• 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
Enforcement Process Flow

1. Risk and Controls Assessment Input
2. Log, Self-Report, Self-Certification
3. Audit, Spot Check, Etc.
4. Noncompliance Review
5. Record Compliance Exception
6. Enforcement Action
7. Feedback to Risk and Controls Assessment
Non-Enforcement Tracks

• 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
Resolution of Serious Violations

Resolution

- Monetary Penalty
- Non-Monetary Sanctions
- Region Interaction
- Other Entity Actions
- Mitigation
Resolution of Serious Violations

Resolution

- Monetary Penalty
- Non-Monetary Sanctions
- Other Entity Actions
- Mitigation
- Region Interaction
Resolution of Serious Violations

Resolution

- Monetary Penalty
- Non-Monetary Sanctions
- Region Interaction
- Other Entity Actions
- Mitigation
Resolution of Serious Violations

Resolution

- Monetary Penalty
- Non-Monetary Sanctions
- Region Interaction
- Mitigation
- Other Entity Actions
Resolution of Serious Violations

Resolution

- Monetary Penalty
- Non-Monetary Sanctions
- Region Interaction
- Other Entity Actions
- Mitigation
Resolution of Serious Violations

Resolution

- Monetary Penalty
- Non-Monetary Sanctions
- Region Interaction
- Other Entity Actions
- Mitigation
• 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

Limited information sharing between business units

Horizonal
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
Questions and Answers