MARCH 21, 2023

RELIABILITY & SECURITY

Virtual Workshop

WECC

Comparative Enforcement Experience

March 21, 2023

Michael Dalebout

David Vitkus

Dulce M. Plaza

Trent Wilson

Michael Shaw

Where We Are

Enforcement

PNC | Triage | Validation | Mitigation | Disposition

What Happens Next

What We Know

Self-Report

Orko determined, then filed a **self-report,** stating it may be in violation of the standard due to how it *failed to update its Supply Chain Risk Management plan to include procurement of PACS and EACMS associated with BES Cyber Systems.*

Audit Finding

The **WECC Audit Team** had an **audit finding** that Sunbear Power may be in violation of the standard for *not updating its Supply Chain Risk Management plan to include procurement of PACS and EACMS associated with BES Cyber Systems.*

What WECC Needs

Needed for Processing		
Full Description of Noncompliance	Yes	?
Basis for Dates	Yes	No
Root Cause Analysis	Yes	No
Extent of Condition (EOC) Analysis	Yes	No
Description of Remediation	Yes	No
Mitigation Activity Details	Yes	No

What We Know

Orko Profile

- GO/GOP
- Medium size
- Detailed entity data available
- Compliance history
- Good controls
- Good compliance program
- Entity provides detailed responses to WECC requests
- Engaged and transparent
- Participates in WECC workshops or training
- Program validated with no issues at past two audits
- Few PNCs in compliance history; mostly self-reports

What We Know

Sunbear Power Profile

- GO/GOP
- Medium size
- Basic entity data available
- Compliance history
- Poor controls
- Weak compliance program
- Entity provides minimal responses, sometimes none
- Rarely communicates with WECC
- Never participates in WECC workshops or training
- Program related issues found at past two audits
- PNCs generally found at audit and not self-detected

Triage

Triage

ORKO Electric Company

Analysis

- Determine whether there is a noncompliance
- Discovered soon after the start date, which lowers the likelihood of potential harm
- Strong compliance program
- Remediated quickly which **lowers** the duration and likelihood of potential harm
- Overall potential risk impact (**minimal**, moderate, serious)

SUNBEAR POWER

Analysis

- Determine whether there is a noncompliance
- Discovery was made at audit and not self-identified, which increases the likelihood of potential harm
- Compliance program lacks internal controls
- Not remediated quickly which **increases** the duration and likelihood of potential harm
- Overall potential risk impact is either moderate or serious

Validation

Validation

ORKO Electric Company

Analysis

- Review of noncompliance
- Risk assessment
- Verification of EOC analysis
- Review of internal controls
- Remediation review
- Requests for information/meetings are not required
- Examination of root cause analysis description and evidence

Analysis

- Review of noncompliance
- Risk assessment
- Verification of EOC analysis
- Review of internal controls
- Remediation review
- Multiple meetings and requests for information would be required
- Examination of root cause analysis description and evidence

Mitigation

Mitigation

Analysis

- The instance was discovered quickly
- Rapid remediation shortened the duration and reduced risks
- Rapid discovery led to updates of preventive controls within one month
- Remediation detailed in self-report, along with mitigating activities

Analysis

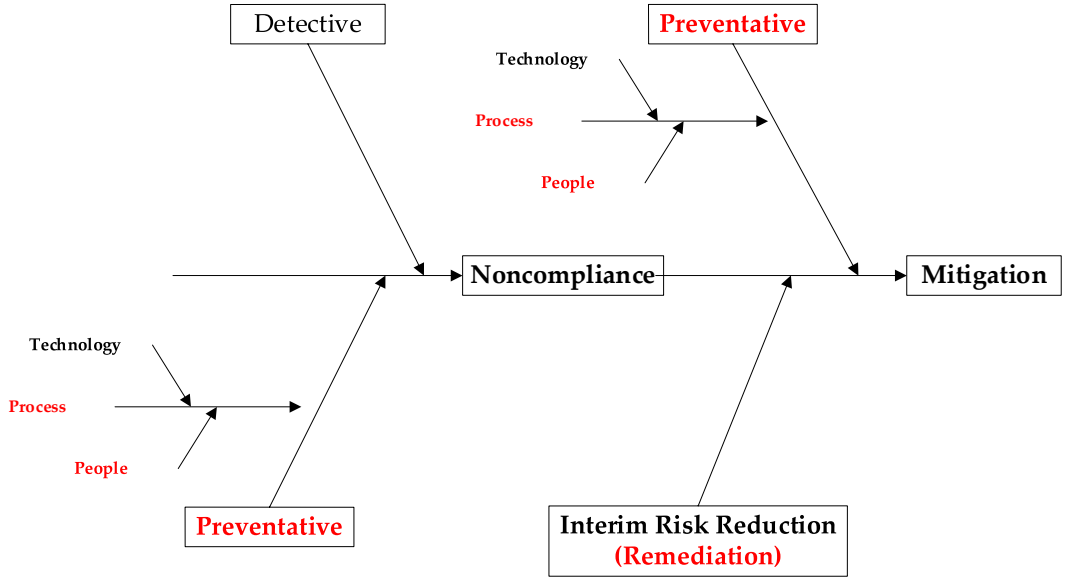
- The instance was not discovered quickly
- No remediation before audit
- Longer duration increased risks
- New processes and internal controls will need to be developed
- Mitigation efforts will be lengthy and will likely require a mitigation plan
- Substantial changes in the CIP program may be required

Mitigation

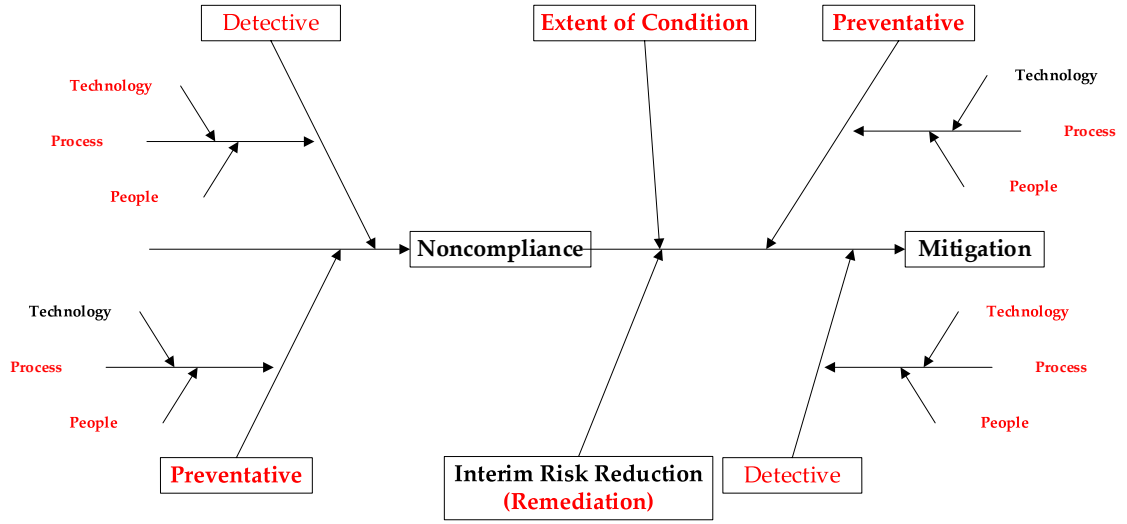
ORKO Electric Company

SUNBEAR POWER

Work Required



Work Required



Disposition Methods

Disposition Methods

Disposition Method	Risk
Dismissal	
Compliance Exception (CE)	Minimal
Find, Fix, Track and Report (FFT)	Minimal or Moderate
Settlement/ Spreadsheet Notice of Penalty (SNOP)	Minimal or Moderate; with a Penalty or Non-Monetary Sanction
Settlement/ Full Notice of Penalty (FNOP)	Serious/substantial
Notice of Alleged Violation Penalty and/or Sanction (NAVAPS)	Any risk

Dismissal

- For-cause dismissal
  - Insufficient evidence to support a noncompliance
- Administrative “dismissal"
  - Consolidation of a subsequent noncompliance of the same Standard and Requirement into an existing noncompliance

Compliance Exception

- Minimal risk
- Mitigating activities must either be complete or will be completed within 12 months from NERC filing with FERC
- No penalty
- Generally—CEs not included in compliance history for penalty purposes
- FERC has a 60-day review period

Find, Fix, Track, and Report

- Most often moderate risk but can be minimal risk
- Mitigating activities must either be complete or will be completed within 12 months from NERC filing with FERC
- FFT process requires that registered entity senior management affirm
- No penalty
- FFT affidavit required upon completion of mitigation
- FERC has a 60-day review period

Spreadsheet Notice of Penalty

- Typically moderate risk but can be minimal risk
- Often includes a penalty
  - Can be a $0 penalty
  - Can include non-monetary sanction(s)
- Mitigation completion verified
- Use the settlement process
- FERC has a 30-day review period

Full Notice of Penalty

- Typically serious/substantial risk
- Typically includes penalty
  - Can include non-monetary sanction(s)
- Mitigation completion verified
- Use the settlement process
- Pre-filing meeting with NERC and approval of penalty is required before submission of settlement/FNOP to the registered entity
- FERC has a 30-day review period

Notice of Alleged Violation Penalty and/or Sanction

- WECC rarely uses this method
- Any risk issue
- Penalty could apply
- NERC approves penalty before filing
- NAVAPS obligates the entity to submit a mitigation plan within 30 days
- Mitigation completion verified
- FERC has 30-day review period
- Parties can move to a settlement track
- Could result in a hearing

Disposition: Orko vs. Sunbear

Factors

- Minimal risk
- No Compliance History
- Other factors

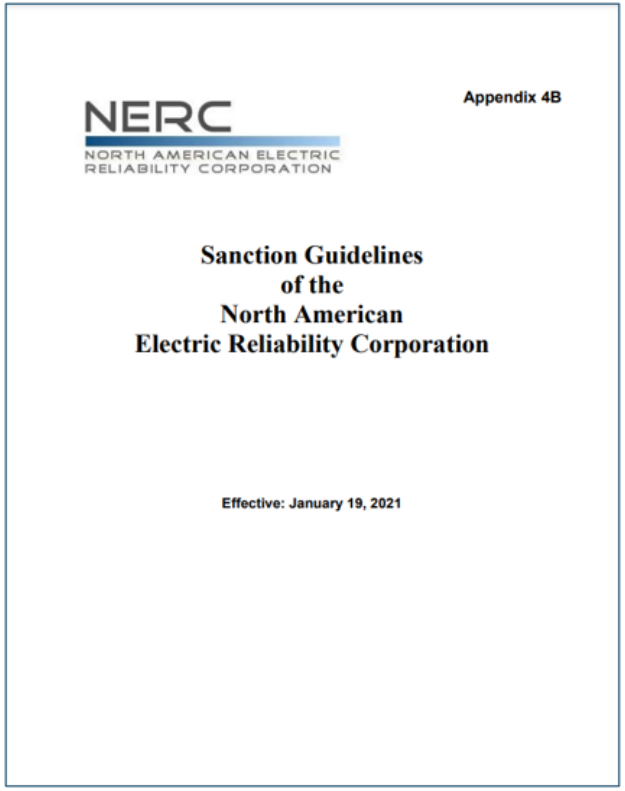
Factors

- At least moderate risk, but potentially serious risk
- Compliance History
- Other factors

Penalty Determination

Penalty Determination

- Determine base penalty amount
  - Violation risk factor and violation severity level table
  - Entity size
  - Assessed risk
  - Violation duration
  - Violation time horizon
- Adjustment factors
  - Mitigating factors
  - Aggravating factors


Appendix 4B

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Sanction Guidelines
of the
North American
Electric Reliability Corporation

Effective: January 19, 2021

Penalty: Orko vs. Sunbear

Factors

- Not applicable since the Orko noncompliance would likely be processed as a Compliance Exception

Factors

- At least moderate risk, but potentially serious risk
- Audit finding
- Weak compliance program
- Cooperation level
- Compliance History

WECC

Electric Reliability and Security for the West

www.wecc.org