

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## Violations Themes Webinar CIP Violations

April 30, 2019

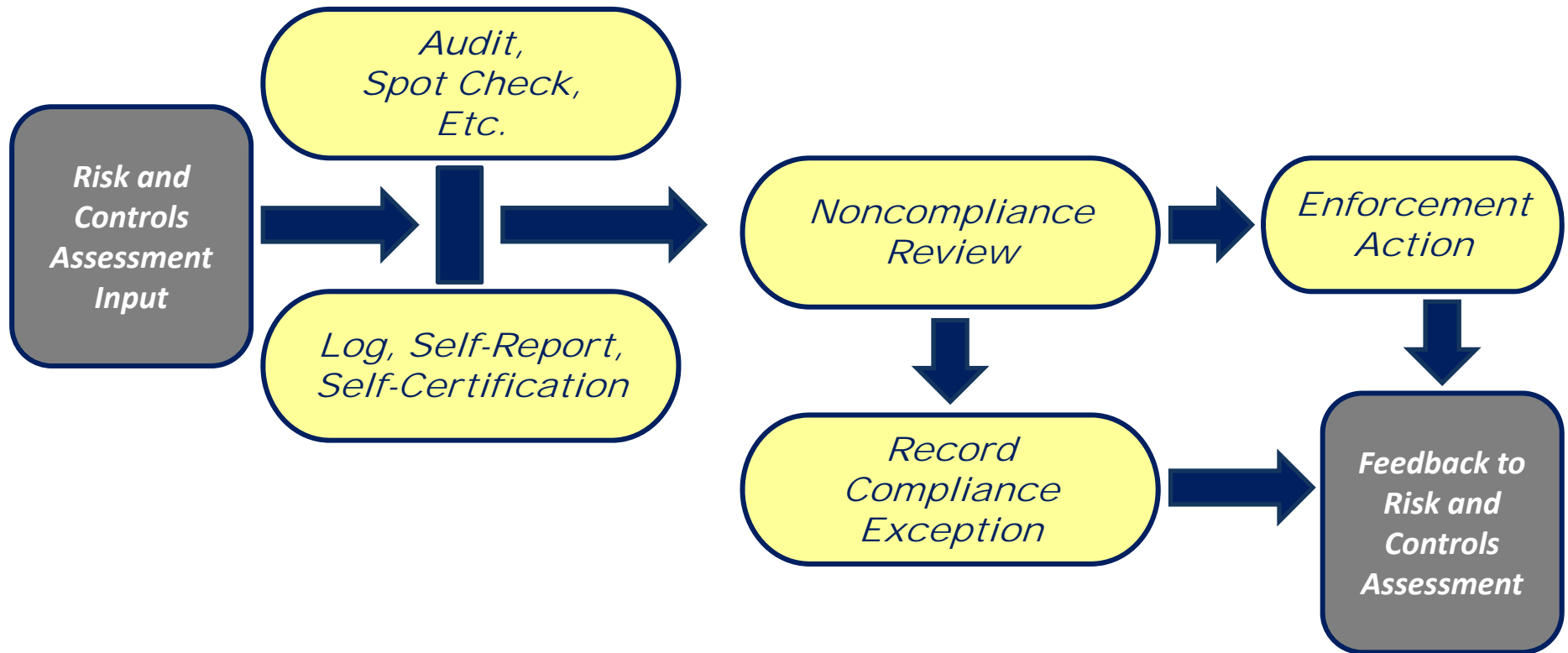
**RELIABILITY | ACCOUNTABILITY**



- The Compliance Monitoring and Enforcement Program (CMEP) promotes a culture of reliability and excellence through a risk-based approach.



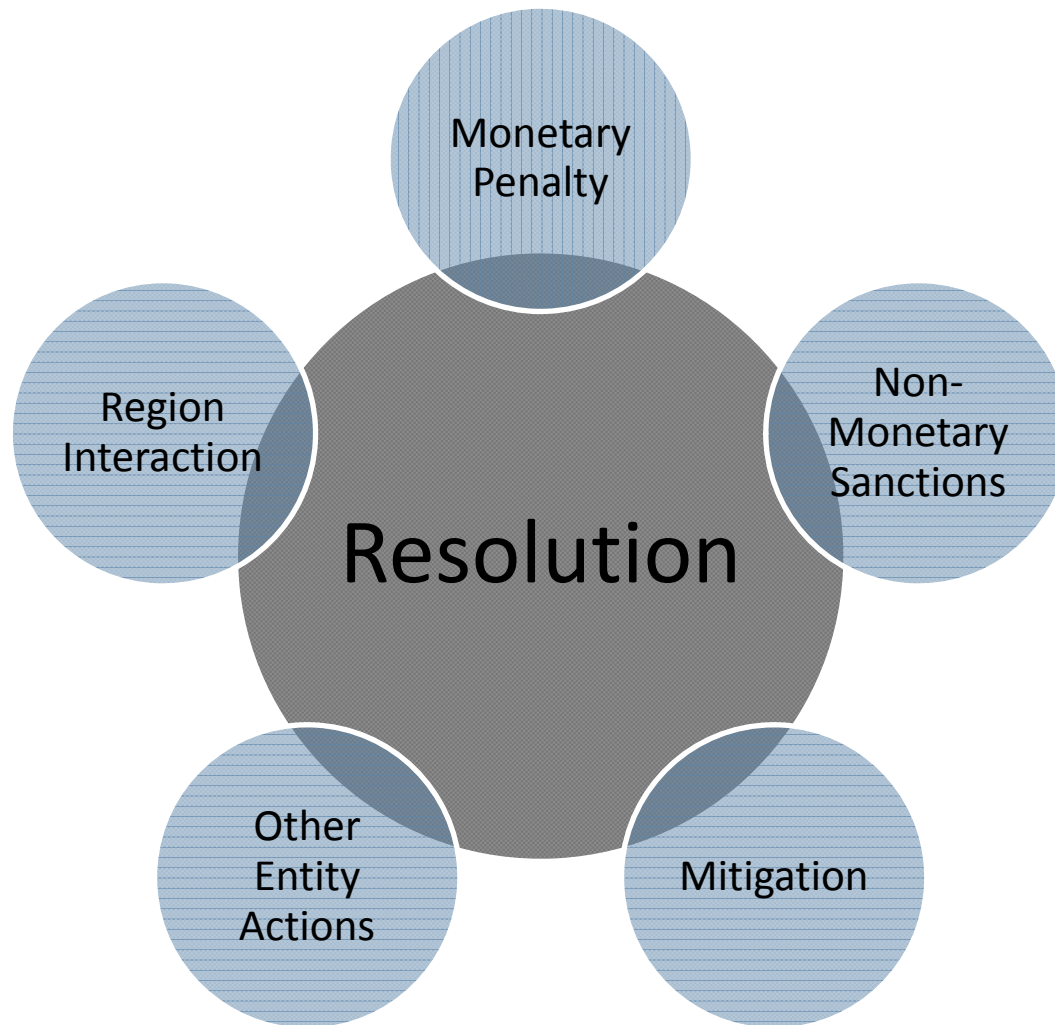
- Outcomes for noncompliance are based on risk
- Risk is based on specific facts and circumstances
- Continuous evaluation and communication of risks
  - Analysis and lessons learned shared publicly
  - Input to risk identification



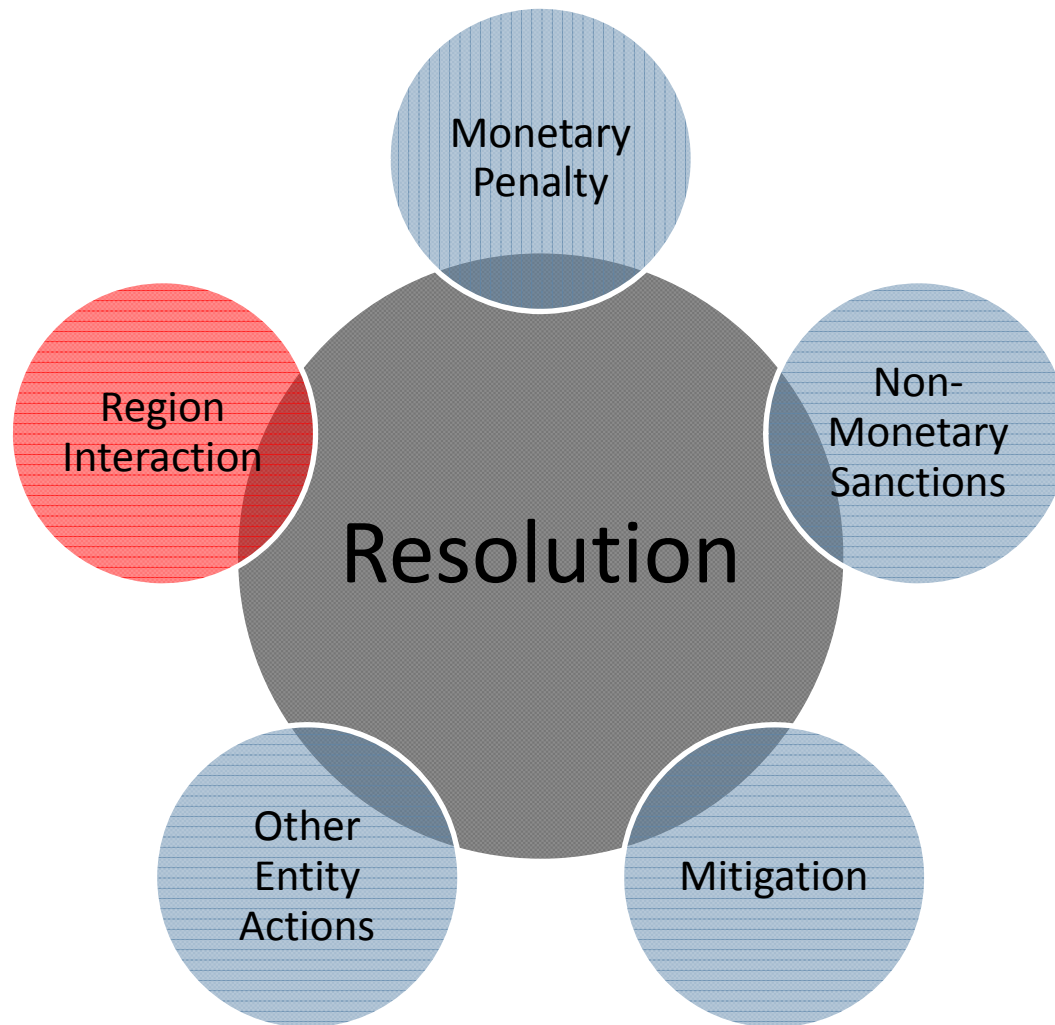
- Non-enforcement treatment for most minimal risk issues
  - Compliance Exceptions
  - Presumed for self-logged items
- Keeps minimal risk issues from escalating

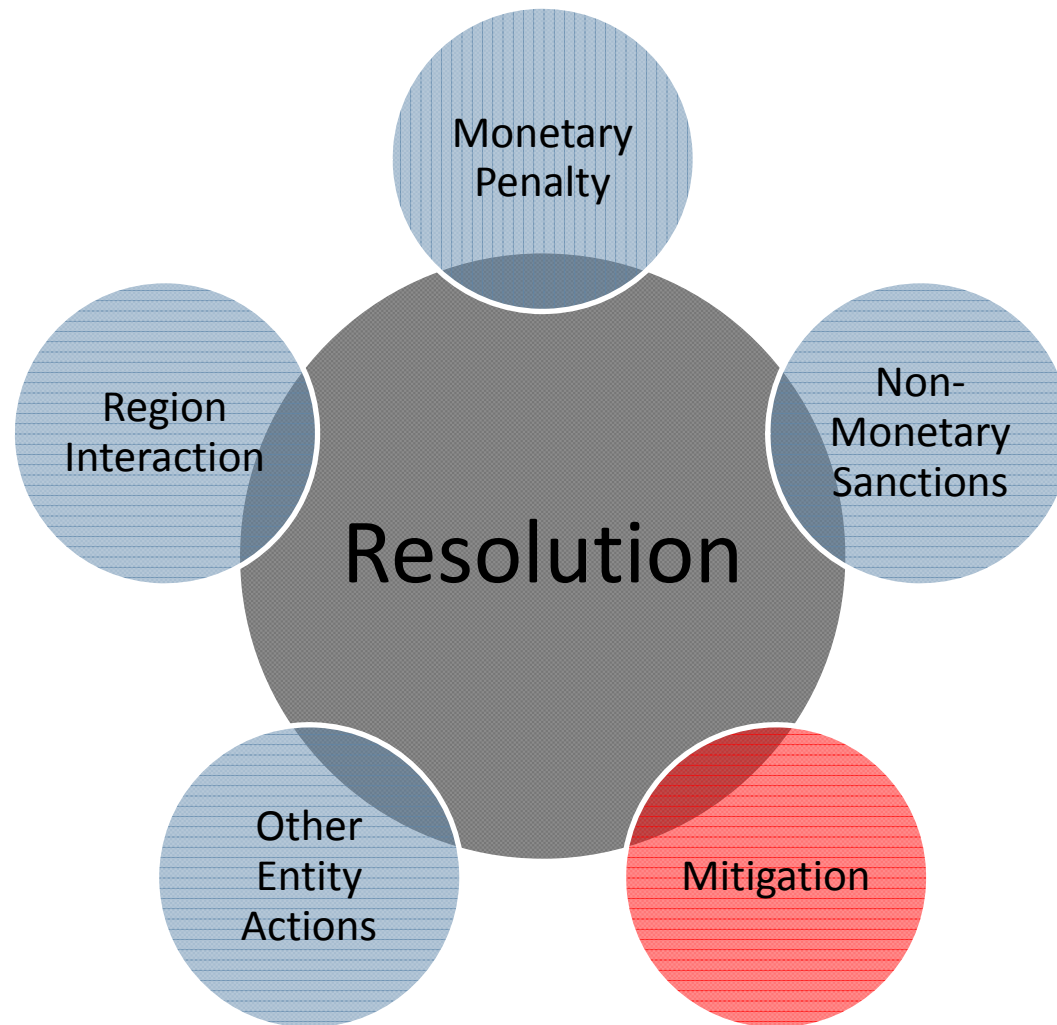
- Spreadsheet Notices of Penalty (NOPs) and Full Notices of Penalty
  - Many Spreadsheet NOPs have no financial penalty
- Ensuring penalties are warranted and commensurate with risk
  - Significant penalties used to deter undesired behavior
  - Offset penalties to encourage valued behavior
- NERC's responsibility to promote alignment on enforcement activities, including penalties
  - Electric Reliability Organization Enterprise alignment activities
  - Communication with industry

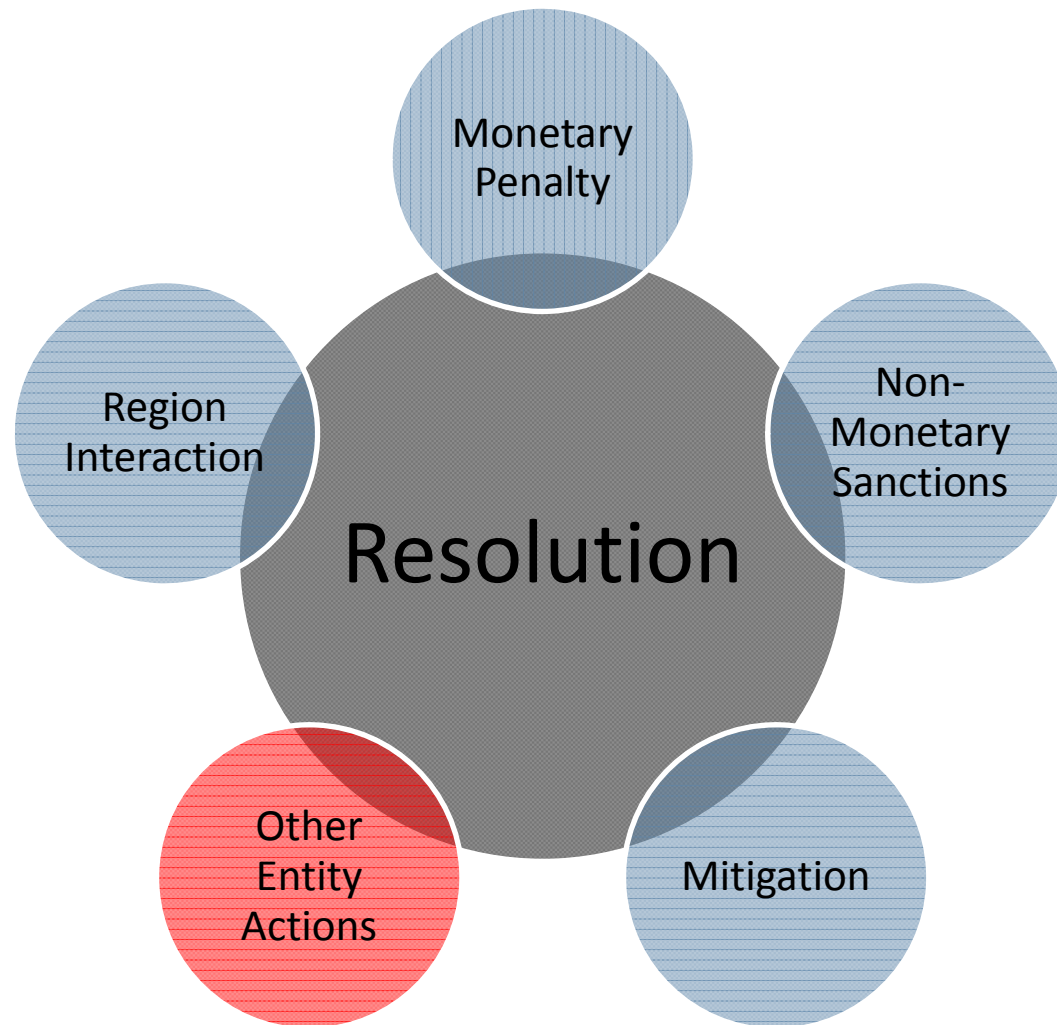
- Overarching goal of sustainable compliance
  - Focus on robust mitigation to reduce risks and likelihood of recurrence
  - Establishing cultures of continuous learning
  - Meaningful engagements and interactions between Regional Entities and registered entities throughout resolution of noncompliance

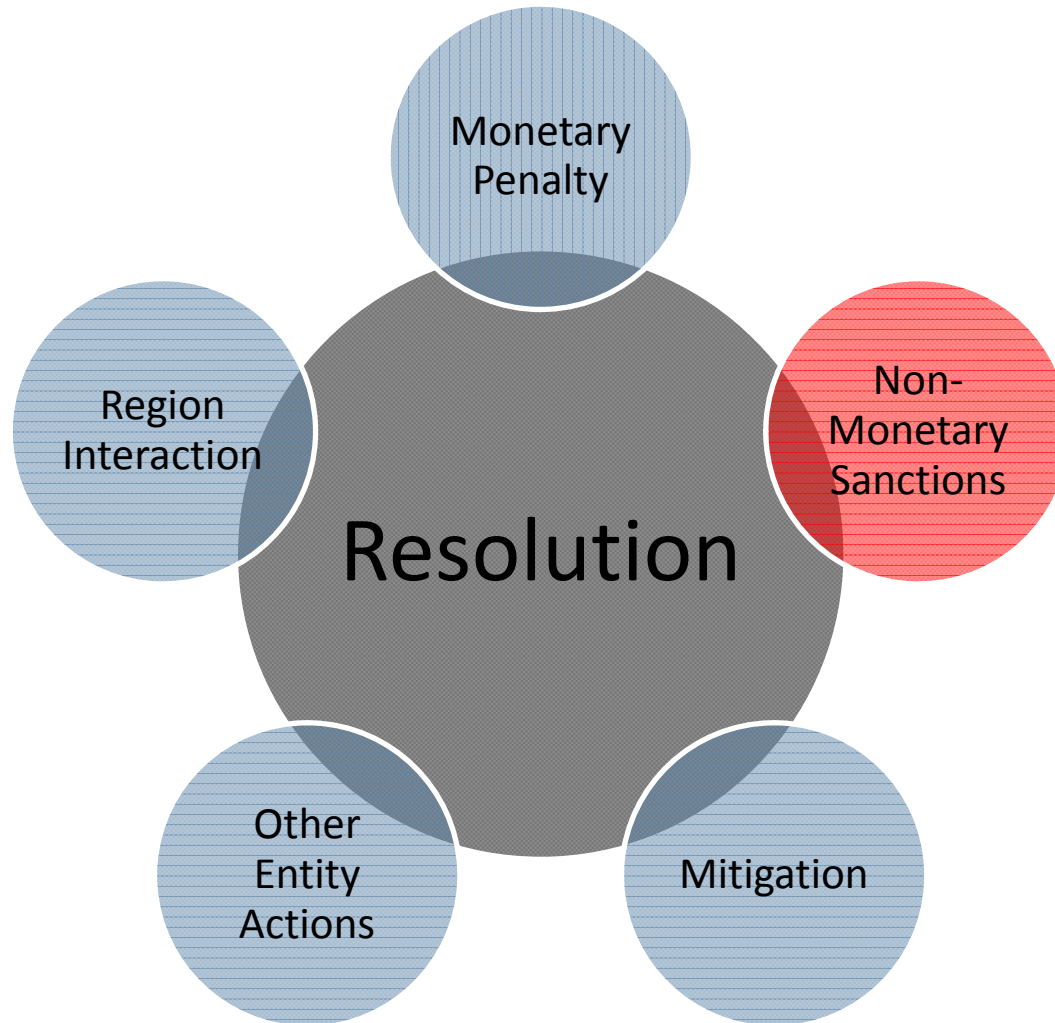


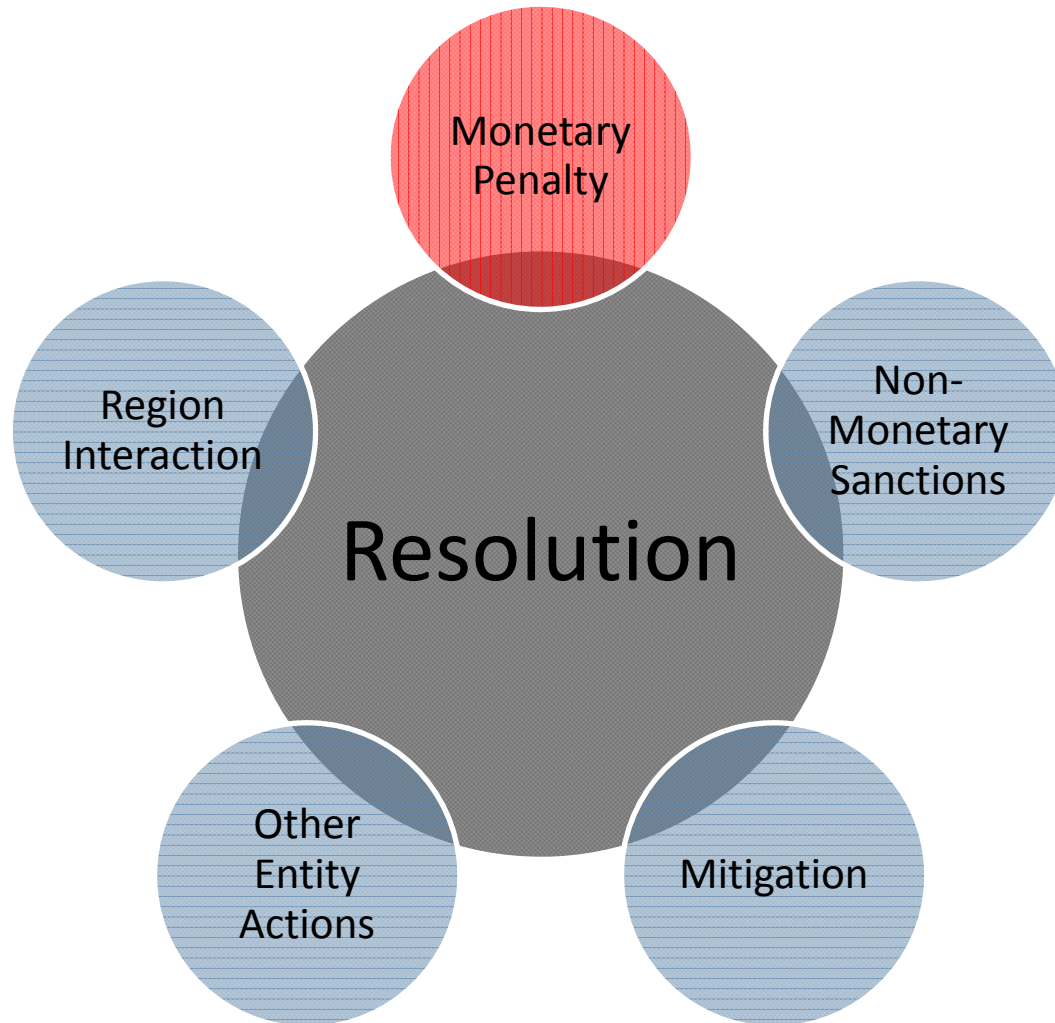




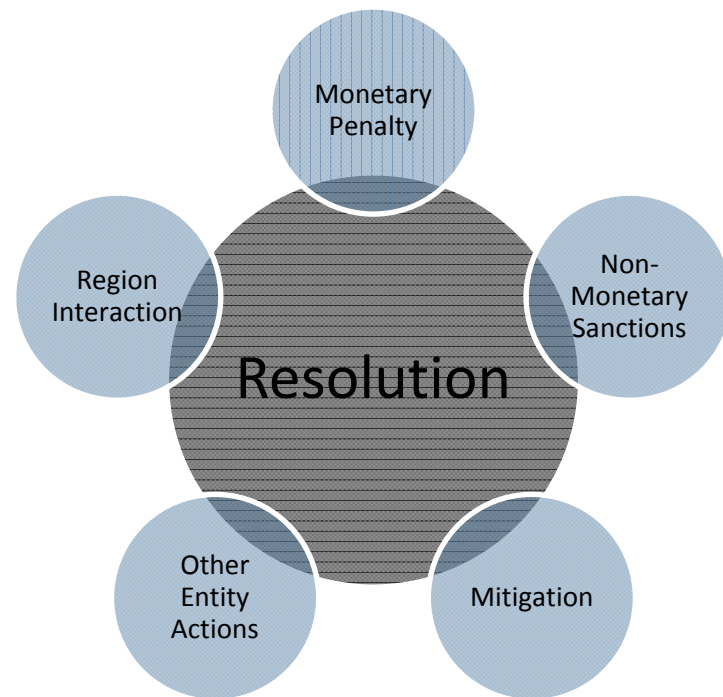




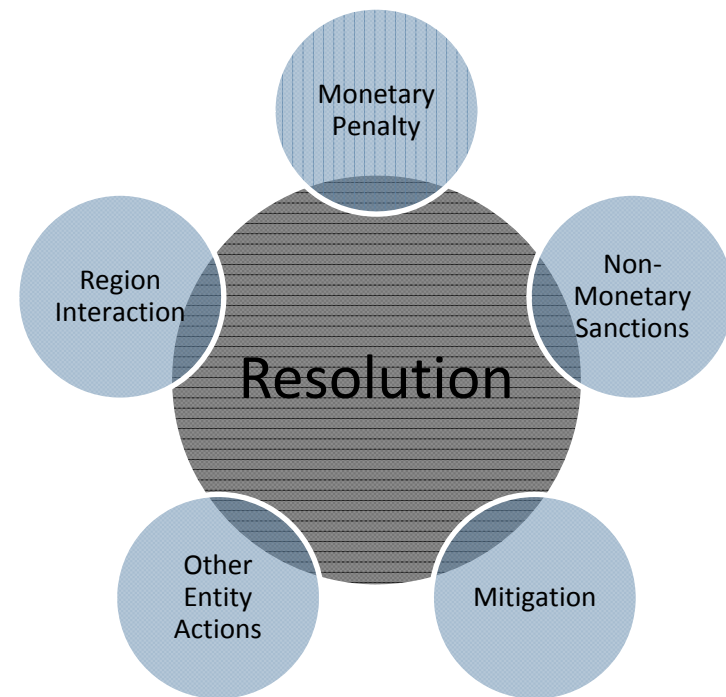




- Serious Critical Infrastructure Protection (CIP) case
  - Inadequate Tools and Organizational Silos
- Early regional interaction
- Comprehensive, forward-looking mitigation
- Significant credit for above and beyond activities
  - Tools, people, and programs
- Increased monitoring

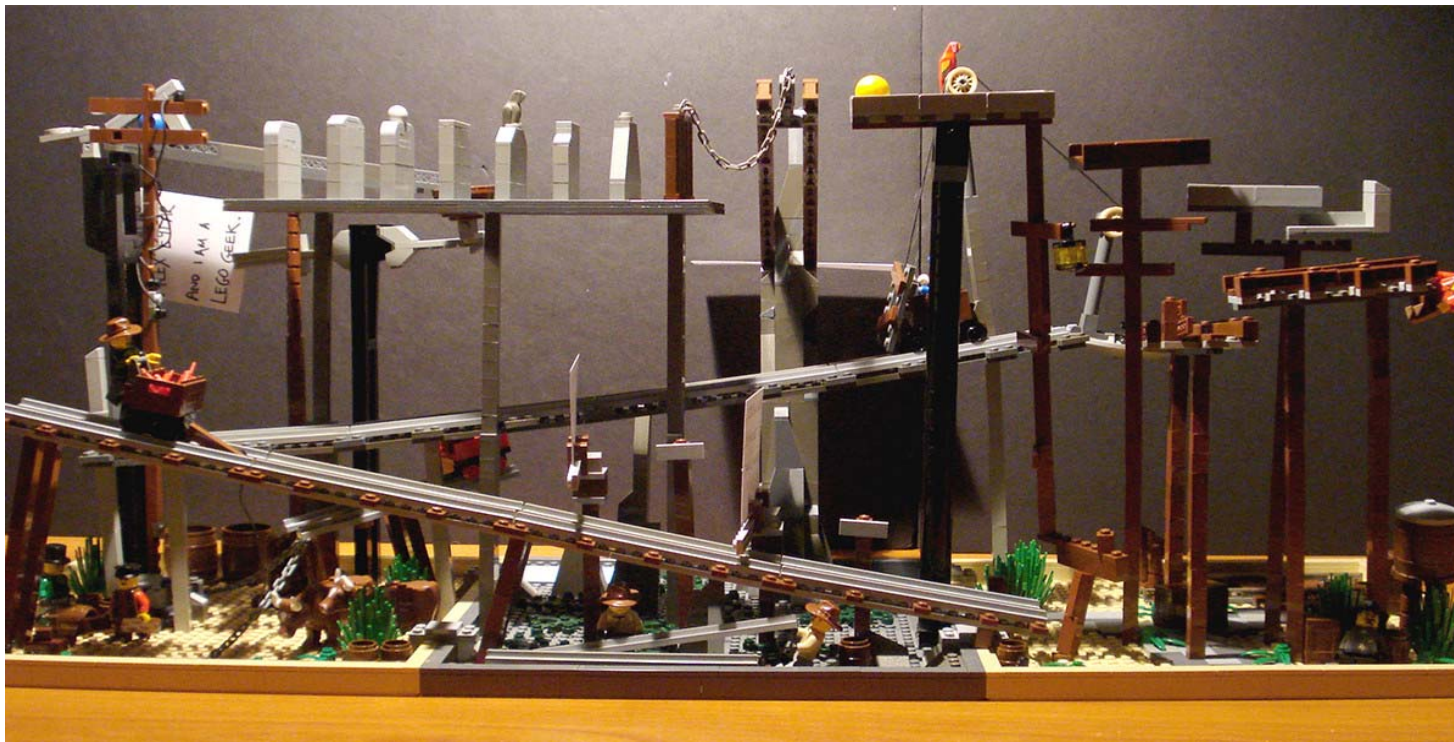


- Serious CIP case
  - Disassociation of Security and Compliance and Lack of Awareness
- Significant regional interaction
  - Regional leadership
  - Subject matter experts
- Holistic mitigation evaluating and improving entire CIP program
  - Increased focus on security and compliance
- Increased monitoring



## Insights

- Large CIP failures often involve multiple Themes (are the underlying causes)
- Preventing Themes promotes best security





## CIP Themes Report

- Organizational silos
- Disassociation of compliance from security
- Lack of awareness
- Inadequate tools



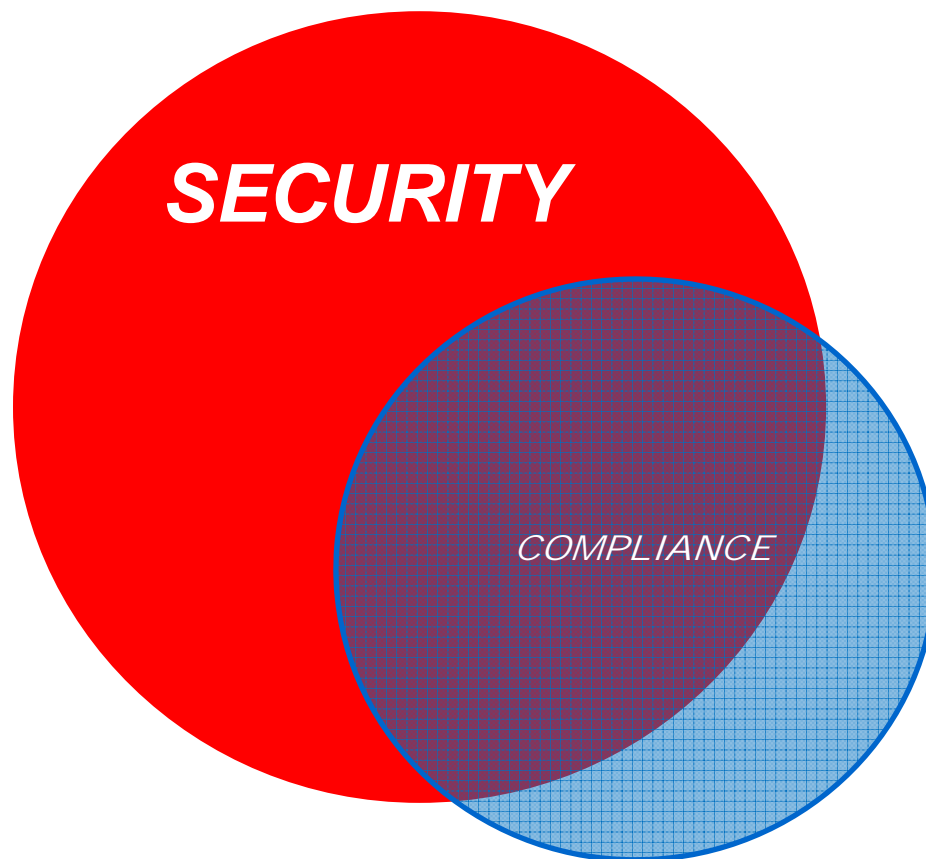
## Organizational Silos

V  
E  
R  
T  
I  
C  
A  
L  
  
L  
imited  
information  
sharing  
between  
business  
units



*H O R I Z O N T A L*

*Upper management not fully aware of compliance  
difficulties until late in the game*



## Lack of Awareness

Isolation

Over-reliance on consultants

Inadequate root cause



## Inadequate Tools

Appropriate  
use of tools  
and  
resources



## Sustainability

- How entities can build sustainable programs:
  - Management communicates expectations
  - Adopt a continuous improvement mindset
  - Keep your focus on security
  - Training, training, training
  - Track your near-misses
  - Internal Controls
  - Team approach



## Resources

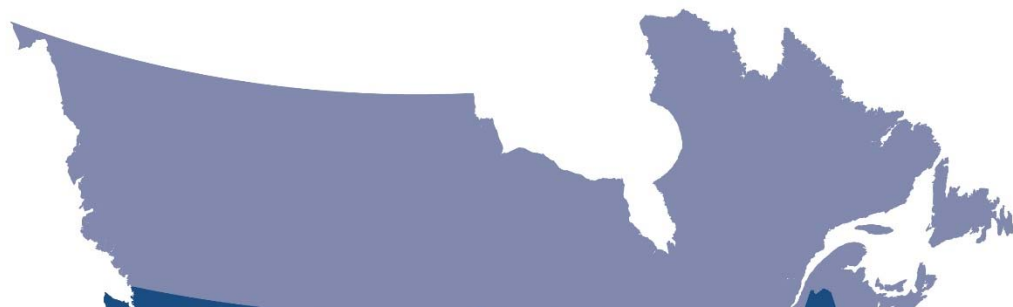
Regional Contact

Regional  
Outreach



**NERC**

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION



# Questions and Answers

