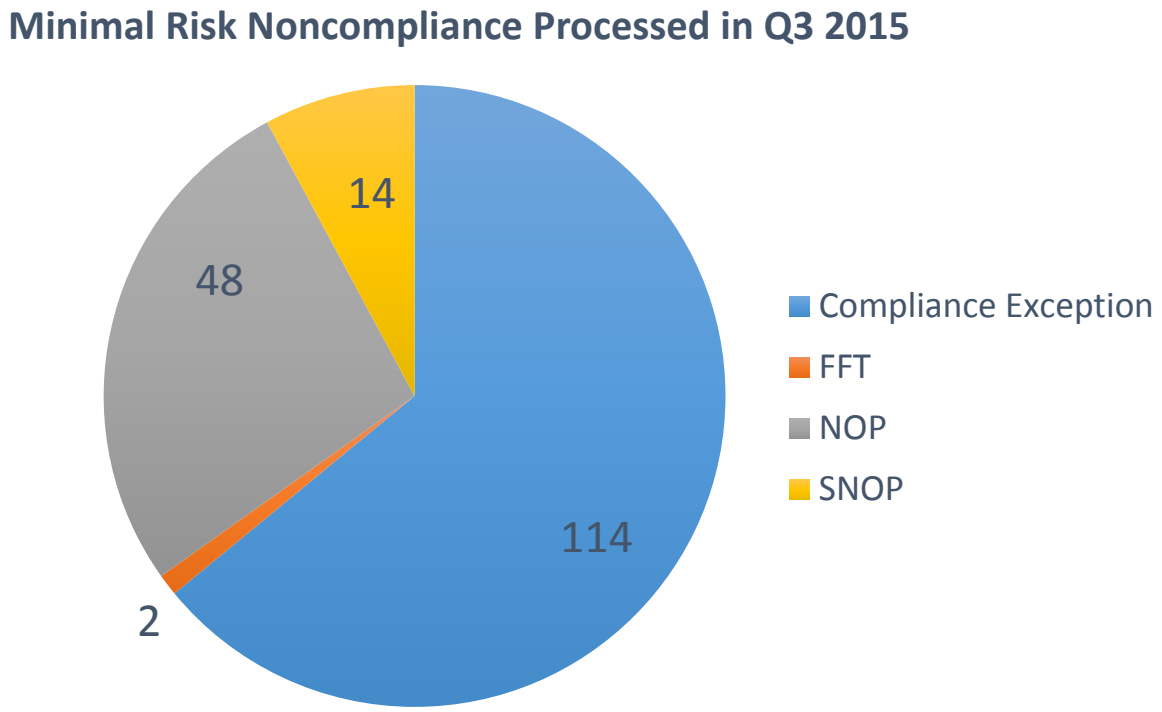



Progress on Risk-based CMEP Implementation

- Progress
  - Risk-based design informs all compliance monitoring and enforcement of ERO Enterprise
  - Transition away from scheduled based compliance monitoring to risk-based compliance monitoring
- Highlights
  - Completion of IRAs for all audits on the 2015 audit schedule
  - Tailored audit scopes and other compliance monitoring for registered entities based on risk

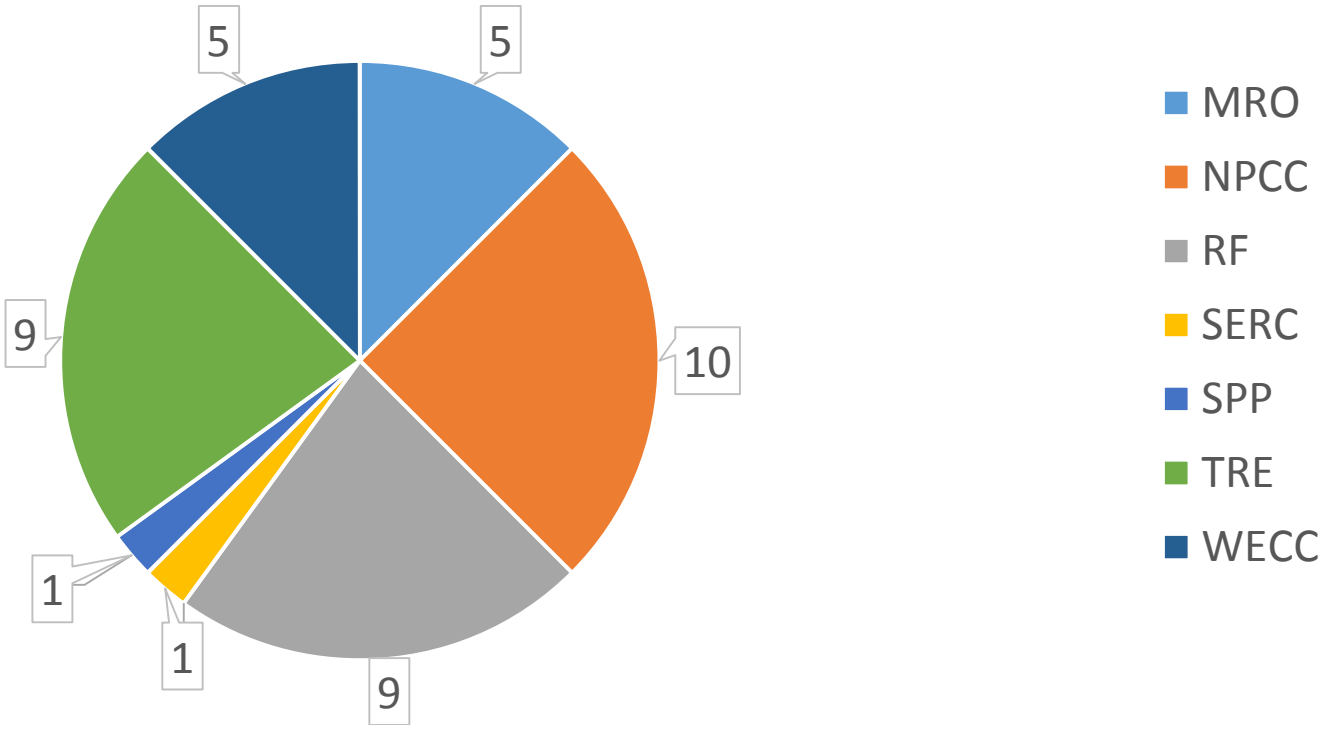
Progress on Risk-based CMEP Implementation

- Highlights (continued)
  - Compliance exceptions account for over 64% of all minimal risk noncompliance dispositions.



Progress on Risk-based CMEP Implementation

- Highlights (continued)
  - The self-logging program covers 40 registered entities and all reliability functions.



Where We Are Today

- Supporting shift to risk-based compliance monitoring

Training and Professional Development

- Refined training program for ERO Enterprise staff
  - Identified risk-based tasks and responsibilities
  - Assessed current competencies and skillsets
- Continued development and tailoring of training and education based on role to help strengthen competencies and capabilities
  - Shape training on role specific needs
  - Determine appropriate delivery methods for training

Collaboration and Sharing of Best Practices and Lessons Learned

- Refinement of risk elements to better prioritize risks
  - Continued review and incorporation of emerging risks for focus
- Collaboration through NERC and Regional Entity working groups
  - Emphasized importance of sharing best practices to achieve successful implementation
- Sharing of best practices for assessing entity risks
  - Identified opportunities for consistency and commons approaches

Looking Ahead to 2016

- Develop schedule for conducting IRA activities of all registered entities
- Build upon lessons learned during 2015 implementation
- Continue NERC and Regional Entities coordination on:
  - Evaluating ERO Enterprise IRA and ICE business rules
  - Promoting consistency in ERO Enterprise IRA and ICE tools and processes
  - Improving training on IRA and ICE performance for ERO Enterprise staff
- Continue emphasis on stakeholder understanding and perceptions

Looking Ahead to 2016

- Coordinated review of compliance exceptions and FFTs with FERC
- Review of self-logging process
- Annual CMEP Report reviewing implementation year

Questions and Answers