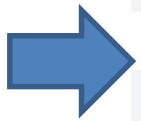
Self Report Guidance

June 12, 2019

Jenifer Vallace Farrell
Jason Wang
Francesco Elmi
Aaron Hornick

CIP & O&P Self Report Guides

- https://www.npcc.org/Compliance/enforcement/default.aspx

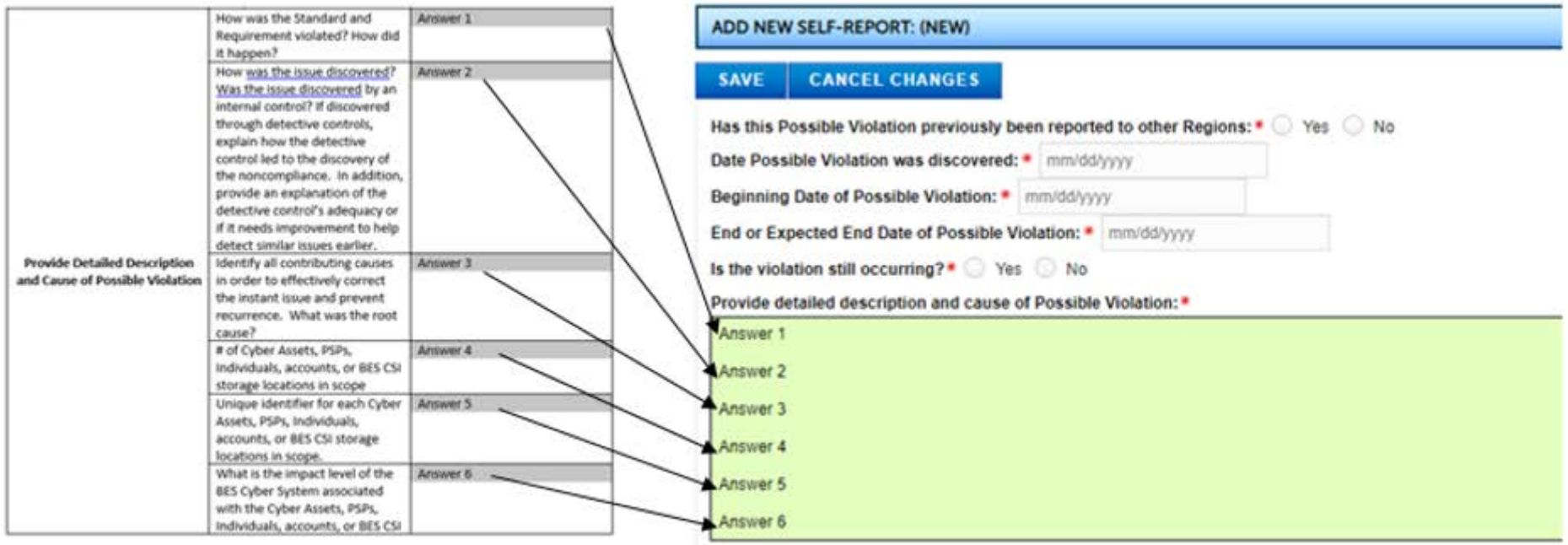


LATEST DOCUMENTS

TYPE	TITLE	POSTED DATE
	Updated Spring 2019 Prelim Workshop Agenda	5/1/2019
	20190430_NPCC Compliance Registry	4/30/2019
	20190430_NPCC Compliance Registry	4/30/2019
	CDAA CIP Self Report Entry Guidance	4/1/2019
	CDAA O&P Self Report Entry Guidance	4/1/2019

CIP & O&P Self Report Guides

- Copy and paste each answer field into the appropriate self-report section.



CIP-010 R1 Description Example

CIP Lacking Description of Noncompliance

- ABC company found that it failed to classify BES Cyber Assets, Protected Cyber Assets and Electronic Access Control or Monitoring Systems. The documentation issue was the result of human error.

Questions?

- How was the issue discovered?
- How many Cyber Assets were not identified?
- What is the function of the Cyber Assets in scope?
- What caused the documentation issue?

CIP-010 R1 Description Example

CIP Better Description of noncompliance

- On Jan 1, 2019 ABC company found that it failed to classify 10 BES Cyber Assets, 5 Protected Cyber Assets and 2 Electronic Access Control or Monitoring Systems, after performing its annual site walkthrough. The Cyber Assets were part of a new SCADA system that was on boarded on Dec 1, 2018 and the Compliance Manager was not aware of the project.

Key Details

- Includes how issue was discovered
- Includes the scope of the issue
- Includes start date of the issue
- Includes root cause details
- Includes function of the BES Cyber Assets

PRC-005 R2 Description Example

O&P Lacking Description of Noncompliance

- XYZ company found that it failed to perform minimum maintenance activities for its VLA batteries. The root cause of this issue was a lack of management review.

Questions?

- How was this issue discovered?
- Which maintenance interval was missed?
- Describe the number of facilities, elements, relays, components, or procedures in scope.
- When were the batteries last tested?
- What caused the lack of management review?

PRC-005 R2 Description Example

O&P Better Description of Noncompliance

- On Dec 31, 2019, XYZ company discovered that it failed to perform minimum maintenance activities for its VLA batteries during an annual review. The entity failed to complete all aspects of the 18-month interval battery maintenance activities for its two Facilities since they were last tested in June 2017. The root cause of the issue was a lack of management oversight around implementing the Protection System Maintenance Program (PSMP) and less than adequate controls for scoping and scheduling PSMP maintenance tasks.

Key Details

- Includes how issue was discovered
- Includes maintenance interval missed
- Includes last battery test date
- Root cause includes greater specificity and better informs mitigation

Cause Analysis

Root Cause Methods

- Events and Causal Factor Analysis
- Change Analysis
- Barrier Analysis
- Management Oversight and Risk Tree (MORT) Analysis
- Human Performance Evaluation
- Kepner-Tregoe Problem Solving and Decision Making
- https://www.nerc.com/pa/rrm/ea/CA_Reference_Materials_DL/DOEGuidelinesforRootCause.pdf

Human Performance tools

- S-A-F-E-R
  - Summarize
  - Anticipate
  - Foresee
  - Evaluate
  - Review

- https://www.nerc.com/pa/rrm/ea/CA_Reference_Materials_DL/DOE%20-%20Vol%202%20Tools%20for%20Individuals%20Work%20Teams%20and%20Management.pdf

Risk Evaluation

Potential impact to the BPS

- System condition
- Size, nature, criticality, and location of facilities
- Scope and function of assets
- What systems, facilities, or staff were exposed?
- Misoperations, exceedances of system operating limits?
- Potential loss of a Protection System devices, degradation or loss of a BES element, or BES Cyber System or information?
- Potential affect to CIP-005 and CIP-007 controls

Factors reducing the Risk

- Likelihood
  - Internal controls
  - Size of facilities
  - Early detection
  - Duration
  - Redundancies

- https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Registered%20Entity%20Self-Report%20and%20Mitigation%20Plan.pdf

CIP-010 R1 Risk Example

CIP Lacking Impact Statement

- The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Cyber Assets were afforded protections.

Questions?

- What are the potential consequences to the BES?
- What kind of protections were afforded?
  - Preventative Controls
  - Detective Controls
  - Corrective Controls

CIP-010 R1 Risk Example

CIP Better Impact Statement

- ABC company reduced the risk of Cyber Assets being rendered unavailable degraded or misused by restricting logical and physical access to individuals based on need. The systems are physical protected from unauthorized access via fenced enclosure, buildings with locked doors allowing only badged entry, and PSP's requiring badge and fingerprint to enter. The cyber systems are also equipped with file integrity monitoring software that would alert personnel to unauthorized changes.
- ABC company further included the cyber assets in its patch management program, monitors the systems with antivirus protection, and monitors the network in scope with its IDS system.
- ABC company personnel have been trained on incident handling and if a cyber security incident had occurred personnel would follow ABC companies CIP-008 process.

Key Details

- Identifies preventative, detective, and corrective controls
  - Restricted logical and physical access
  - Calls out layered physical protections
  - Identifies protections that were afforded:
    - Patching
    - Antivirus
    - File integrity monitoring
  - Identifies that personnel are trained to identify and correct issues

PRC-005 R2 Risk Example

O&P Lacking Impact Statement

- This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. When the maintenance testing was completed, no changes were necessary.

Questions?

- What are the potential consequences to the BES?
  - GOs
    - name of host TO and RC
    - provide POI with host TO (POI offers clues to strengths/weaknesses of the local system)
  - TOs
    - name of RC (offers clues to the RC's operating reserves)
    - specify locations of transmission facilities; are they IROLs, SOLs? tie-lines with external systems?
- What factors were in place during the noncompliance to mitigate the risk?
  - Operating conditions (peak?, off-peak?)
  - Attenuating factors (e.g. redundancy, back-up measures in place)
  - Aggravating factors (e.g. visible signs of degradation, relatively long in-service life of untested device)
- Actual Harm During the noncompliance period?
  - Elaborate on the inherent design of the local system affected by the noncompliance and its ability to sustain potential outages without shedding load.

O&P Risk Example

O&P Better Impact Statement

- This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. When the maintenance testing was completed, no changes were necessary. Unmaintained VLA batteries could cause components to fail when needed and cause a generator to trip offline, potentially exasperating an ongoing real time BES situation. However, the period of noncompliance was of short duration (October-February). Also, the rated capability of the generation is approximately 2% of the Entity's Balancing Authority required Operating Reserve. In addition, the generator operated below a 15% capacity factor the last two years. The batteries missed were only 3/95 (3%) of XYZ's total protection system devices. Finally the entity regularly performed monthly visual inspection on batteries in question.

- No harm is known to have occurred.

Key Details

- The potential consequences are included
- The risk posed by this entity is more detailed
  - generating facility's performance trends
  - reference to its BA's adequate operating reserves
- Identifies other factors that mitigate risk while the noncompliance was occurring
  - noncompliance affected only off-peak operating conditions

Mitigation

- Actions and Milestones
  - Steps to end noncompliance
  - Controls that reduce risk until the noncompliance can be mitigated
  - Steps to address the root cause
  - Controls to prevent recurrence
- Mitigation Completion
  - Submit evidence upon Mitigation Completion (includes Compliance Exceptions)

Evidence Retention (Data Hold)

- Notice of Preliminary Screen
  - This letter serves as official notice to preserve all documentation pertaining to the potential noncompliance.
  - Provides an NPCC Enforcement Contact

Evidence Retention Continued

- Notice of Compliance Exceptions
  - The data retention directive provided in the Notice of Preliminary Screen shall continue and the registered entity shall maintain evidence, including mitigation evidence, related to these Compliance Exception(s) for no less than **18 months** from **the later of**: (1) the date of this Notice of Compliance Exception; or (2) the date the registered entity completes the mitigation activities.
  - NPCC may verify completion of mitigation through an audit, spot check, random sampling, or other means.

Questions?

Jenifer Vallace Farrell

jvallace@npcc.org