NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Critical Infrastructure Protection Violation Themes

Ken McIntyre, North American Electric Reliability Corporation
Deandra Williams-Lewis, ReliabilityFirst
Holly Hawkins, SERC Reliability Corporation
Dave Godfrey, Western Electricity Coordinating Council

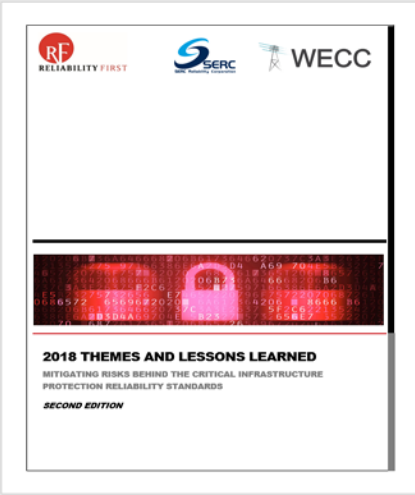
Compliance Committee Meeting
May 9, 2018

RELIABILITY | ACCOUNTABILITY

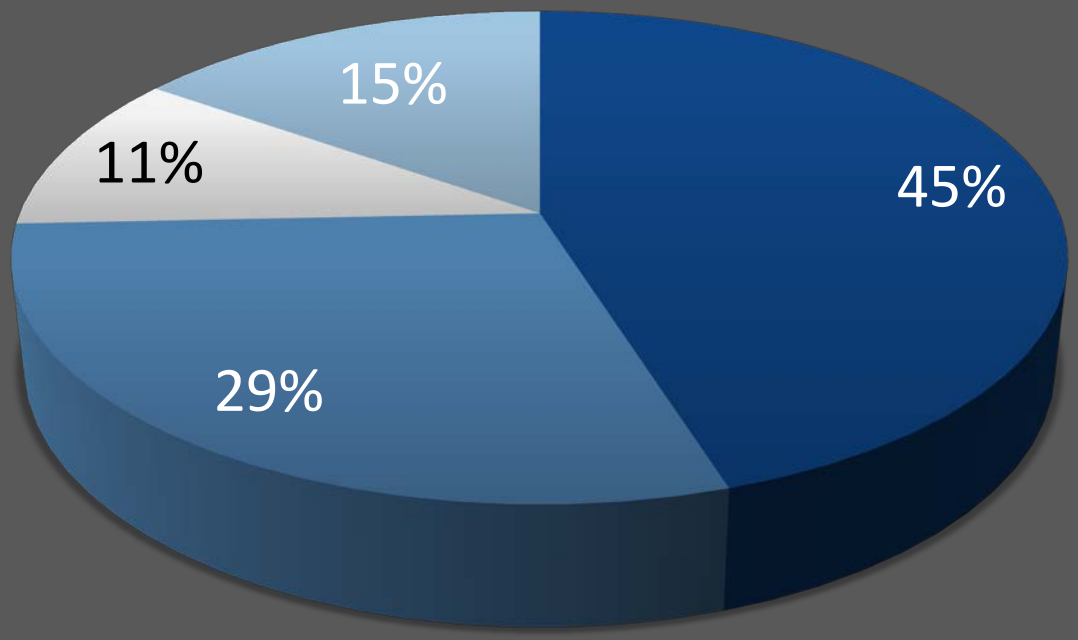



2018 CIP Themes Report

- Purpose
  - Lessons Learned
    - Identify themes in violations of the Critical Infrastructure Protection (CIP) Standards
    - Suggest potential resolutions
- Collaboration
  - RF, WECC, and SERC worked with registered entities to identify the themes and resolutions
- Second Edition
  - First edition in 2015



CIP Themes



Disassociation
Organizational Silos
Inadequate Tools
Lack of Awareness

* *The graph represents the violations that concern the more significant CIP compliance program deficiencies.*

Theme - Awareness

- Lack of awareness of entity's capabilities, deficiencies, systems, and processes
- Recurring Causes
  - Lack of vigilance
  - Insufficient expertise
  - Inadequate root cause analysis
  - Lack of engagement with regulator

Theme-Awareness Example

Failure to verify

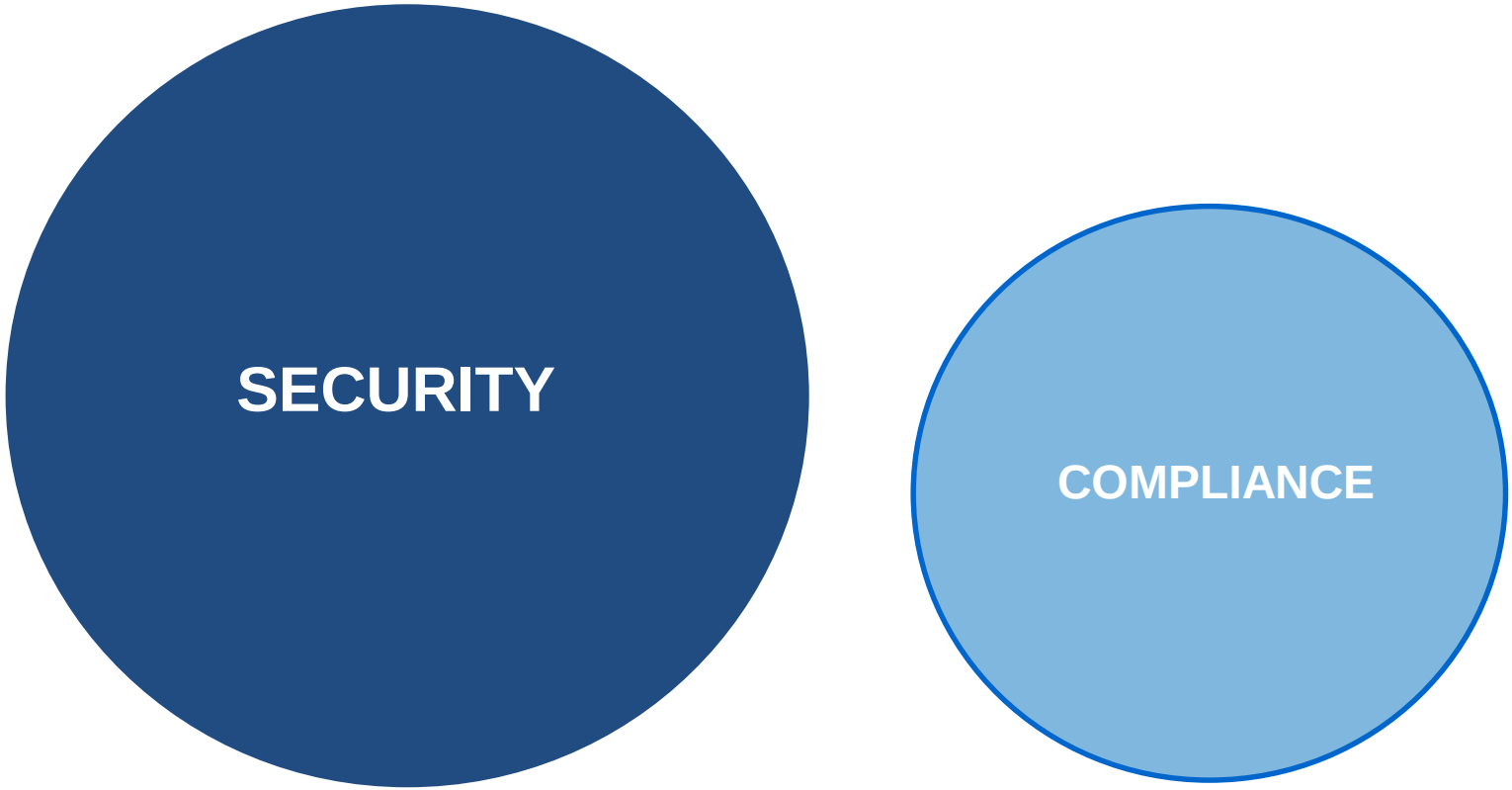
- Entity advanced in terms of security practices
- Entity assumed its program was working as intended in certain business areas
- Patch management program in those areas suffered.

Improvement

- Entity focused on evaluating the quality of their reliability activities
- Leveraged cross-functional teams to ensure consistency in implementation

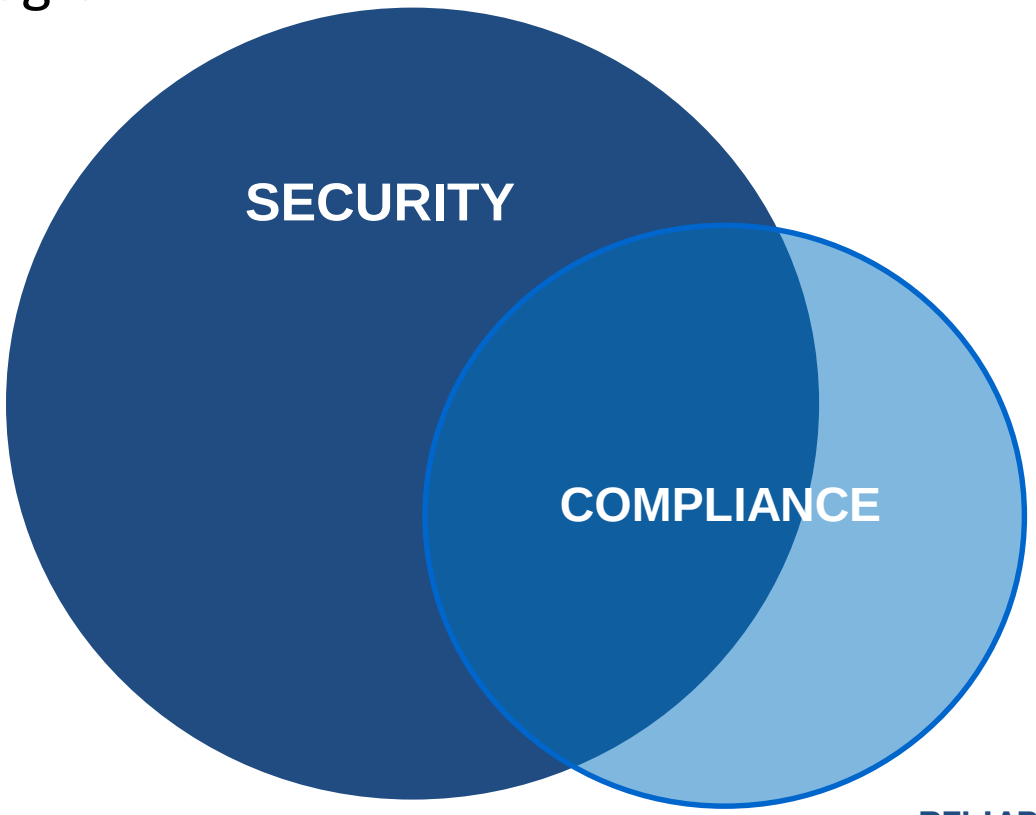
Theme - Disassociation

- Disassociating compliance from security by extension and reliability, resulting in diminished value or emphasis on compliance



Theme - Disassociation

- Compliance is the baseline level of what a registered entity needs to do to maintain security.
- Compliance should be a byproduct of an effectively implemented security program.



Theme - Disassociation Example

Root Causes

- CIP-014 -2 physical security delegated and overseen by facilities or operations personnel
- Use of minimal security measures and accepting risk

Actions Taken

- Outreach and education with entities
- Executive management is getting engaged to understand the scope of the issue
- Additional Transmission studies will be performed
- Create cross functional team to ensure that threats and vulnerabilities

Theme – Inadequate Tools

- Inadequate tools, ineffective use of tools, and overreliance on automation

Theme – Inadequate Tools Example

Systemic Issues

- Improperly configured intrusion detection system and firewall rules
- Over-reliance on automated tools
- Over-reliance on consultants

Actions Taken

- Update firewall configuration
- Implement automated tools along with manual oversight processes
- Focused training with consultants and internal personnel

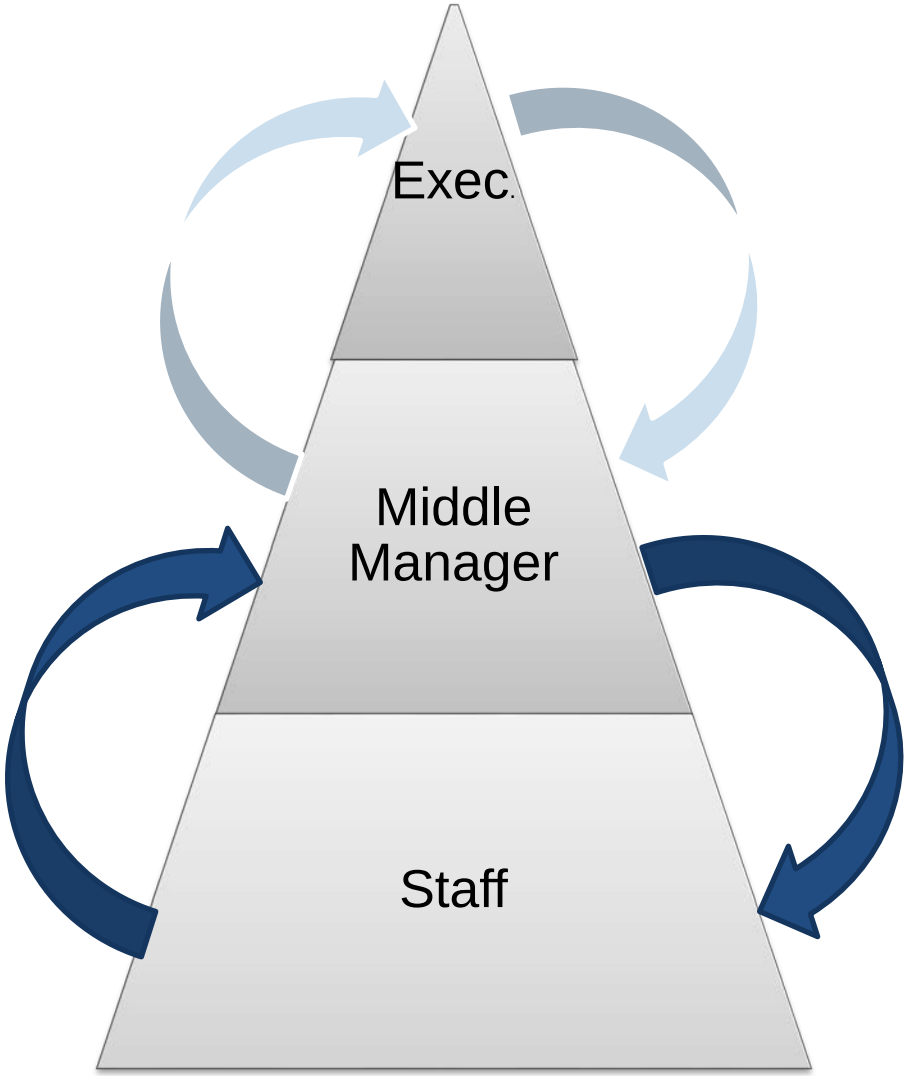
Theme - Organizational Silos

- Lack of coordination between departments, business units, and different levels of management

Vertical Silos (Between Business Units or Departments)

Horizontal Silos (Between Layers from the Top Down)

Theme - Organizational Silos



Theme-Organizational Silos Example

Failed Compliance Program

- Entity's compliance program developed by upper management
- Not practical when applied at operational level
- Lack of internal communication in developing program

Improvement

- Entity focused on better communication among departments
- Communication improved from upper management down as well as from the operational level up

Themes Intersect

- Generally, significant CIP compliance program deficiencies are result of multiple causes that overlap and are interrelated
- Example
  - Disassociation and Lack of Awareness
    - Lack of engagement and/or participation
    - Organizational barriers and overreliance on consultants
- Lessons learned from both sides
- Recommendations

Next Steps

- Outreach and Education
  - Interactions and engagements with registered entities
  - Standards & Compliance workshops
  - Regional Webinars
  - Newsletter articles
  - Engagement of the CIPC
- FERC Lessons Learned
  - Lessons identified from FERC ledP audits
  - Aligns with the ERO themes
- References
  - 2018 CIP Themes and Lessons Learned
  - FERC lessons learned

Questions and Answers

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Monitoring and Enforcement Program Quarterly Report

Q1 2018

Sonia Mendonça, Vice President, Deputy General Counsel, and Director of Enforcement
Ken McIntyre, Vice President of Standards and Compliance

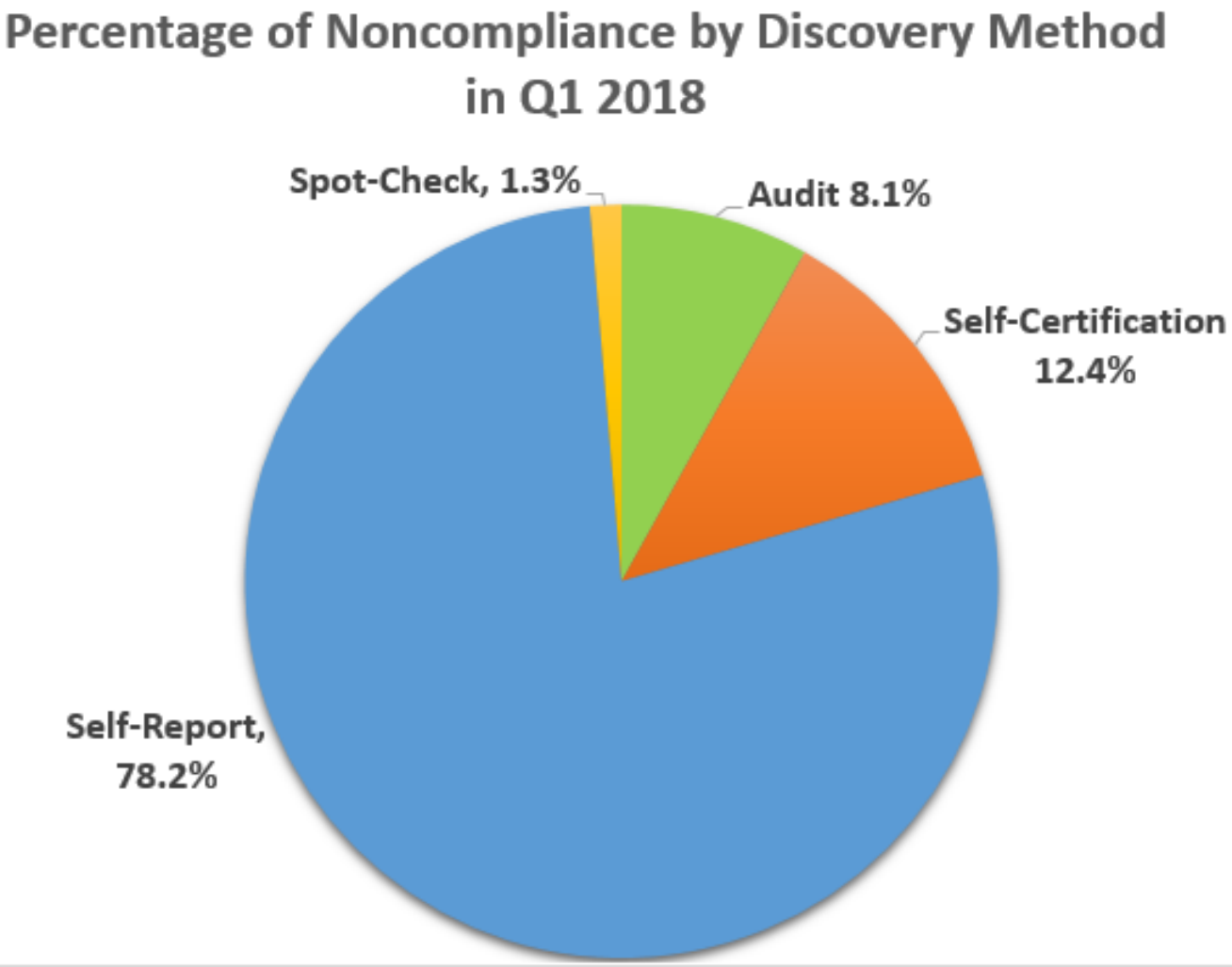
Compliance Committee Meeting

May 9, 2018

RELIABILITY | ACCOUNTABILITY

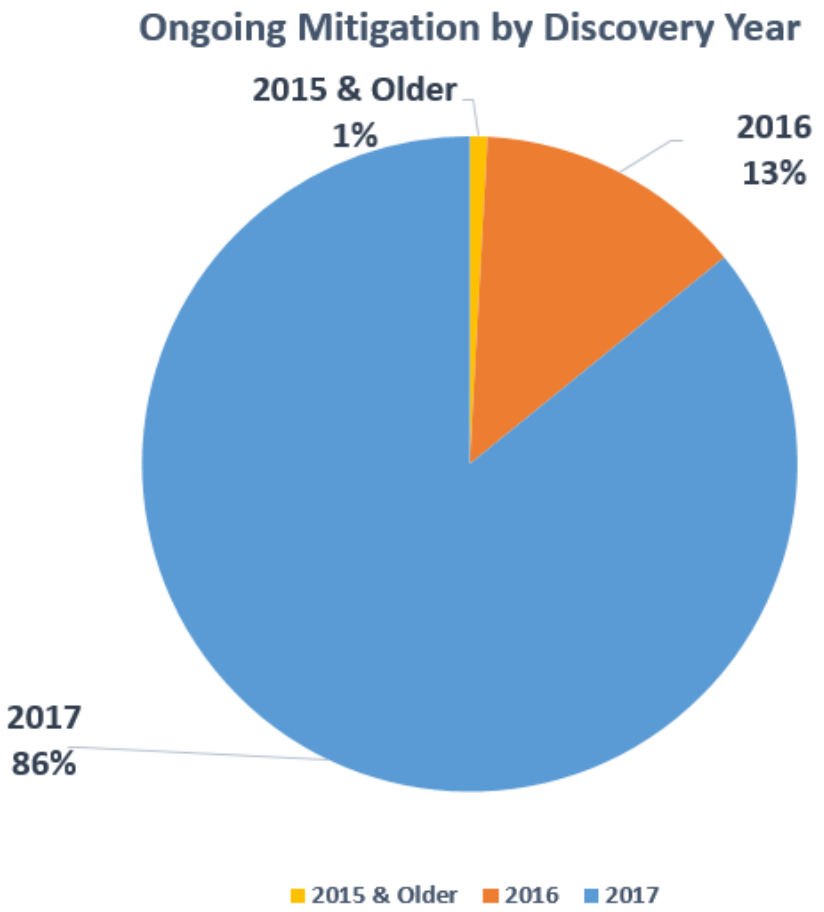



Discovery by Self-Report

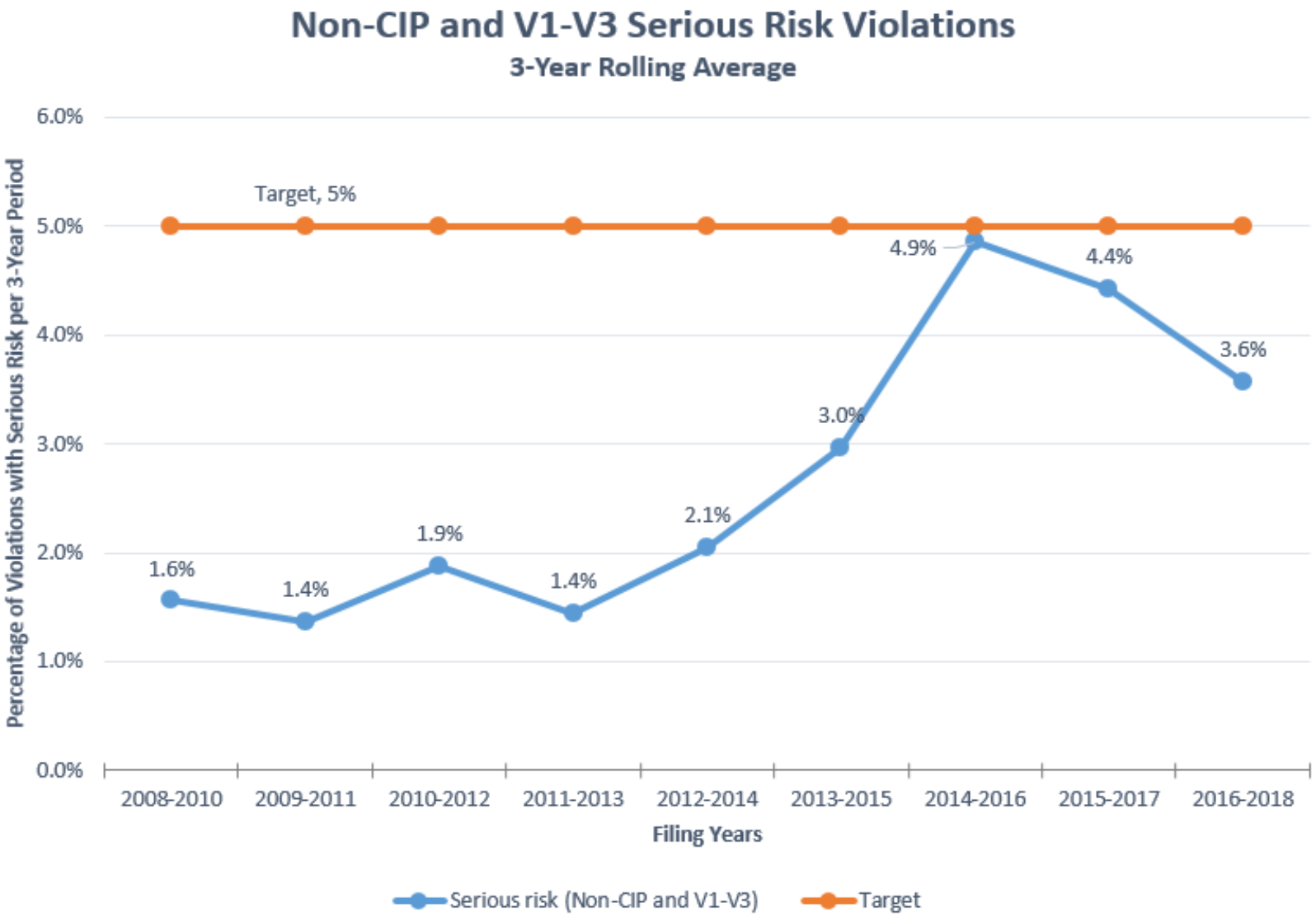


Mitigation Completion

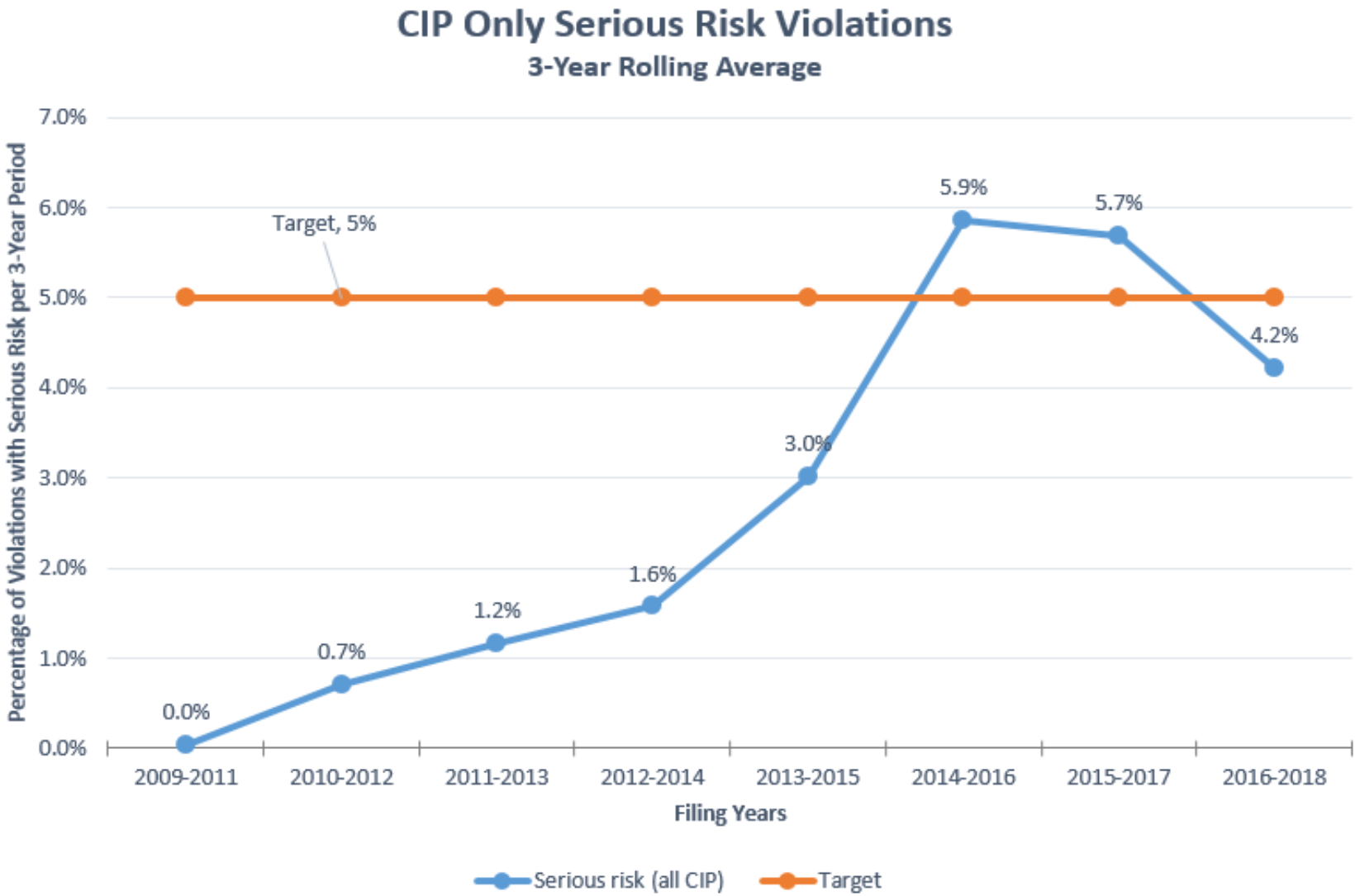
Table A.1: Mitigation Completion Status						
Time Frame	Required Mitigation	On-going	Progress Toward Goal	Threshold	Target	Progress Since Last Quarter
2015 and Older	10209	11	99.9%	99%	100%	0.02%
2016	1155	168	85.5%	85%	90%	5.34%
2017	2014	1086	46.1%	70%	75%	10.68%



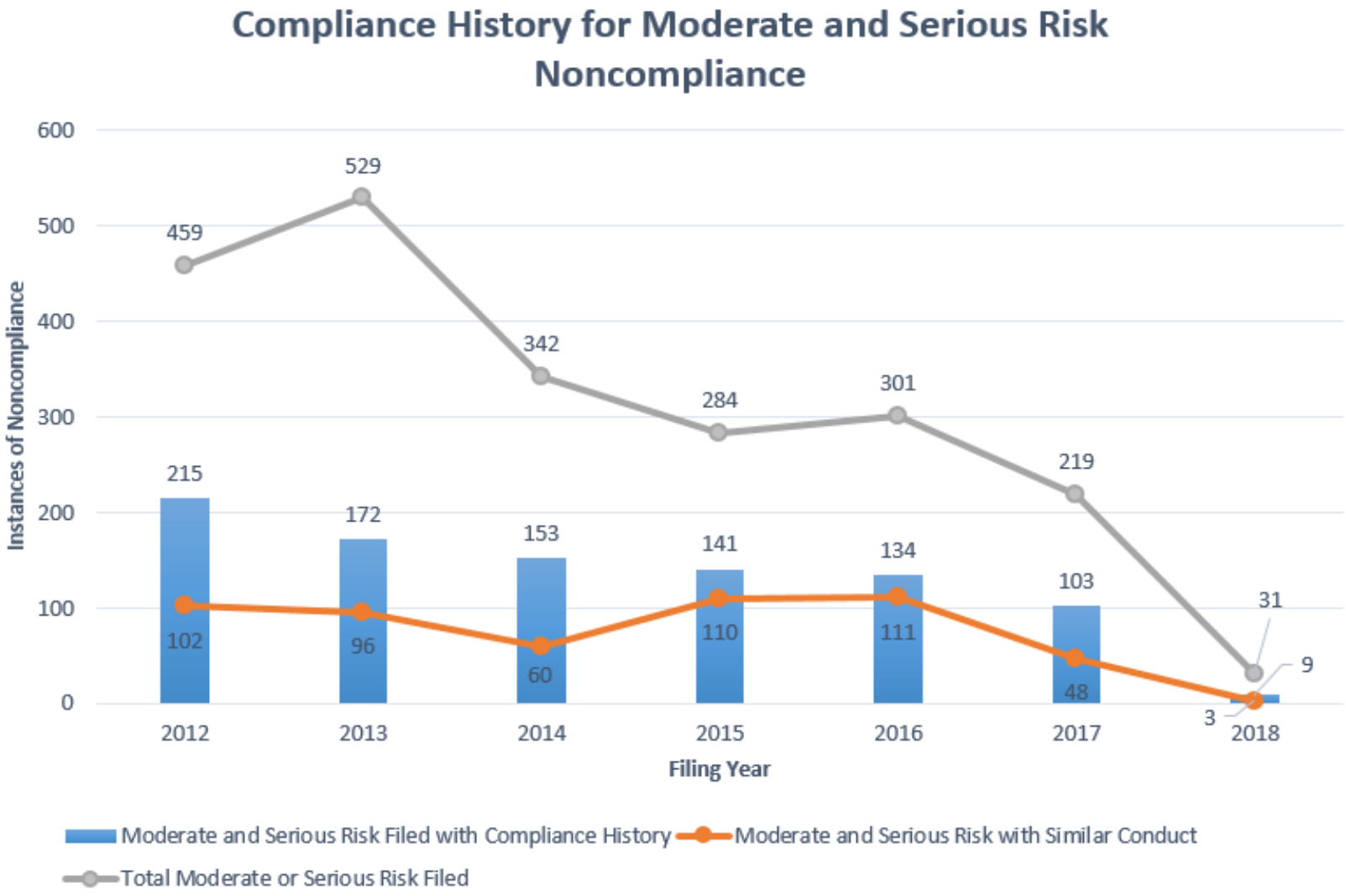
Serious Risk – Excluding CIP V5/V6



Serious Risk – All CIP



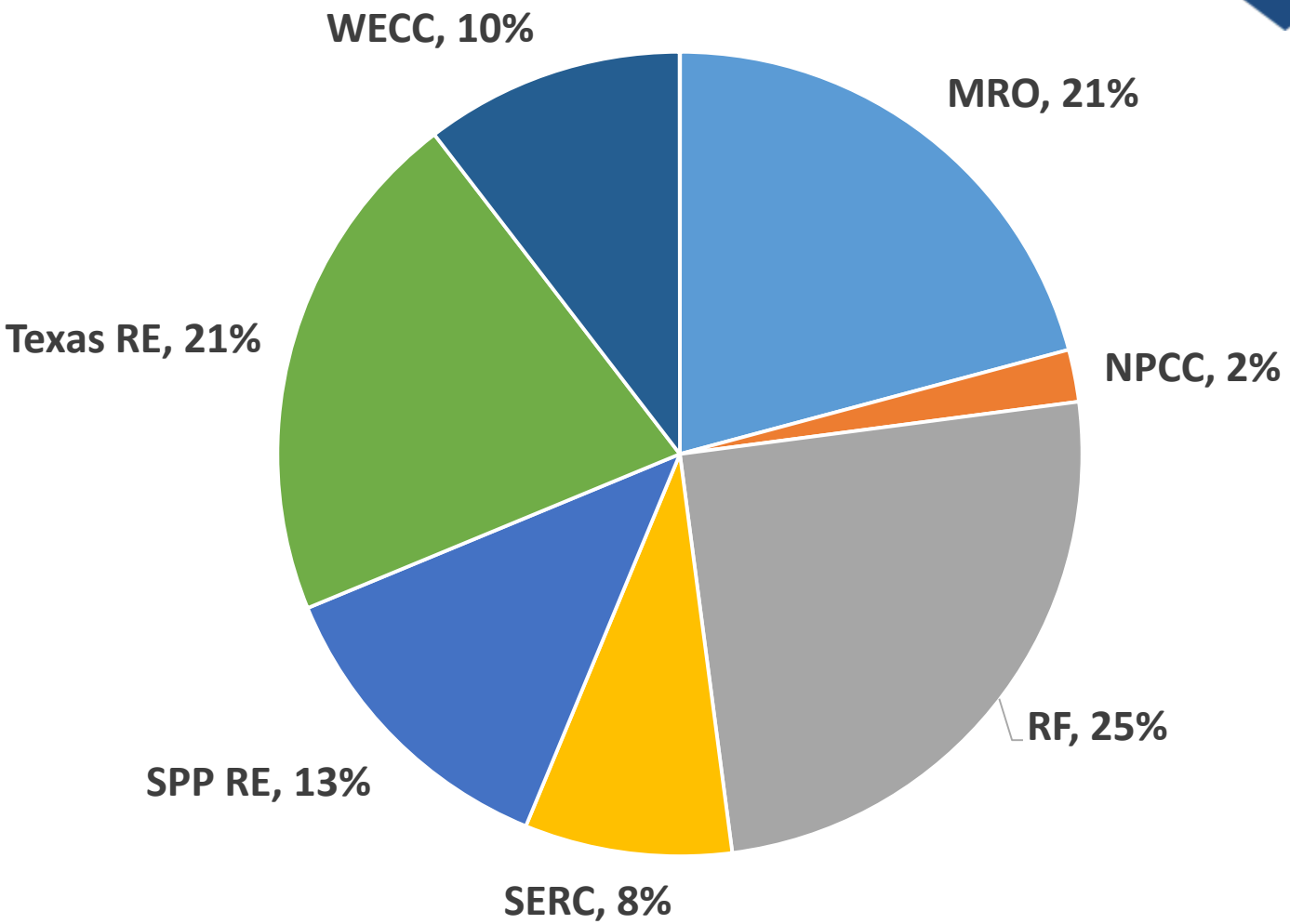
Similar Prior Conduct



Compliance Guidance

- Implementation Guidance
  - Eight endorsed, one non-endorsed, and four currently under review
- The Compliance and Certification Committee (CCC) approved a new Pre-qualified Organization.
  - EnergySec

Coordinated Oversight Program for MRREs



Percentage of MRREs under Coordinated Oversight by Lead RE

Program Alignment

- Program Alignment Items:
  - Twelve completed, and
  - Five in progress.
- Continued outreach in collaboration with CCC Alignment Working Group at Regional Entity workshops

Questions and Answers