



The Next ICE Age Has Arrived



NPCC Compliance Workshop
November 7, 2018

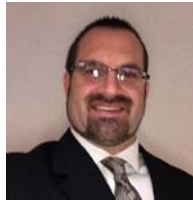
Ben Eng/NPCC
Manager, Entity Risk Assessment
*'Assuring BES Reliability through Risk
and Controls Management'*



NPCC ERA Presentation

- NPCC ERA Group
- ICE Oversight
- Process Improvements
- Process Flow Diagrams
- NPCC ICE Working Group
- NPCC Complementary Controls
- Learnings

NPCC Entity Risk Assessment

- Ben Eng – Manager, ERA 
- Duong Le – Sr. Compliance Engineer, ERA 
- Lee Budd – Risk Consultant 
(🎵 “*thanks for the memories*” 🎵)
- Mike Bilheimer – Sr. CIP Analyst 
- ICE Teams – SMEs from Audit Group
(Jim Castle, Phil Creech, John Ravalli, Will Houston,
Lou Maiocco, Jim Pirro, Emile Khan, Val Ayers)



ICE Oversight

2017 NERC Oversight Report

- Focus on ICE Team Workpapers to support conclusions in ICE Report
- Liked Process Flow Diagrams
- AFI: Wants to see more sampling of how entity determines the effectiveness of the control design.
- AFI: See more basis for the deferral of requirements from scope of upcoming engagements



ICE Oversight

2018 NERC Observation of Eversource Energy ICE

- Review of NPCC processes, tools and skilled human capital to implement IRA and ICE.
- Review of entity submittals, onsite walkthrough, NPCC ICE team workpapers and draft ICE Summary Report.
- Review of communication between NPCC ICE Team results and NPCC Compliance Audit Team.

ICE Oversight

2018 NERC/FERC 2 day IRA/ICE meeting

- Review of processes, tools and skilled human capital to implement IRA and ICE.
- Review of 2 recent ICE – entity submittals, NPCC ICE team workpapers, NPCC ICE Summary Reports.
- Confirmation of NPCC's improvements
- Acknowledge the role of Complementary Controls offered by NPCC.



ICE Oversight

2018 NERC Internal Audits Group and CCC audit of NPCC ICE

- Questionnaire answers and supporting documentation provided to NERC via NPCC secure portal upload on October 30, 2018.
- Meeting scheduled for December 13th 2018
- CCC attendees (2) not from the NPCC Region



Process Improvements

2017 NERC Oversight

- NPCC: Developed Workpaper Forms for ICE Team capture of documentation demonstrating entities' implementation and effectiveness of controls.
- NPCC: Developed ICE Working Group
- NPCC: Proposed the development and cataloging of NPCC Complementary Controls



Process Improvements

2018 NERC/FERC 2 day IRA/ICE

- NPCC: Implemented ICE Workpapers and incorporated questions into onsite ICE Walkthroughs for two entities.
- ICE Working Group developing draft template to catalog SP-7 Working Group's process flow and controls as example of NPCC Complementary Controls
- Waiting for report to capture other process improvements prior to updating NPCC ERA Compliance Instructions for IRA and ICE.



Process Flow Diagrams

- Examples provided in NPCC ERA Webinar 4/19/18, and other NPCC Workshop presentations

<https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/Forms/Public%20List.aspx>

ENTITY RISK ASSESSMENT

TYPE	TITLE	POSTED DATE
	NPCC ICE Workpaper - blank	11/6/2018
	NPCC IRA Update Template rev.2 (blank) - xls version	11/1/2018
	sample ICE Invitation Letter - 2019	10/26/2018
	2019 NERC Risk Elements and Associated Areas of Focus	10/26/2018
	Sample Flow Diagram template - CIP-010 (partial)	10/26/2018
	Sample EGO - Protection System Analysis and Misop Reporting - PRC-004	10/26/2018
	ERA NPCC 2018 Spring Workshop - ICE Better Practices, Lessons Learned, Lookahead	5/23/2018
	NPCC ERA ICE Better Practices 041918	4/19/2018
	ERA NPCC 2017 Fall Workshop - O&P ICE Update; CIP Risk Management	11/13/2017
	NPCC 2017 Fall Workshop - Ontario IESO Internal Controls	11/13/2017



ICE Objective

2.4.1 ICE Objective

The primary objective of ICE is to review internal controls to obtain reasonable assurance that their design and implementation better ensure compliance with Reliability Standards. ICE supports more informed decisions on compliance monitoring (i.e., develop COPs or modify nature, extent, and timing of testing of compliance), facilitates selection of tailored CMEP tools, and provides direction on continuous improvement for the registered entity.

The CEA is ultimately responsible for determining whether a registered entity has internal controls that provide reasonable assurance of compliance with NERC Reliability Standards. The CEA makes this determination by understanding the BPS risks the registered entity is susceptible to and understanding how the registered entity manages or mitigates those risks.

- The **primary** purpose of ICE is **not** Scope Reduction/Deferral (although some entities still think so).
- Scope Reduction/Deferral for Compliance Monitoring is merely a byproduct of ICE fully implemented controls.
- We feel the purpose and value of ICE is to:
 - Make you more Risk Aware and understand the internal control controls and designs that mitigate risks
 - Provide a free gap analysis to help them become a **High Reliability Organization**
 - Provide non-binding recommendations to enhance entity controls to:
 - Meet/exceed compliance to the NERC Reliability Standards
 - Enhance Reliability and Resilience
- You have told us it is useful as training and succession planning
- Brings other parts of your organization together to identify and strengthen communications, handoffs and deliverables



When does ICE “Season” Begin?

2.4.2 ICE Timing and Selection of Internal Controls

The ICE process involves collaboration and coordination between the CEA and a registered entity. CEAs typically conduct an ICE outside of a compliance monitoring activity. The CEA will work with the registered entity to determine the timing of ICE activities. For example, an ICE may occur prior to a scheduled compliance audit to help refine the scope of the audit or inform testing of compliance with NERC Reliability Standards during the audit. As another example, an ICE may occur after a compliance audit if the registered entity and CEA have identified internal controls that could inform future compliance monitoring and the COP.

- “an ICE may occur prior to a scheduled compliance audit to help refine the scope of the audit or inform testing of compliance with NERC Reliability Standards during the audit.”
- “an ICE may occur after a compliance audit if the registered entity and CEA have identified internal controls that could inform future compliance monitoring and the COP.”

ICE is a voluntary process, and registered entities, regardless of size, may participate in an ICE. The complexity of internal controls will vary across registered entities, and the CEA evaluation of such internal controls will be adjusted according to the registered entity’s BPS risk.



When does ICE “Season” Begin?

“an ICE may occur prior to a scheduled compliance audit to help refine the scope of the audit or inform testing of compliance with NERC Reliability Standards during the audit”

Activity for Entity - <i>Excellent Generator Operator</i> (EGO)	Target Date
NPCC’s EGO Pre-ICE Webinar: [approximately 1 week after receipt of ICE Logistics Letter] (t-185 days)*	December 2018
EGO’s ICE Worksheets, Process Flow Diagrams and Supporting Docs Completed and sent to NPCC: (t-155 days)*	January 25, 2019
ICE Team Walkthrough of EGO Controls: (t-141 days) *	February 8, 2019
ICE Summary Report Issued to EGO: (t-127 days)	February 22, 2019
EGO Audit Notification Letter: (t-120 days)	March 1, 2019
EGO Onsite Audit Start Date: (t)	July 1, 2019

* In all cases, “the sooner the better” to allow more time



Audits

- Audit interested in Pass/Fail, No Finding (NF) or Possible non-Compliance (PnC)
- Once pass/fail, NF/PnC is determined, there may be additional items provided to improve reliability (e.g. Areas of Concern, Recommendations, Suggestions)
 - RSAWs do not lend themselves to pointing out the key controls (and your monitoring their effectiveness) for meeting compliance
 - RSAWs do not credit controls to ensure “compliance” margin
 - No leading questions from auditor
- Backward looking (Audit Period)
- (New) Emphasis has been placed on the review of internal controls during compliance audits
 - (Good news) NPCC has been checking for the presence of controls during monitoring. Auditors ask for procedures, qualifications, who performs actions in a timely manner, how does the entity know when actions have been completed etc. to enable the entity to show compliance.



Internal Controls Evaluations

- Very interested in the (**preventative**) controls you have in place that enable you to ensure
 - passing the audit by meeting the requirement.
 - **exceeding** the requirements to improve reliability
- Interested in how you are aware of degradation in reliability or identify drift from compliance (**detective** controls)
- Interested in the controls in place to mitigate non-compliance once it has been confirmed (**corrective** controls)
- ICE is not Pass/Fail, it is a **Graduated Scale** (Fully, Largely, Partially...)
- Real time and forward looking
- Uses Process flow diagrams, ICE Worksheets and ICE Workpapers
- Candid conversations and Leading questions to tease out controls, identify key controls and how their implementation/testing is done
- Non-binding recommendations to improve controls
- ICE is **not** a pre-Audit
- NPCC's separate ICE prior to the engagement fosters the above.

Audit vs ICE

(Compliance vs Reliability/Resilience)

- Does being compliant mean you are reliable?
- Does being compliant mean you have controls in place to remain compliant?
- Can you develop controls to meet/exceed compliance?
- Are there controls offered by 3rd parties that complement reliability?



Let's have an audit of PRC-004

1. **Title:** Protection System Misoperation Identification and Correction
2. **Number:** PRC-004-5(i)
3. **Purpose:** Identify and correct the causes of Misoperations of Protection Systems for Bulk Electric System (BES) Elements.
 - R1. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated under the circumstances in Parts 1.1 through 1.3 shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation: *[Violation Risk Factor: High][Time Horizon: Operations Assessment, Operations Planning]*
 - 1.1 The BES interrupting device operation was caused by a Protection System or by manual intervention in response to a Protection System failure to operate; and
 - 1.2 The BES interrupting device owner owns all or part of the Composite Protection System; and
 - 1.3 The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation or was caused by manual intervention in response to its Protection System failure to operate.



Audit Results

- Entity A (GO) has not had a protection system operation since it began operation 6 years ago. It has been a record run. Therefore there have been no protection system operations to analyze during the audit period nor any misoperations to report.
- Audit result: No Finding



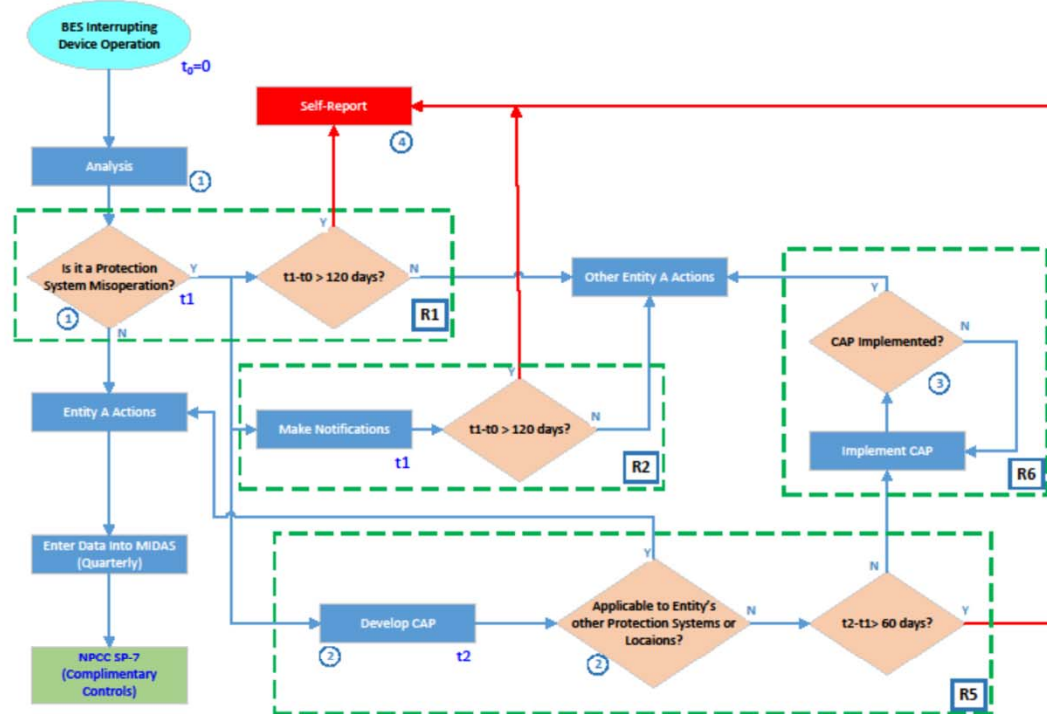
Let's talk controls

- Does being compliant mean you are reliable?
- Do you have any controls in place to remain compliant?
- Do you have evidence on implementation, monitoring, or determining the status/effectiveness of the control?
- Are there controls offered by 3rd parties that complement reliability?



Process Flow Diagram – PRC-004

Entity A (GO) – PROTECTION SYSTEM OPERATIONS/ANALYSIS



LEGEND:

Policies and Procedures

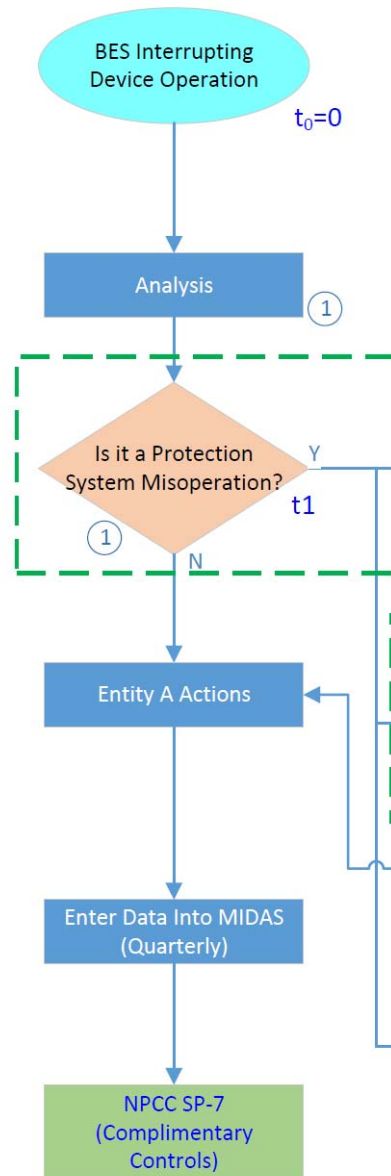
- ① EGO-PCE-001, Protection System Analysis, Rev. 0
- ② EGO-PCE-002, Corrective Actions, Rev. 1
- ③ EGO-PLN-007, Plant Modifications, Rev. 13
- ④ EGO-CMPL-003, Potential Non-Compliance and Self Reporting, Rev. 3

- R1. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated under the circumstances in Parts 1.1 through 1.3 shall, within 120 calendar days of the BES interrupting device operation, identify whether its Protection System component(s) caused a Misoperation; [Violation Risk Factor: High] [Time Horizon: Operations Assessment, Operations Planning]
- 1.1 The BES interrupting device operation was caused by a Protection System failure or by manual intervention in response to a Protection System failure to operate; and
- 1.2 The BES interrupting device owner owns all or part of the Composite Protection System; and
- 1.3 The BES interrupting device owner identified that its Protection System component(s) caused the BES interrupting device(s) operation or was caused by manual intervention in response to its Protection System failure to operate.
- R2. Each Transmission Owner, Generator Owner, and Distribution Provider that owns a BES interrupting device that operated shall, within 120 calendar days of the BES interrupting device operation, provide notification as described in Parts 2.1 and 2.2.
- R5. Each Transmission Owner, Generator Owner, and Distribution Provider that owns the Protection System component(s) that caused the Misoperation shall, within 60 calendar days of first identifying a cause of the Misoperation; [Violation Risk Factor: High] [Time Horizon: Operations Planning, Long-Term Planning]
 - Develop a Corrective Action Plan (CAP) for the identified Protection System component(s), and an evaluation of the CAP's applicability to the entity's other Protection Systems including other locations; or
 - Explain in a declaration why corrective actions are beyond the entity's control or would not improve BES reliability, and that no further corrective actions will be taken.
- R6. Each Transmission Owner, Generator Owner, and Distribution Provider shall implement each CAP developed in Requirement R5, and update each CAP if actions or timetables change, until completed; [Violation Risk Factor: High] [Time Horizon:

Let's talk controls (cont'd)

- Does being compliant mean you are reliable?
 - EGO provided audit evidence (no events) and controls demonstrating how they would meet compliance IF a qualifying event were to occur
- Do the requirements instill qualitative rigor to enhance Reliability?
 - Compliance = Identify misop, notify others, develop/implement Corrective Action Plan with timeliness criteria

But wait.... There's more!

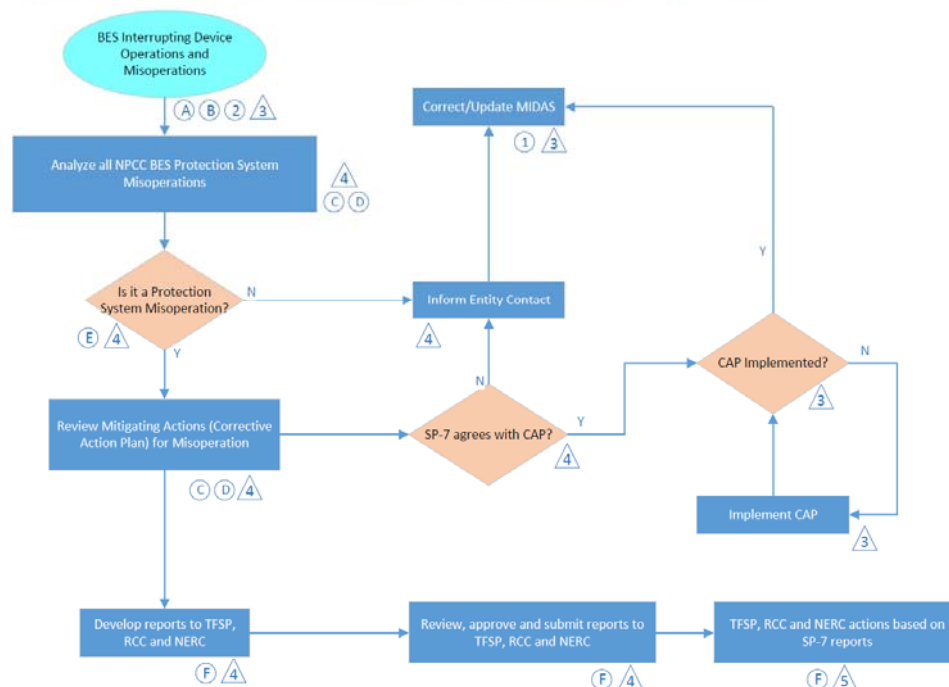


- Are there controls offered by 3rd parties that complement reliability?

What is this?

Process Flow Diagram – SP7

NPCC SP-7 WORKING GROUP – PROTECTION SYSTEM OPERATIONS/ANALYSIS [Complementary Controls]



LEGEND:

Policies and Procedures

- (A) NERC Introduction to Misoperation Information Data Analysis System (MIDAS)
- (B) NERC RoP Section 1600 Data Request, *Request for Data or Information, Protection System Misoperation Data Collection*
- (C) NPCC SP-7, Scope
- (D) NPCC C-45, Procedure for Analysis and Reporting of Protection System Misoperations
- (E) NERC Glossary and Q&A for Misoperations
- (F) Adequate Level of Reliability ALR 4-1 Correct Protection System Operations

Tools and Skilled Human Capital:

- (1) NERC Misoperation Information Data Analysis System (MIDAS)
- (2) MIDAS/SPCS Reporting Templates (Tab 1, Operations; Tab 2, Misoperations)
- (3) NPCC Registered GOs, TOs, DPs
- (4) NPCC SP-7 Roster (Protection System Engineers, various entities and NPCC)
- (5) NPCC Task Force System Protection (TFSP)



Governance – SP7

From SP7 Scope

Responsibilities

- Review the analysis of misoperations of protection systems on the bulk electric system to ensure a misoperation cause has been identified by the system protection owner. This review will determine whether further analysis or data is needed. Based on the data submitted by the entities, SP-7 will confirm that the event is a misoperation and all applicable data has been submitted. The SP7 review comments will be communicated to the entity. After a consensus is reached the misoperation report will be transferred by NPCC to NERC as part of the quarterly submission.

From NPCC Guide C-45

The NPCC Protection System Misoperation Review Working Group SP-7 will review all BES Protection System Misoperations on behalf of the Task Force on System Protection (TFSP) and the Chair of the SP-7 will report to the TFSP at each meeting in accordance with the SP-7 Terms of Reference (work scope). For Misoperation causes involving relay system malfunctions, the review will confirm that mitigation is defined and scheduled in order reduce the potential for Misoperation reoccurrence.



Controls Questions for the NPCC SP-7 Working Group's ICE

- How does the entity know to enter Operations and Misoperations data into MIDAS quarterly?
- What if the entity forgets to provide quarterly data?
- How often does SP-7 meet? Do they review all misoperations that occur during each quarter?
- How does SP-7 maintain its expertise?
- Obtain proof that they do their analysis and reporting on a regular basis as specified in their charter, policies, procedures, guides etc.
- What ensures consistency for input, analysis and output?
- Who has oversight over SP-7?
- How often are reports provided to TFSP, RCC and NERC?
- How does SP-7 act as a Complementary control to enhance reliability?

Audit vs ICE (Compliance vs Reliability/Resilience)

- The Registered Entity is still responsible for meeting its Compliance obligations or Self-Log, Self-Report as necessary.
- Being compliant to the requirement may not enhance reliability
- Be cognizant of Complementary Controls offered by NPCC Task Forces and Working Groups to enhance Reliability and Resilience

ICE Working Group

- Has taken on the challenge to develop a catalog of **Complementary** controls offered by other NPCC Task Forces and Working Groups
- The process flow diagram, governance, and controls questions and answers for SP7 activities will be captured and documented.
 - These will be used as a template for other NPCC TFs, WGs that enhance Reliability and Resilience. (e.g. SS-37, SS-38)
- It will be made clear that the Registered Entity is still responsible for meeting its Compliance obligations or Self-Log, Self-Report as necessary.
- ICE Working Group and NPCC ERA Group collaborative effort



What is Reasonable Assurance?

As described in the ERO Enterprise Guide for Compliance Monitoring⁵, the ERO Enterprise recognizes that internal controls cannot provide absolute assurance of compliance with Reliability Standards. CEAs may modify the nature, timing, or extent of compliance monitoring activities based on their understanding and evaluations of internal

The NERC ICE Guide acknowledges that “internal controls **cannot** provide absolute assurance of compliance with NERC Standards”

Reasonable* Assurance: Conclusions based on evidence that is sufficient and appropriate to support the CEA’s conclusions. **Note: Emphasis on “reasonable”, not “complete” or “absolute” assurance.*

Walkthrough: A procedure used during an evaluation of an entity's internal control to gauge the effectiveness of an internal control. A walkthrough traces a process step-by-step from its inception to the final disposition.



Assessment Criteria

- NPCC ICE team review of entity ICE worksheets and supporting documents
 - Offsite review (develop questions, actions for onsite walkthrough)
 - Onsite ICE walkthrough and interviews (“tease out” and document “unacknowledged/taken for granted” control designs)

Assessment Criteria

The CEA may use a binary effective/not effective method for assessing implementation effectiveness, or it may use a measured approach to assess internal control implementation. CEAs should have a documented methodology for assessing implementation, and this methodology may include, but is not limited to, the following:

- The automation of internal controls
- Compensating and supporting internal controls
- Registered entity identification of key controls
- The level of available internal control documentation
- Peer review of key controls within the registered entity
- Feedback on control design processes
- Registered entity’s internal review and testing of existing internal controls

Internal Controls

- Attributes of good controls design
 - Address Single Point of Failure
 - redundancy/alternate means to achieve objective
 - Confirmation of expected actions or timely response
 - Layering - Institute of Internal Auditors strongly suggests combination of all three types (P, D, C).
 - Enables consistency, repeatability, resiliency
 - Automation, early warning reminders
 - Frequent monitoring/shorter intervals

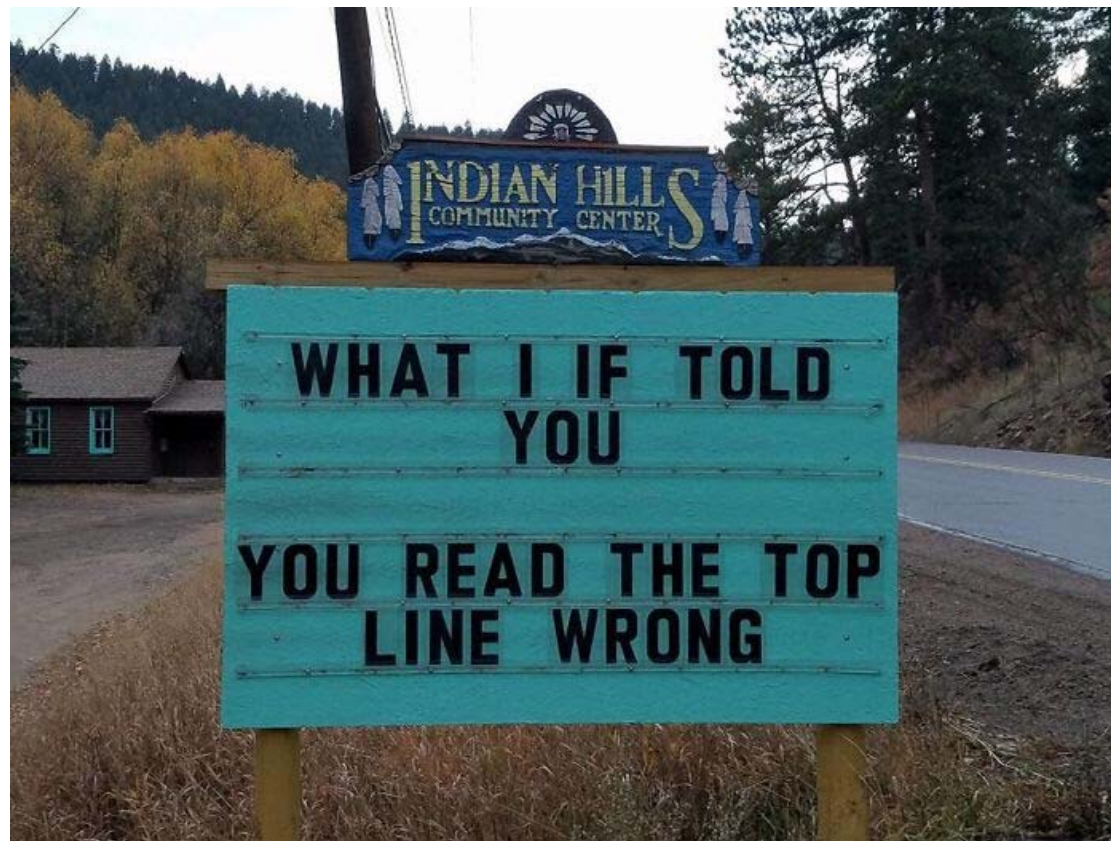


Internal Controls

"It doesn't matter in what order the letters in a word are, the only important thing is that the first and last letter be at the right place. The rest can be a total mess and you can still read it without problem. This is because the human mind does not read every letter by itself, but the word as a whole."

Someone said earlier that the brain is an amazing tool. It certainly is!

Internal Controls



But it may be a little too amazing



Lessons Learned

- Process Flow Diagrams can be segmented/modularized
- If your procedures cross reference specific NERC requirements in the body, that's a good start for building the process flow
- Independent checker to confirm the applicable 5Ws and 1H questions.
- Document implementation testing
- How do you monitor effectiveness of controls once installed?
- Controls can be overridden or degrade over time
 - Control Designs are living and dynamic, not static
 - Apply Change Management
 - Has the control objective changed?
 - Have the Risks changed?



Closing Remarks

- The 2nd ICE Age has arrived
- The future of Compliance Monitoring is being driven by the IRA and ICE processes
- Internal Controls factor into Enforcement decisions
- Compliance alone may no longer be enough to answer whether you are Reliable and Resilient



Questions

Please email questions and/or feedback to ERA@npcc.org

More information available at NPCC ERA webpage

<https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/Forms/Public%20List.aspx>

If interested in joining the SP7 Working Group contact Rafael Sahiholamal (rsahiholamal@npcc.org)

Thank you!!!



Compliance Monitoring

John Muir

Director, Compliance Monitoring

Agenda

- 2019 Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan
- Compliance Oversight Plans (COP)
- Attestations
- Diverse and Redundant
- FAC-008-3 Field Validation
- CIP Monitoring Team Update
 - CIP Evidence Request Tool
 - BES Cyber System Questionnaire

2019 CMEP IP

- Identifies Risk elements
- Provides Areas of Focus for each Risk Element
- May be updated quarterly
- U.S. <https://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx>
- IESO and Nova Scotia follow U.S. IP
- Quebec and New Brunswick IPs are not yet final

2019 CMEP IP

2019 NERC ERO Risk Elements / Areas of Focus

- Improper Management of Employee and Insider Access
 - CIP 4, 5, 6, 7, 10 and 11
- Insufficient Long-Term Planning Due to Inadequate Models
 - FAC 2, MOD 32, 33, and TPL 1
- Insufficient Operational Planning Due to Inadequate Models
 - MOD 32, 33, TOP 3, TPL 1
- Spare Equipment with Extended Lead Time
 - CIP 14, TPL 1
- Inadequate Real-time Analysis During Tool and Data Outages
 - IRO 8, TOP 1
- Improper Determination of Misoperations
 - PRC 4
- Inhibited Ability to Ride Through Events
 - PRC 19, 23, 24, 25
- Gaps in Program
 - FAC 3, 8, PRC 5

2019 CMEP IP

NPCC Regional Risk Elements / Areas of Focus

- Improper BES Cyber System Classification
 - CIP 2
- Improper UFLS Settings
 - PRC 6 NPCC
- Failure to Report Generator Capabilities
 - MOD 25

NPCC 2019 Compliance Monitoring

- Operations & Planning Audits
 - 5 On-site Audits
 - 30 Off-site Audits or Spot Checks
- Critical Infrastructure Protection Audits
 - 8 On-site Audits
 - 34 Guided Self-Certifications (CIP-002-5.1)

Compliance Oversight Plans

- COP Template approved for ERO-wide use.
- Captures how a Region will monitor a registered entity's compliance with selected NERC Reliability Standards based on entity-specific risks.
- Does NOT change any obligation for a registered entity to be compliant with all NERC Reliability Standards.
- Will be generated for each entity that is on the schedule for 2019, and shared with the entity.
- Eventually every entity will have one.

Compliance Oversight Plans

- Contents:
 - Purpose – What it is and is not
 - Analysis and Results – Communicates identified risks for the specific registered entity
 - Oversight Strategy – Places the entity in 1 of 4 categories to prioritize compliance monitoring
 - Appendices – IRA Results Summary, ICE Results Summary, Standards / Requirements associated with identified risks

'One Time' Attestations

- ERO encourages each Region to identify Requirements that are not applicable to registered entities.
e.g. PRC-005-6, R4 - If an entity is not utilizing a performance based program for its Protection System Component maintenance.
- A process is being developed to track these attestations, with the understanding that the entity will notify NPCC if their status changes.

Diverse and Redundant

- Requirements:
 - TOP-001-4 R20, R21, R23, R24
 - IRO-002-5 R2, R3
- When evaluating “redundant and diversely routed data exchange infrastructure” and “redundant functionality”, NPCC will:
 - Determine how the registered entity understands, designed for, and constructed the data exchange infrastructure within their primary Control Center and its data center(s) to address single points of failure.
 - Ensure that redundant components are not routed through shared network infrastructure (i.e., switches, routers, and firewalls) in order to provide continued data exchange functionality during component outages.

Diverse and Redundant

- NPCC Compliance Monitoring will:
 - Address whether adequate diversity in routing has been achieved
 - Obtain an understanding of the entity's overall strategy to meet the objective of the requirements
 - Focus on possible component failure or outages rather than large impact physical events, which could trigger the entity's plans for loss of Control Center Functionality under EOP-008

FAC-008-3 Field Validation

- **What** – Field verification of installed equipment versus equipment inventory used for ratings.
- **Why** - Some registered entities have Facility Ratings based on inaccurate equipment inventories, or ratings are not being updated during projects or following severe weather.
- **When** – During an audit.
- **How** – Process is still being refined. In addition to the data requested in the RSAW
 - Request for list of BES facilities
 - Select BES facilities and equipment for field verification
 - Request detailed drawings and ratings
 - Perform field inspection



CIP Monitoring Team Update

David Cerasoli, CISSP
Manager, CIP Audits

Agenda

- CIP Evidence Request Tool
- BES Cyber System Questionnaire
- Q & A



CIP Evidence Request Tool

Background Information

- Evidence Request Tool (ERT) was created in 2016
- Initially not all Regional Entities used it
- Development of the 2nd version of the ERT (ERTv2) began in late 2017
- Input for the ERTv2 was solicited from auditors from all Regional Entities
- ERTv2 was reviewed by CIPC and CEIWG, and approved for use in August

Background, Cont.

- As part of NERC's efforts to better align the ERO all Regional Entities will use the ERTv2
- NPCC will begin using the ERTv2 next year for all onsite CIP audits

Handling and Retention of Evidence

- You will be asked to upload all audit submittals including the ERT to NPCC Drive
- The Primary Auditor will move your submittal to a secure server that is owned, maintained and physically resides in a protected zone within NPCC's office
- Access (electronic and physical) to this server is highly restricted
- All evidence is handled and retained in accordance with applicable NPCC policies and procedures
- NPCC will maintain the official audit record

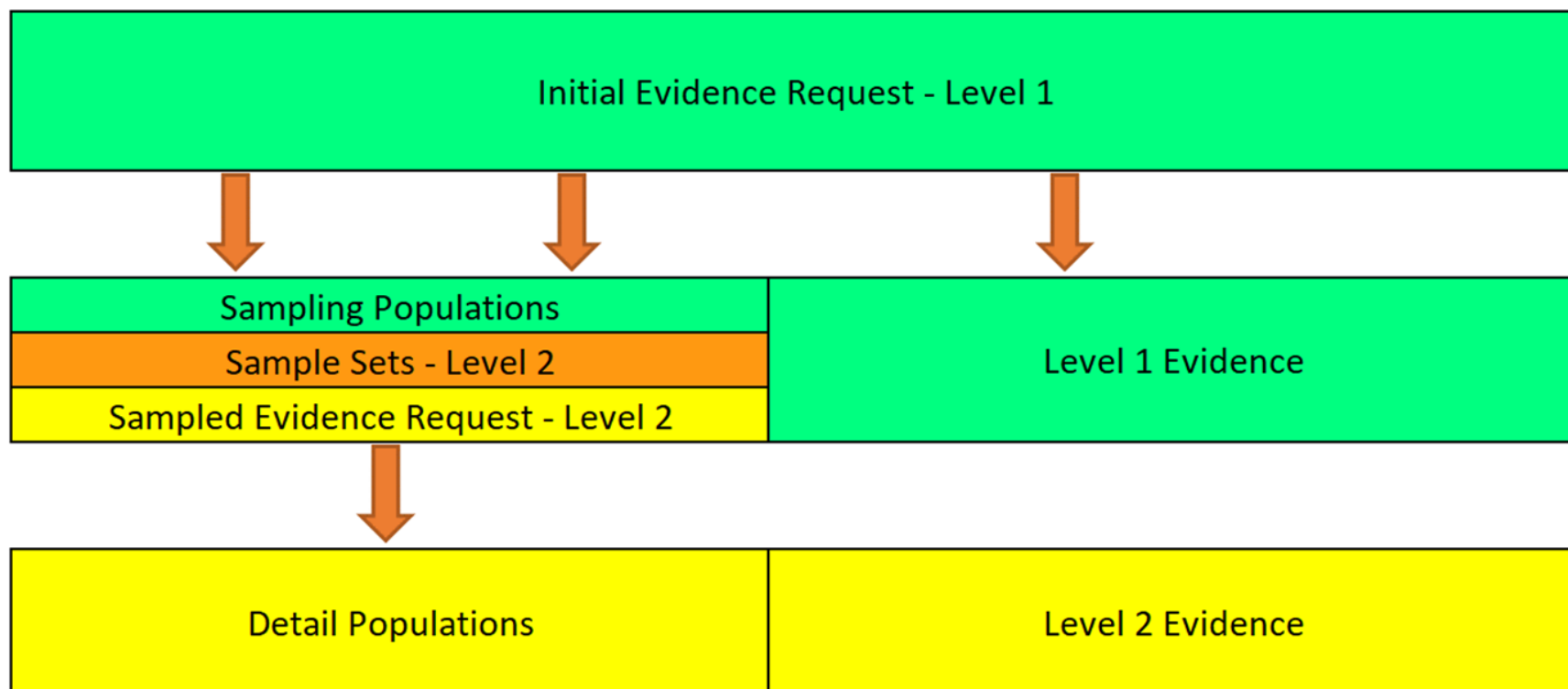
What is the ERT?

- The ERT is a common request for information that will be available for use by all regions
- It will help the ERO be more consistent and transparent in its audit approach
- It will help entities (especially those in multiple regions) fulfill requests more efficiently by understanding what types of evidence are useful in preparation for an audit

The ERT's Structure

- An Excel workbook with 19 worksheets or tabs
- 4 tabs contains evidence requests
- 14 tabs are to be completed by the audited entity

Evidence Request Flow



Key Pre-Audit ERT Milestones

Day 0: You will receive the Audit Notification Letter

Day 30: Pre-audit Survey and Level 1 requests are due

Day 90: RSAWs and supporting evidence, Level 2 requests and NPCC specific requests are due

Day 104: You may receive 'Level 3' requests, which are requests beyond what is in the ERT

Day 114: Responses to 'Level 3' requests are due

Day 120: Onsite portion of audit begins

Handling of Level 3 Requests and Beyond

- Level 3 requests and beyond will be tracked using NPCC's Evidence Tracking Sheets (ETS), which many of you are already familiar with
- Level 4 requests and beyond would be considered onsite requests

Additional Notes

- You will still be required to submit RSAWs, but you can cite any evidence that you may have already supplied in response to an ERT request in your RSAW so that you don't have to submit the evidence twice
- In addition to any cited evidence you may have already provided, you may need to provide a supplemental submittal to support your RSAW responses

Additional Notes, Cont.

- You may use NERC's ERTv2, but NPCC has developed its own ERT
- Our ERT is very similar to NERC's with two main differences:
 - It has a tab with requests specific to our region
 - Some of the tabs contain two additional columns
- Of note is one of these columns, 'Entity Response',
- This column was added after feedback from our entities that they would appreciate an opportunity to explain the relevance of a piece of evidence
- The NPCC ERT is available on NPCC's website
- You will receive a copy of the ERT along with the associated user guide when you receive your Audit Notification Letter



Finally - Don't panic.

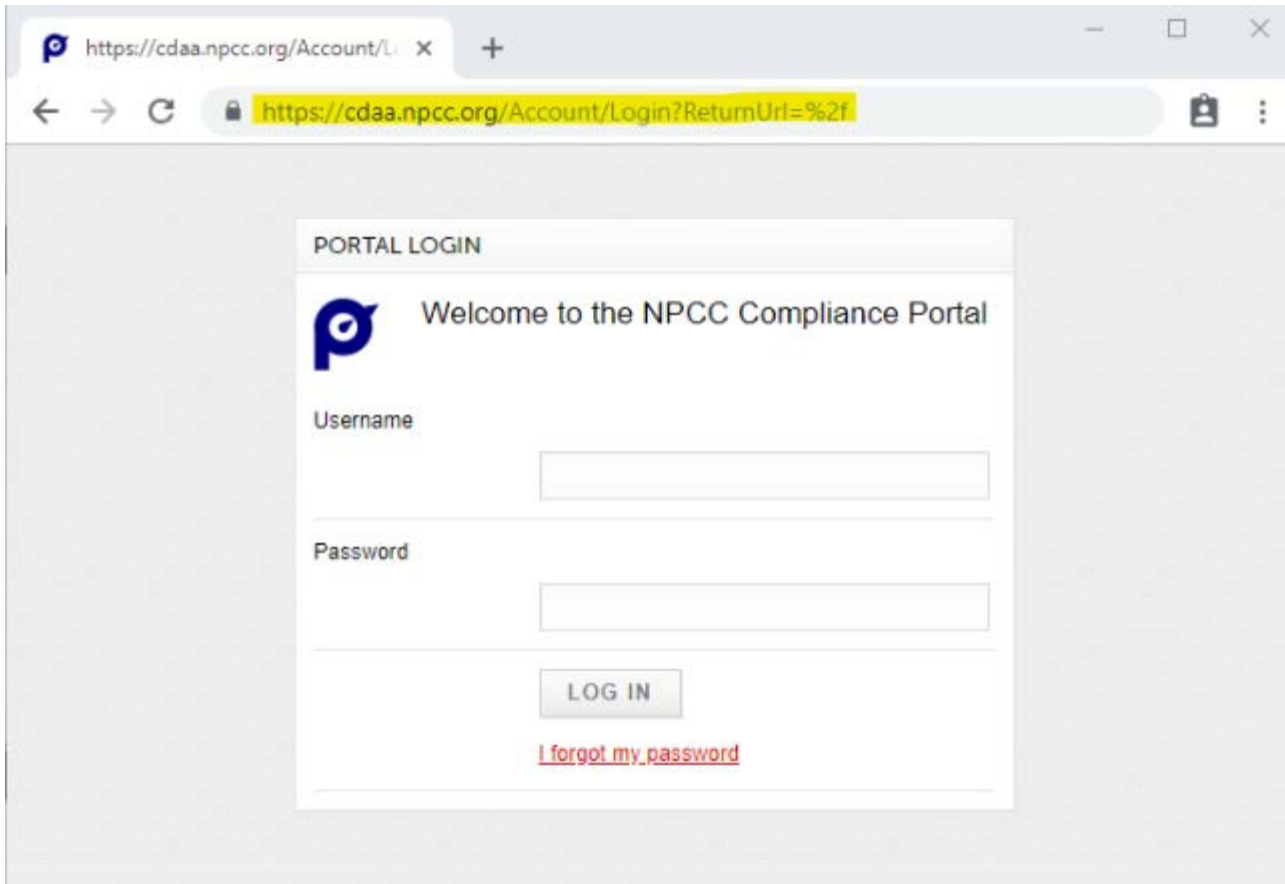
Our ERT and process may change as we gain more experience with it - **so we welcome your feedback!**



BES Cyber System Questionnaire

- Located in the CDAA on your Company Info page
- Replaces the previous questions that asked you to indicate whether you had CCAs
- Three new questions:
 - Do you have high impact BES Cyber Systems?
 - Do you have medium impact BES Cyber Systems?
 - Do you have low impact BES Cyber Systems?
- Responses are simply 'Yes' or 'No' and will only be used for planning purposes (audits, self-certs, etc.)
- We would greatly appreciate your responses by February 1, 2019

Step 1 – Login to the CDAA



A screenshot of a web browser displaying the NPCC Compliance Portal login page. The browser's address bar shows the URL <https://cdaa.npcc.org/Account/Login?ReturnUrl=%2f>. The page content includes a header "PORTAL LOGIN" and a welcome message "Welcome to the NPCC Compliance Portal" next to the NPCC logo. Below this, there are input fields for "Username" and "Password", a "LOG IN" button, and a red link that says "I forgot my password".

<https://cdaa.npcc.org>

Step 2 – Go to Company Info

 **NPCC Compliance Portal**

HOME
SYSTEM ADMINISTRATION

- > Change Password
- > My Contact Information
- > Search Contacts
- > Add New Contact
- > **Company Info**

TFES
SELF-CERTIFICATIONS
SELF-REPORTS
SCOPE EXPANSIONS
COMPLAINTS
MITIGATION PLANS
NON-COMPLIANCE
PERIODIC DATA SUBMITTALS
QUESTIONNAIRE

EDIT ENTITY: A TEST COMPANY

SAVE **CANCEL CHANGES** **DELETE** **CREATE PDF**

MAILING ADDRESS

Address Line 1: 1 Window Place

Address Line 2:

City: New York

Country: US

State: New York

Zip: 10000

BES CYBER SYSTEMS

Do you have high impact BES Cyber Systems? * ☐ Yes ☐ No ☒ Unspecified

Do you have medium impact BES Cyber Systems? * ☐ Yes ☐ No ☒ Unspecified

Do you have low impact BES Cyber Systems? * ☐ Yes ☐ No ☒ Unspecified

Step 3 – Select Responses

EDIT ENTITY: A TEST COMPANY

SAVE **CANCEL CHANGES** **DELETE** **CREATE PDF**

MAILING ADDRESS

Address Line 1:

1 Window Place

Address Line 2:

City:

New York

Country:

US

State:

New York

Zip:

10000

BES CYBER SYSTEMS

Do you have high impact BES Cyber Systems? *

☐ Yes

☒ No

☐ Unspecified

Do you have medium impact BES Cyber Systems? *

☒ Yes

☐ No

☐ Unspecified

Do you have low impact BES Cyber Systems? *

☐ Yes

☒ No

☐ Unspecified

Step 4 – Save Changes

EDIT ENTITY: A TEST COMPANY

SAVE CANCEL CHANGES DELETE CREATE PDF

MAILING ADDRESS

Address Line 1: 1 Window Place

Address Line 2:

City: New York

Country: US

State: New York

Zip: 10000

BES CYBER SYSTEMS

Do you have high impact BES Cyber Systems? * ☐ Yes ☒ No ☐ Unspecified

Do you have medium impact BES Cyber Systems? * ☒ Yes ☐ No ☐ Unspecified

Do you have low impact BES Cyber Systems? * ☐ Yes ☒ No ☐ Unspecified



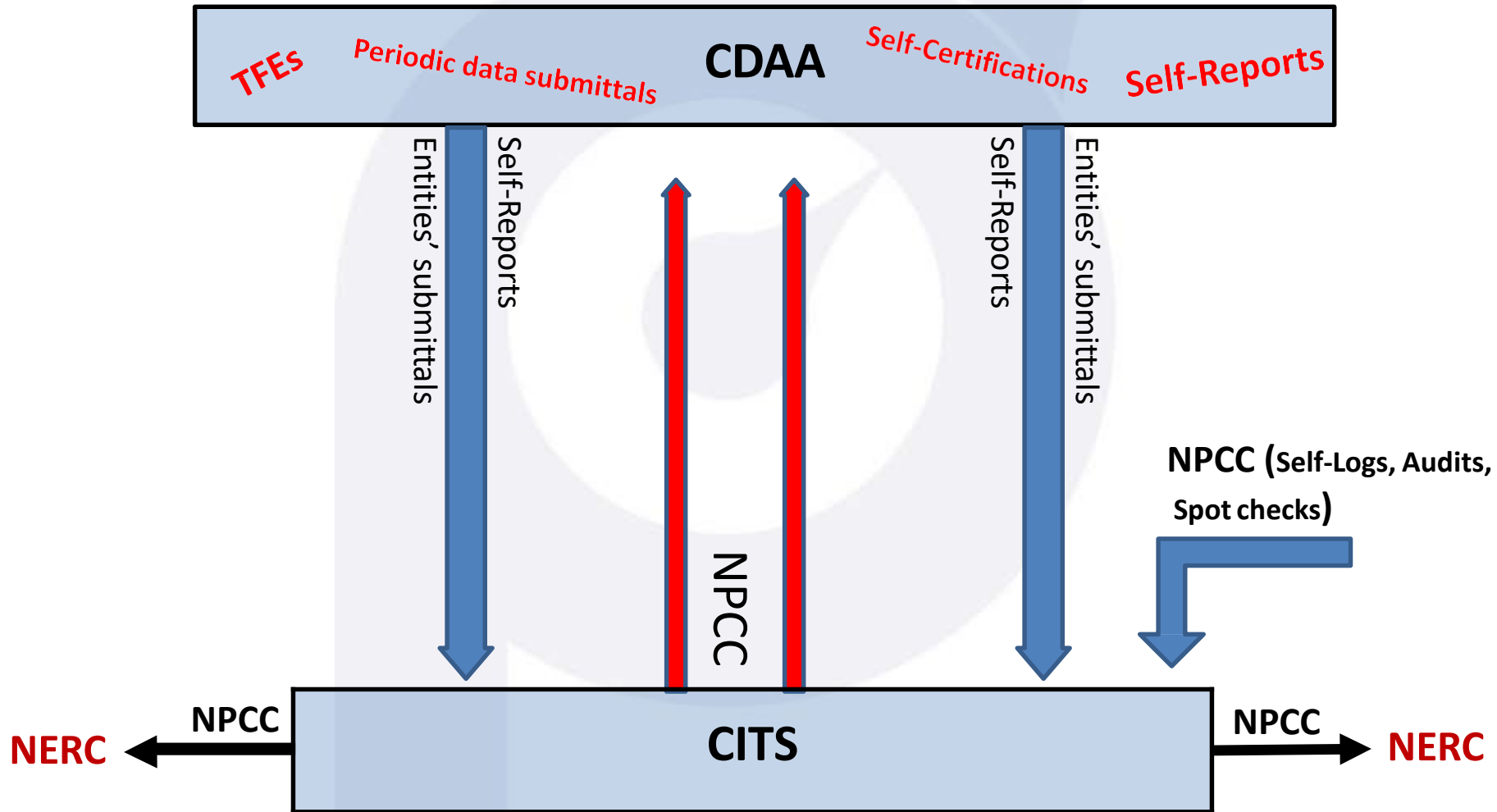
Questions?

cip@npcc.org

Enforcement Process

Francesco Elmi
November 2018
Providence, RI

Life of a noncompliance (CDAA & CITS)



Self-Report Tips

- See Registered Entity Self-Report and Mitigation Plan User Guide – June 2018
- Review previously filed non-compliances on NERC website (spreadsheets)
 - a) Details of noncompliance (description, affected devices/facilities, start/end dates)
 - b) Risk assessment
 - c) Root cause
 - d) Mitigation activities
 - Rectification of noncompliance
 - Prevent recurrence
 - e) Documentary evidence (dated & signed)

Processing Self-Logs

1. **CDA is bypassed**
2. **Entity alerts NPCC via email of a Self-Log submittal**
 - a) Description of documents uploaded in NPCC Drive
 - b) Main document: a spreadsheet similar to the one NPCC sends to NERC
 - Description of violation, Start/End, Root Cause, mitigation activities
3. **NPCC Enforcement enters noncompliance in CITS – syncs with NERC sending Self-Log spreadsheet**
 - a) NPCC ask for clarifications/additional information - NPCC issues a Notice of CE
 - Entity may re-send a new spreadsheet
 - c) NPCC does not agree on the risk
 - NPCC advises Entity of this determination
 - NPCC may issue a Notice of Possible Violation, etc.
 - d) Note: NPCC still sends its own report (spreadsheet) to NERC



Future

The new CMEP tool, Self-Logs submitted directly by Entities into this tool

Self Logging program

- Selected Entities, voluntary
- Document minimal risk issues
- Provide update to Region quarterly
- Identified issues will be (presumably) treated as Compliance Exceptions
 - *The burden is on Entity to provide a high quality report*
- Better use of entity and region resources
- 14 NPCC entities participate

Enforcement Process Steps



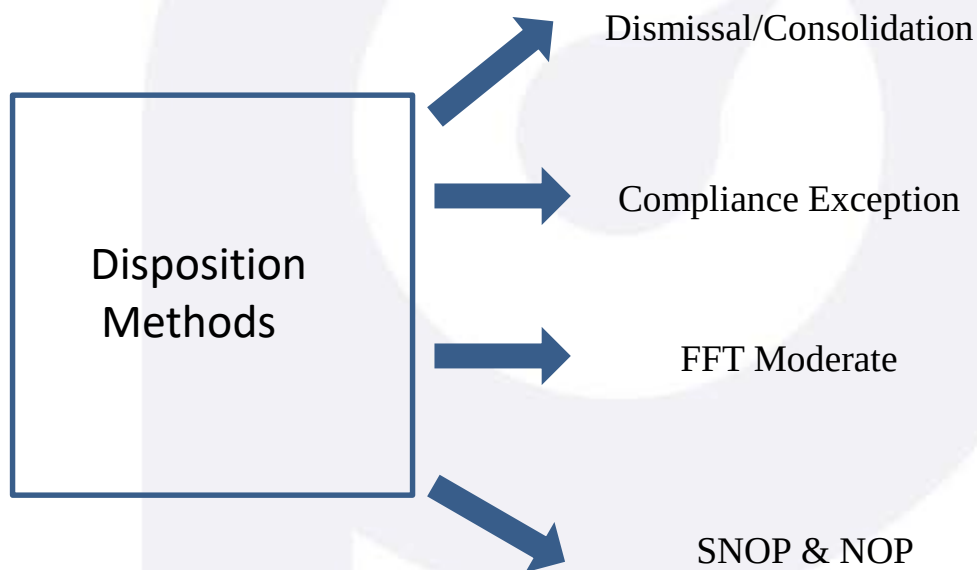
Discovery

- Screening performed by NPCC Enforcement
- Notice of Preliminary Screen
 - Assigns NERC Violation ID
 - Data Hold Notification
 - NPCC SPOC
 - Mitigation instructions

Enforcement Review and Determination

- Violation Description
 - Discovery Method
 - Standard/Requirement
 - Start/End Dates
 - Root Cause and contributing causes
- Requirement change
 - NPCC changes requirement to a more appropriate
 - Sends an email to Entity
 - Retain the same NERC Violation #
- Risk Assessment
- Mitigation Activities
- Compliance History

Disposition



Dismissal/Consolidation

- Dismissal
 - Not a non-compliance of requirement
 - Letter of Dismissal
- Consolidation
 - Identical Reliability Standard requirements for the same registered entity
 - Not always appropriate
 - Letter of Consolidation

Compliance Exceptions

- Minimal Risk only
- Self-logged items are presumably minimal and CE's.
- No NPV
- Notice of Compliance Exception
- Must be mitigated within 12 months or less.
- Certification of Mitigation Completion in CDAA required (as requested in preliminary screen)

FFTs

- Certain Moderate Risk
- Minimal Risk Violations that relate to moderate risk FFT
- NPV Issued
- Notice of FFT Issued
- Executed Affidavit required
- Certification of Completion in CDAA required

Mitigation Completion

- Mitigation activities must be completed
- Once completed, entity must certify completion of mitigating activities in CDAA
- Applies to all non-compliances and/or violations.

Mitigating Activities vs Formal MP

- Formal MP not required by any disposition method
- Timeline - Formal MP & mitigating activities
 - CEs and FFTs: 12 months from posting of spreadsheet on NERC website
 - SNOPs and NOPs: variable
- Verification – NPCC will do it for FFTs, SNOPs and NOPs

NEW

Verification of Mitigation for CEs

NEW

- NPCC Enforcement will not verify every mitigation activity associated with Compliance Exceptions.
- NPCC will sample CEs for mitigation activity verification.
- This means NPCC may ask entity for mitigation evidence AFTER Compliance Exception was processed.



CIP Enforcement

Jenifer Wallace Farrell, CISSP, CISA

CIP Self Report / Self Log

- Violation description
 - # of devices / facilities / personnel in scope
 - Names/IDs of devices/facilities/personnel
 - Where are the devices located (e.g. ESP, PSP, facility)
 - What are the devices used for
 - What type of access do the personnel have (e.g. cyber, physical, both)

CIP Self Report / Self Log

- Violation description continued
 - How was the noncompliance discovered?
 - On what date was the noncompliance discovered?
 - Root Cause
 - What control failed or was lacking

CIP Impact Statement

- Risk to the Bulk Power System
 - What can go wrong due to this violation?
 - What are the consequences when the “wrong” occurs?
- Controls Analysis
 - Preventative, Detective, and Corrective Controls
 - Compensating controls

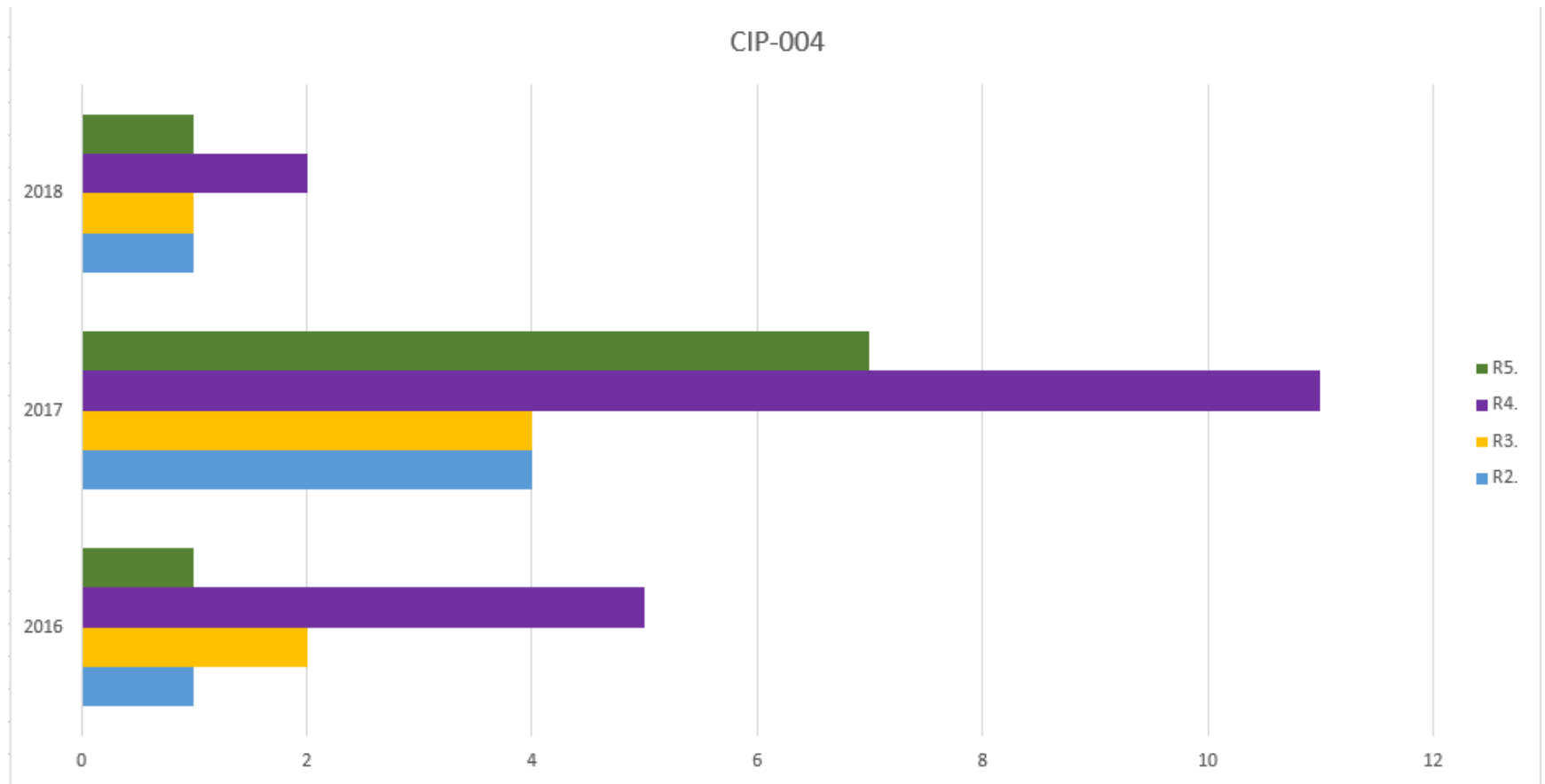
CIP Mitigation Plan

- Is the root cause addressed?
- Future Prevention
 - Identify preventative measures
 - Identify detection measures
 - Training

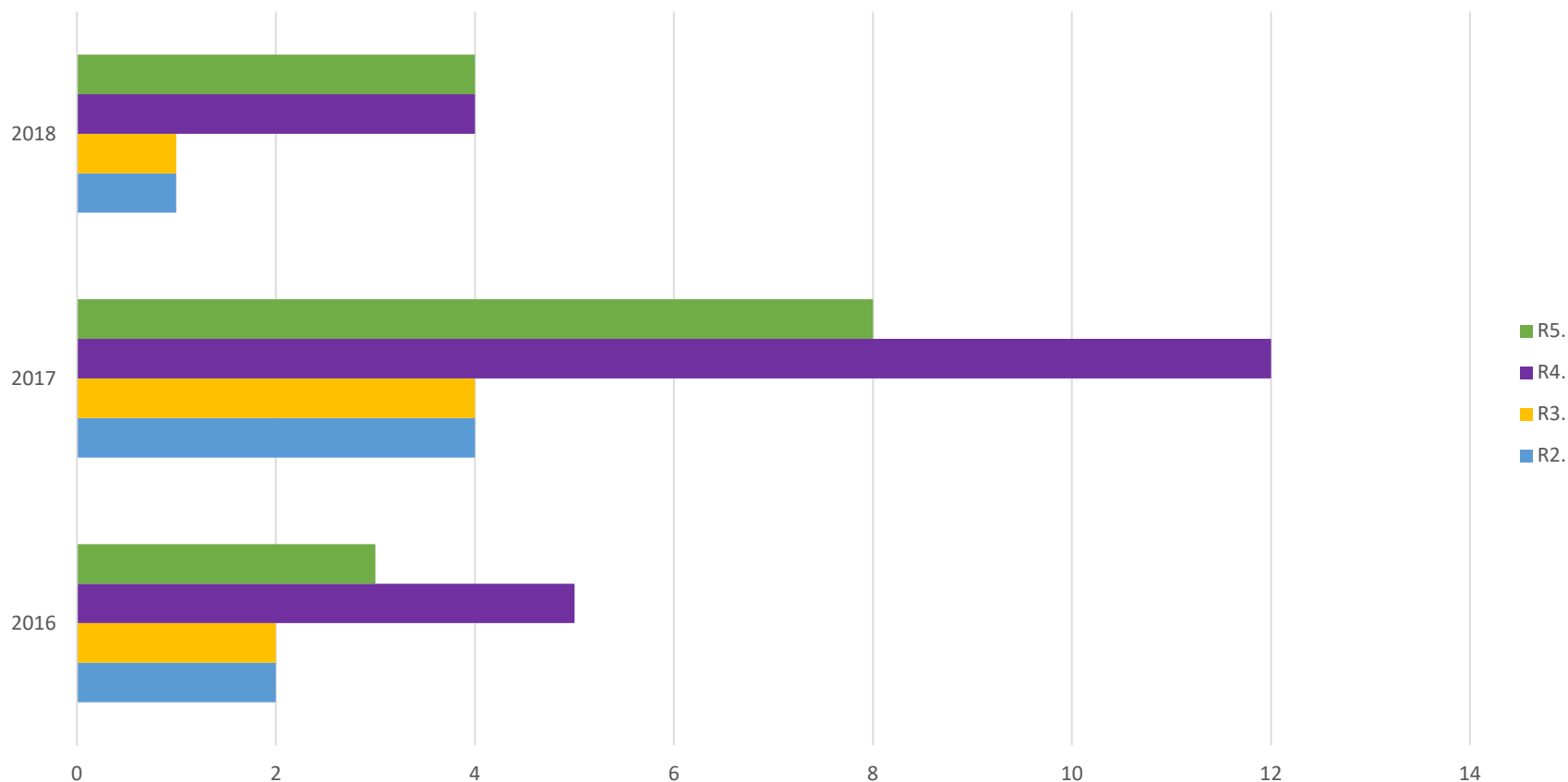
Violation Trends

- CIP-004 R4, R5
- CIP-006 R1, R2
- CIP-007 R2, R4, R5
- CIP-010 R1, R2, R3

May CIP-004



October CIP-004



CIP-004

- Common Root Causes
- R4
 - Misinterpreted the classification of the cyber asset
 - Failure to follow process when granting
 - Automated Access – system bug
- R5
 - Automated task failure
 - Management not aware of CIP Procedures
 - Failure to follow documented process
 - Use of outdated lists

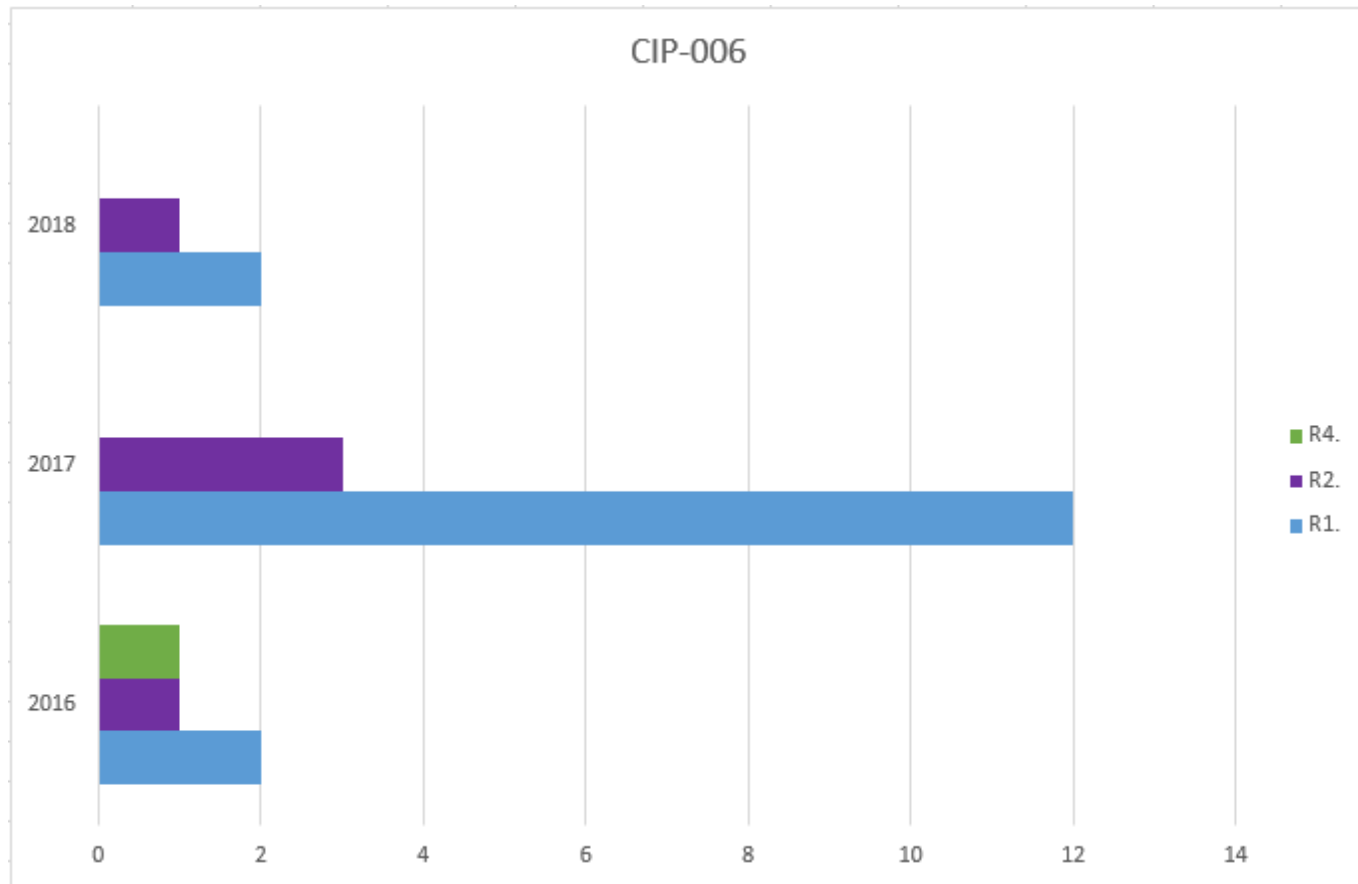
CIP-004

- Things to look for
 - Do you have a process for flagging Cyber Assets that need to be included in Quarterly Reviews?
 - Do you have a method for being alerted when an automated task fails?
 - If an automated process fails, do you have a back-up manual process?
 - Do individuals with access understand who is allowed to use the mouse/keyboard and why?

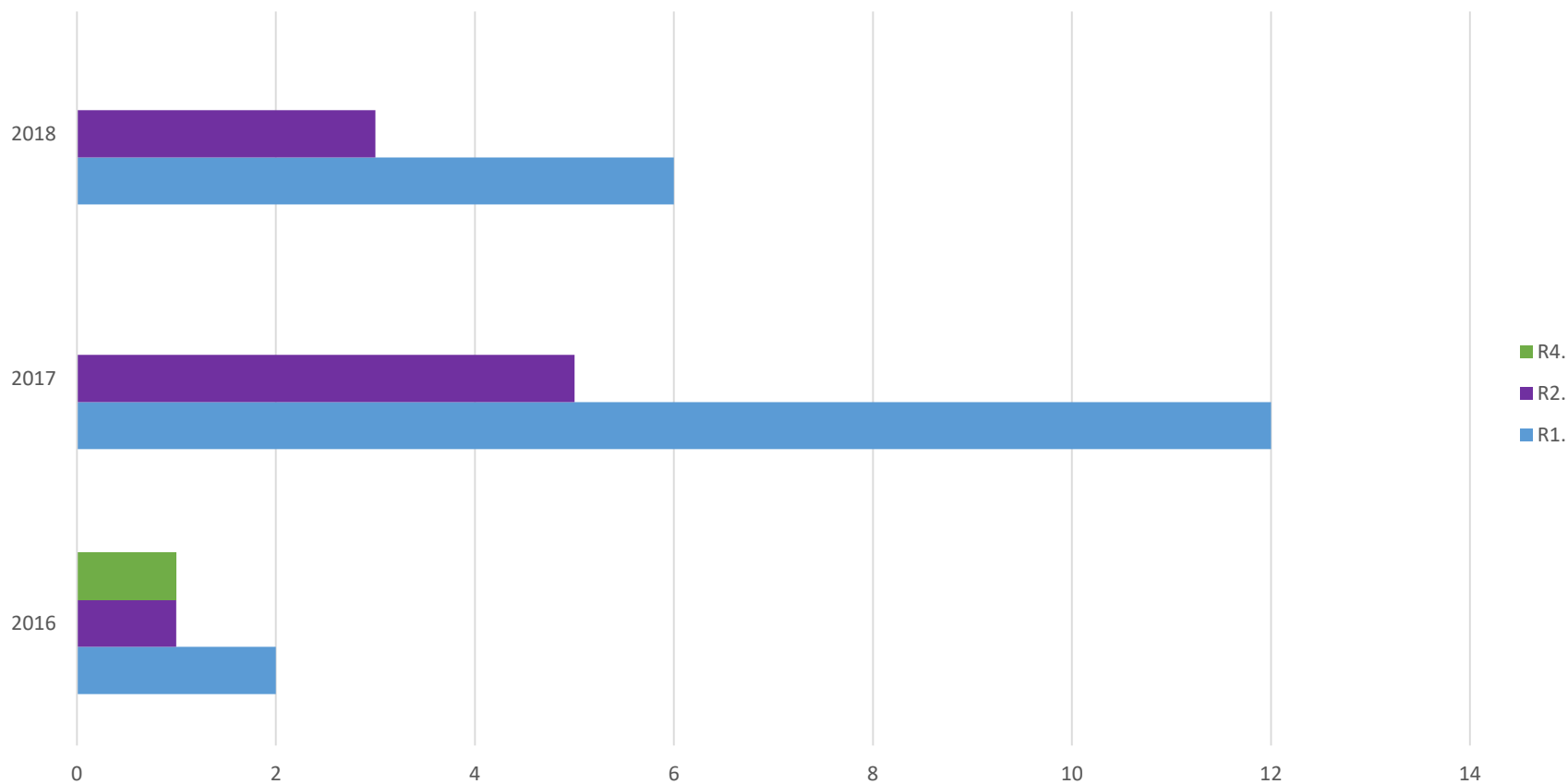
CIP-004

- Things to look for
 - Do you have clear communication between departments?
 - Do you test your tracking tool?
 - How often do you check for expiring Training/PRA's?
 - Do personnel know how to respond when they are under pressure to grant access?

May CIP-006



October CIP-006



CIP-006

- Common Root Causes
 - R1
 - Door latch malfunction
 - Authorized personnel propping doors / disabling locks
 - Asset list discrepancy
 - Lack of a process to review PSP to PSP connections
 - Failure to follow process / communicate process

CIP-006

- Common Root Causes
 - R2
 - Failure to document all required information
 - Misunderstanding of responsibilities
 - Failure to follow process
 - Lack of awareness

CIP-006

- Things to look for
 - Survey employees
 - Do they know they shouldn't prop open doors?
 - Do they know they shouldn't tape over locks?
 - Do they confirm PSP Doors, Racks and other access points are securely closed when they finish work/leave?
 - Do they know what to do if a door must be propped?
 - Do they know there is a visitor process?

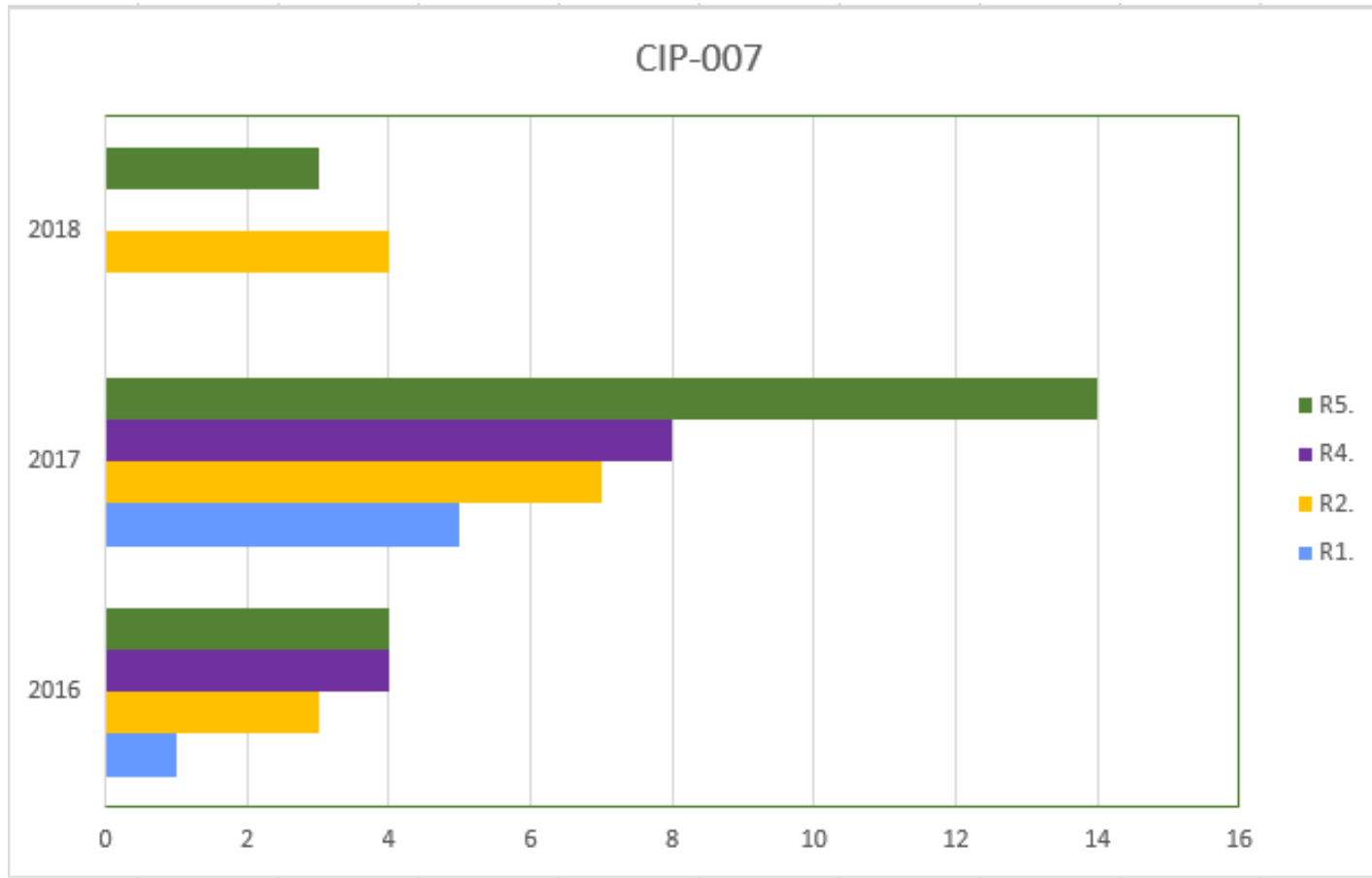
CIP-006

- Things to look for
 - How often are door latches tested?
 - Do door locking mechanisms have a delay?
 - Do personnel know how to report door issues?
- Visitors
 - How do personnel know the visitor process applies?
 - What should personnel do if they don't know how to bring a visitor into a facility?

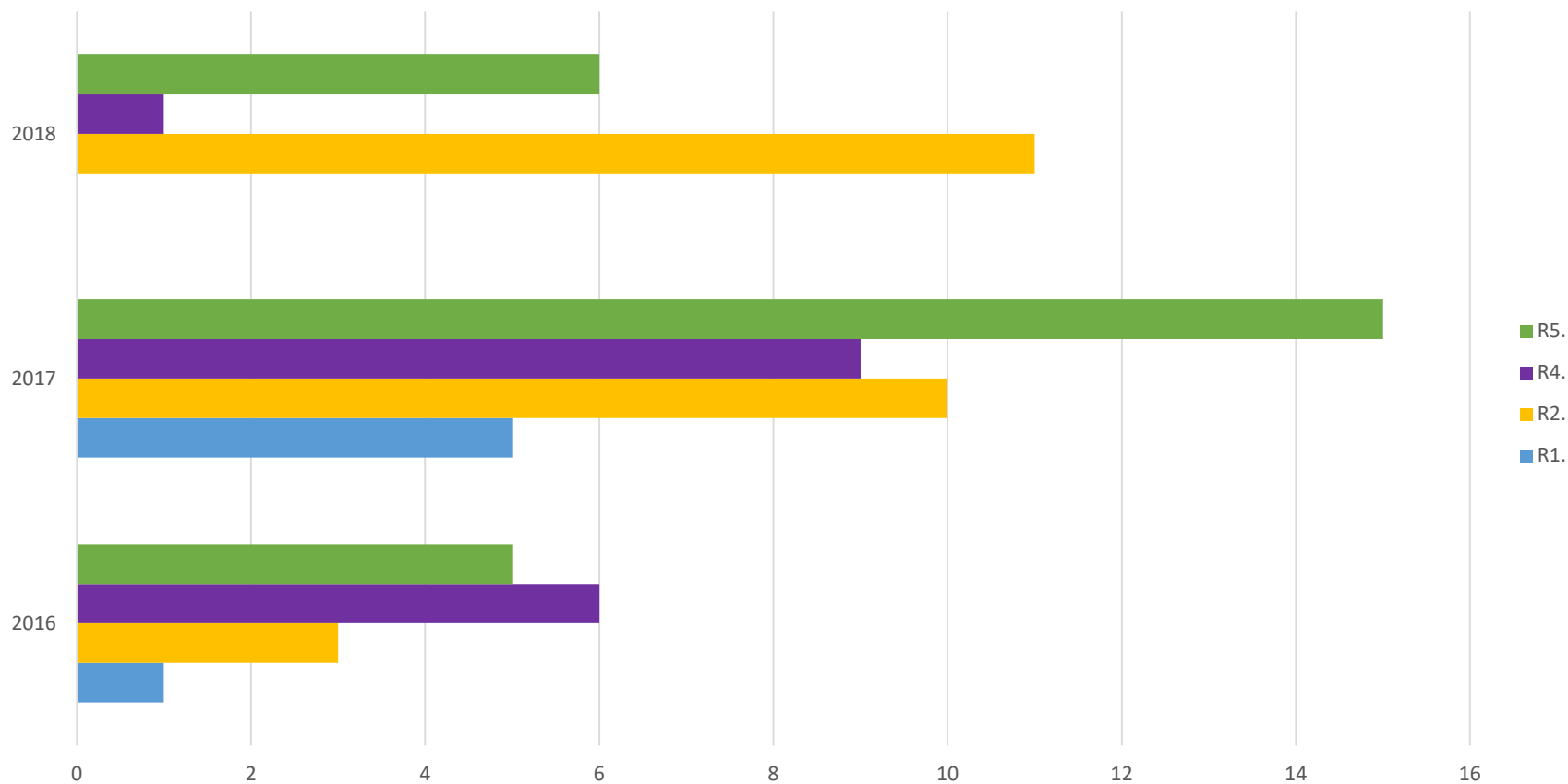
CIP-006

- Visitors continued...
 - Do your personnel know there is a process but choose not to follow it? Why? Is your process too complex?
 - Do personnel know what to do if they can't follow the regular process (off hours – not enough badges, they don't know where to go to get badges)

May CIP-007



October CIP-007



CIP-007

- Common Root Cause
 - R2
 - Misunderstanding the applicability of the requirements
 - Failure to ensure all software was tracked
 - Lack of control to ensure Mitigation Plans included actions to mitigate the vulnerabilities

CIP-007

- Common Root Cause
 - R2 continued...
 - Lack of training on patch tracking system
 - Patch evaluation reminder failure
 - Failure to request a Mitigation Plan extension
 - Failure to assign responsibility upon transfer of personnel

CIP-007

- Common Root Causes

- R4

- Misconfiguration
 - Lack of understanding of the requirement
 - lack of process/failure to verify and test logging/alerts

- R5

- Lack of understanding how policies apply to admin accounts
 - Password inventory out of date / accounts misidentified
 - No method to track password changes
 - No process to change passwords on new deployment / upgraded devices

CIP-007

- Things to look for
 - When deploying new projects / multiple assets have responsibilities been assigned?
 - Are personnel trained on the use of tools?
 - Do you test your reminder tools to ensure alerts are working?
 - Is your process clear on what to do if a Mitigation Plan date cannot be met?
 - Do you track individual responsibilities and have a method to assign responsibilities to another individual (sick, vacation, transfer)

CIP-007

- Things to look for
 - During times of heavy workload, do personnel have a process for managing workload, setting priorities and escalating issues (Daily/weekly scrum)?
 - Do you have a clear process for identifying what devices need CIP-007 controls?
 - Do you have a method for verifying and testing that logging and alerting are functional (initial deployments and after baseline changes)?

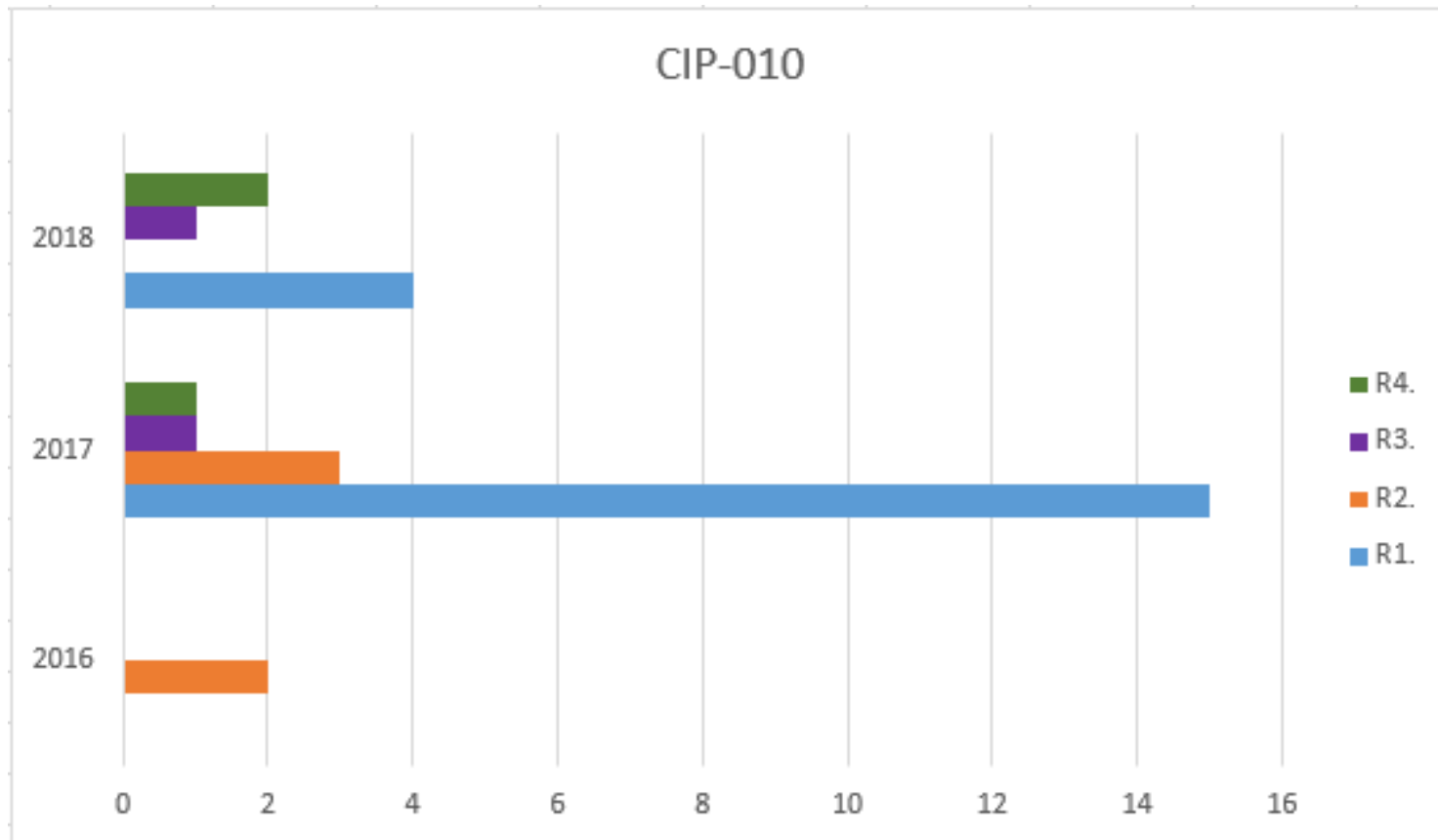
CIP-007

- Things to look for
 - Do you have a job aid for all applicable device types that describes how to enable logging / adjust settings?
 - Does your logging set-up process include a validation step?
 - Do you have a method to alert for detected failure of event logging?
 - Do you have a method to identify all application accounts and default shared accounts within applications?

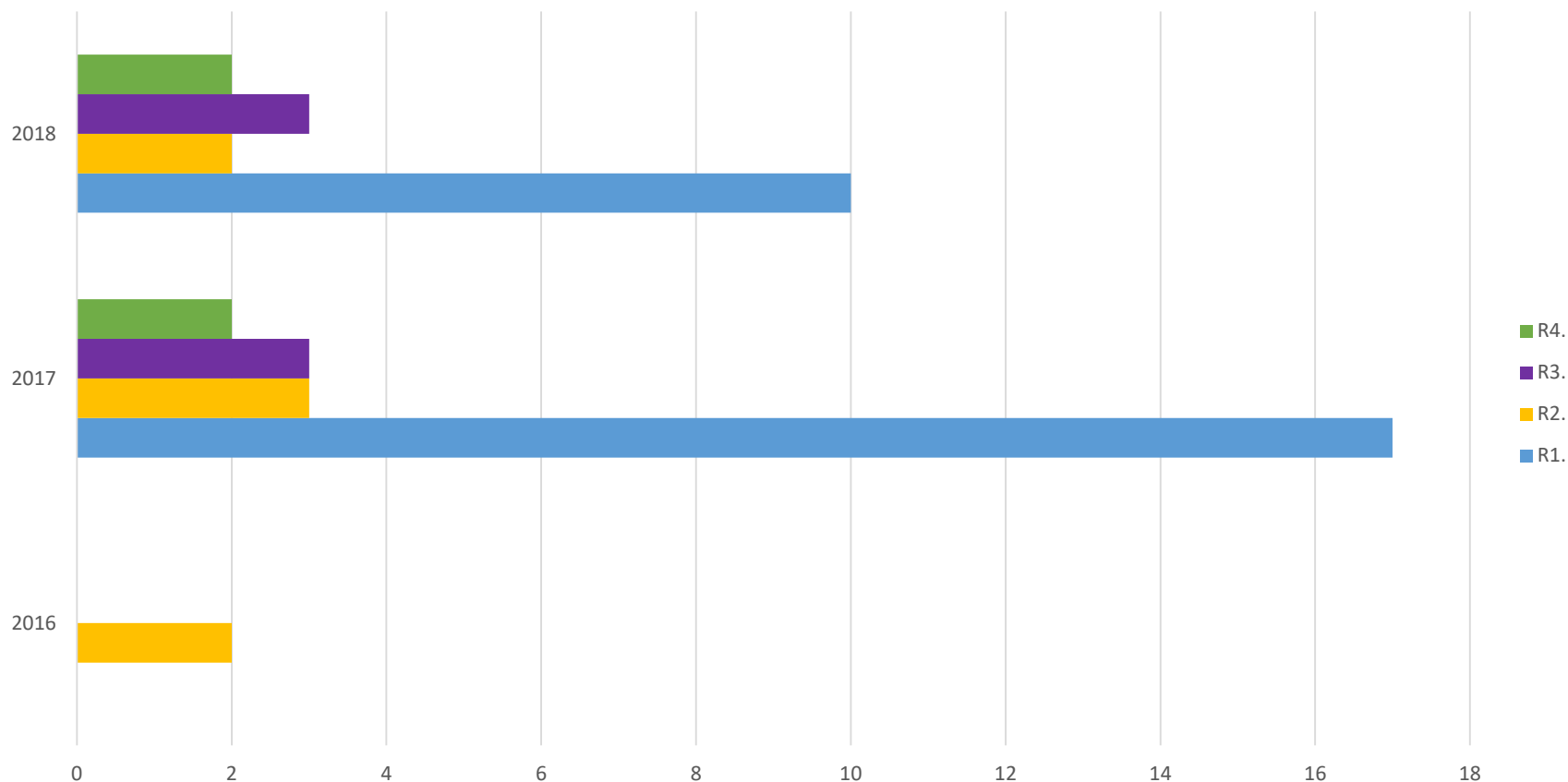
CIP-007

- Things to look for
 - Does your current process ensure all applicable accounts are identified and inventoried?
 - Do you have a method for checking the timeframes for password changes that are enforced procedurally?
 - Do personnel know what requirements need to be implemented when installing new/replacement devices (What if the replacement device has more functionality than the prior TFE'd device)?

May CIP-010



October CIP-010



CIP-010

- Common Root Causes

- R1

- Lack of understanding what should be a PACS, EACMS, PCA
 - Lack of control to ensure all baseline elements are collected
 - Insufficient training on new technology
 - Lack of awareness, communication and oversight
 - Lack of a process for requiring CIP compliance evaluations prior to performing system restoration or troubleshooting tasks.

CIP-010

- Common Root Causes
 - R2
 - Individual responsible out of office
 - Individuals responsible for monitoring forgot
 - Failure to follow documented procedures
 - Lack of a process for identifying communication failures
 - R3
 - Lack of a process to perform paper or active assessment
 - Lack of a process and controls to ensure vulnerability scans and mitigation plans were coordinated and completed.

CIP-010

- Things to look for
 - Do your personnel have a clear understanding or have job aid or process for identifying PACS, EACMS, and PCAs?
 - Does someone have assigned responsibility for completing a baseline for new/updated assets?
 - Do you have a process to identify new substation projects?

CIP-010

- Things to look for
 - For manual baseline collection, do personnel have a clear understanding or job aid for what they should be collecting and documenting?
 - Have personnel been trained on how to use new technology and how to identify errors?
 - Have personnel been trained on what job tasks require authorization?
 - Do personnel have a job aid for identifying changes that deviate from the baseline?

CIP-010

- Things to look for
 - Raise awareness that system restoration and troubleshooting tasks can lead to baseline changes
 - Do personnel know what adequate evidence is when it comes to demonstrating testing?
 - During times of heavy workload, do personnel have a process for managing workload, setting priorities and escalating issues (Daily/weekly scrum)?

CIP-010

- Things to look for
 - Do you have a process to re-assign compliance tasks when responsible individuals are out of the office?
 - Do you have methods for reminding and escalating incomplete work tasks before you are in noncompliance?

CIP-010

- Things to look for
 - Do you have a process for identifying device communication failures before you are in noncompliance with the 35 calendar days monitoring?
 - If your monitoring process fails, are alerts going to more than 1 person? (in the event that the responsible individual is out of the office)
 - Do you have a paper and a active vulnerability assessment process documented?

CIP-010

- Things to look for
 - Do you have a process to ensure vulnerability scans and mitigations plans are coordinated and completed?
 - Do you have a method for identifying control failures on TCA's?
 - Have contractors been trained on your TCA and Removable media processes?
 - Do personnel have a way to identify who is authorized to use a TCA?

Questions?

Jenifer Wallace Farrell, CISSP, CISA

Senior CIP Analyst

jvallace@npcc.org

Non Compliance: Trends and Prevention

NPCC Mitigation and Enforcement Team

November 7, 2018 Providence, RI

Scott Nied

Total Number of Non Compliances Discovered in NPCC (10/29/18)

Total Noncompliances by Year

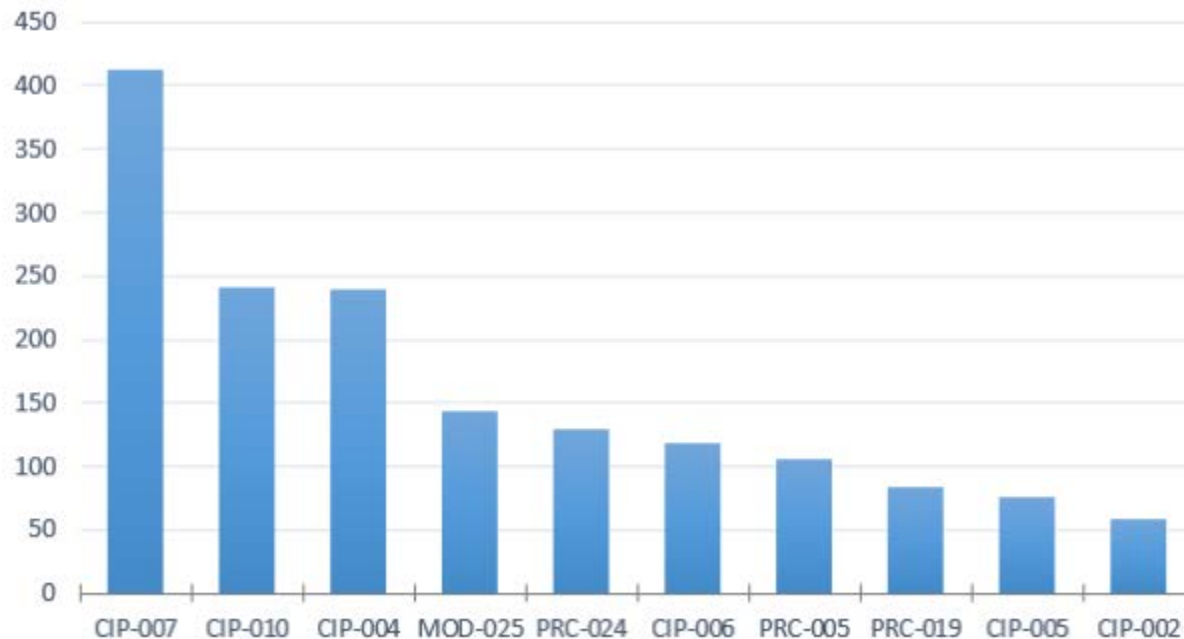


United States 2018 by Region

Table A.2: Noncompliance Discovered in 2018

Discovery Month	FRCC	MRO	NPCC	RF	SERC	SPP RE	Texas RE	WECC	Total
January	10	27	7	23	30	11	15	49	172
February	1	0	30	34	18	24	21	54	182
March	4	7	16	35	33	5	9	31	140
April	3	32	7	25	18	11	33	25	154
May	4	11	7	42	41	0	26	35	166
June	2	7	16	30	27	0	32	40	154
July	5	22	20	39	22	0	19	67	194
August	0	5	8	35	52	0	12	57	169
September	1	1	15	11	7	0	11	36	76
Total	30	112	126	274	248	51	178	394	1407

Top 10 Most Violated Standards in ERO in 2017

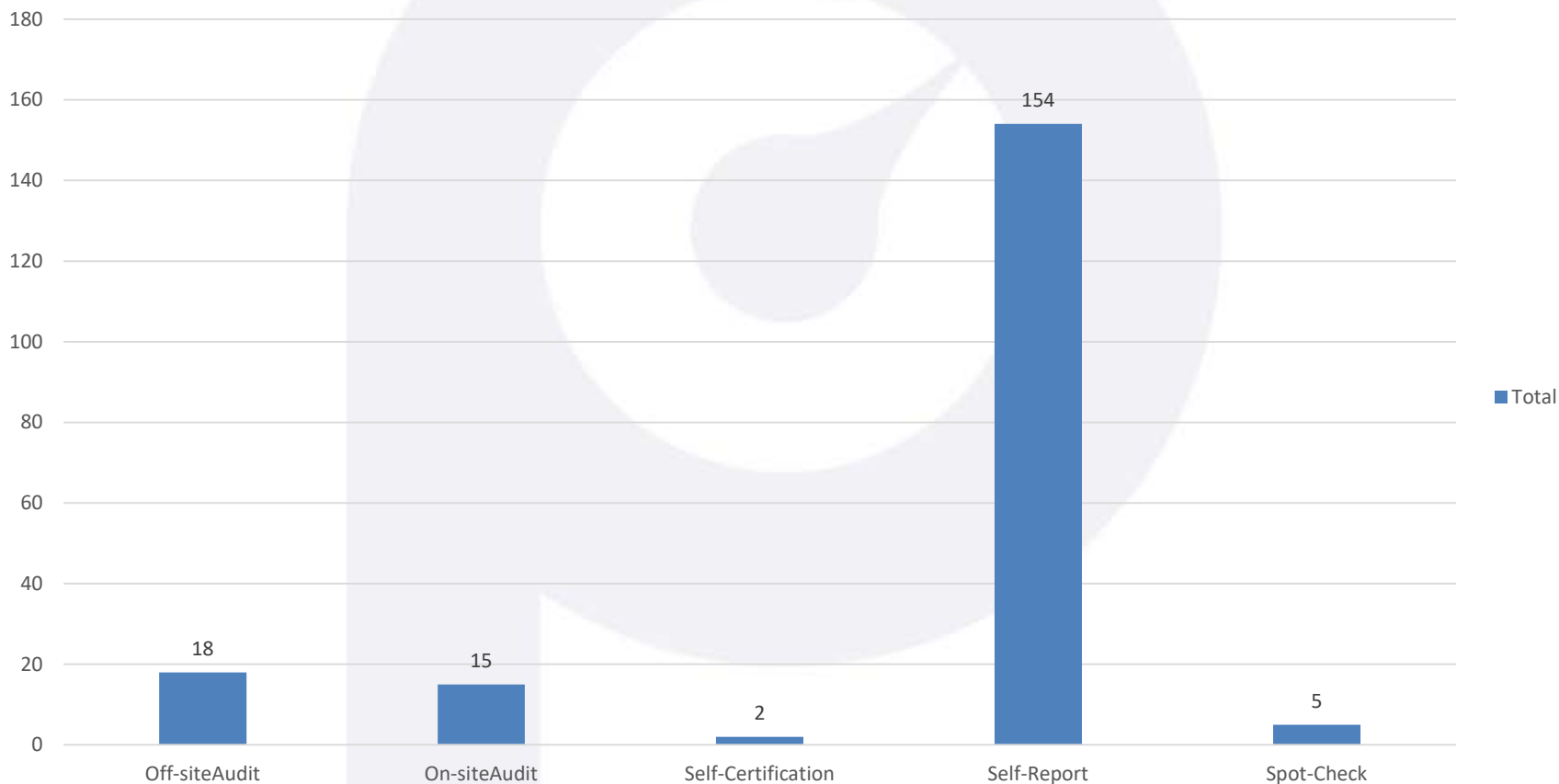


2018 Most Violated Standard By Requirement in NPCC (10/29/18)

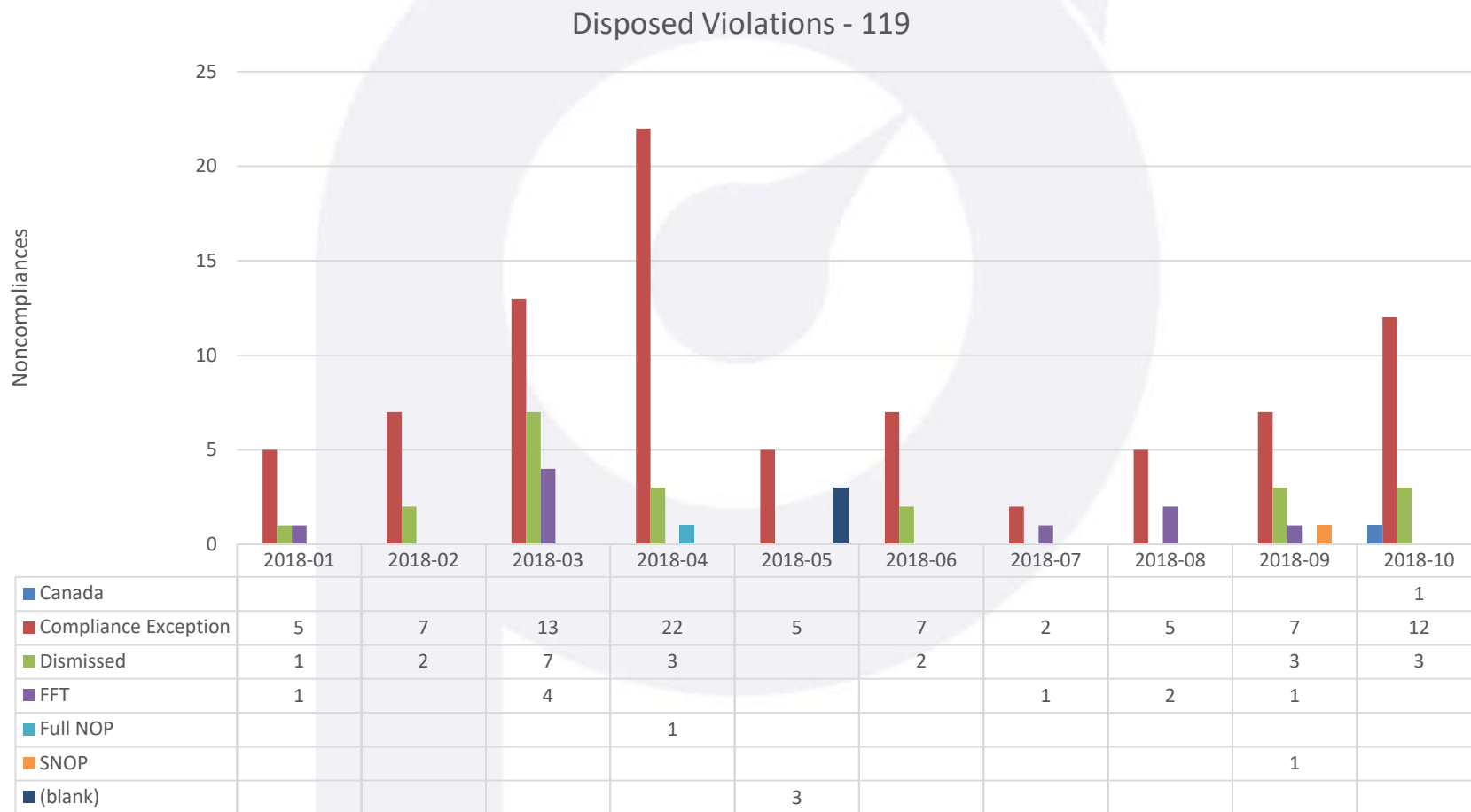


2018 Non Compliances by Discovery Method in NPCC

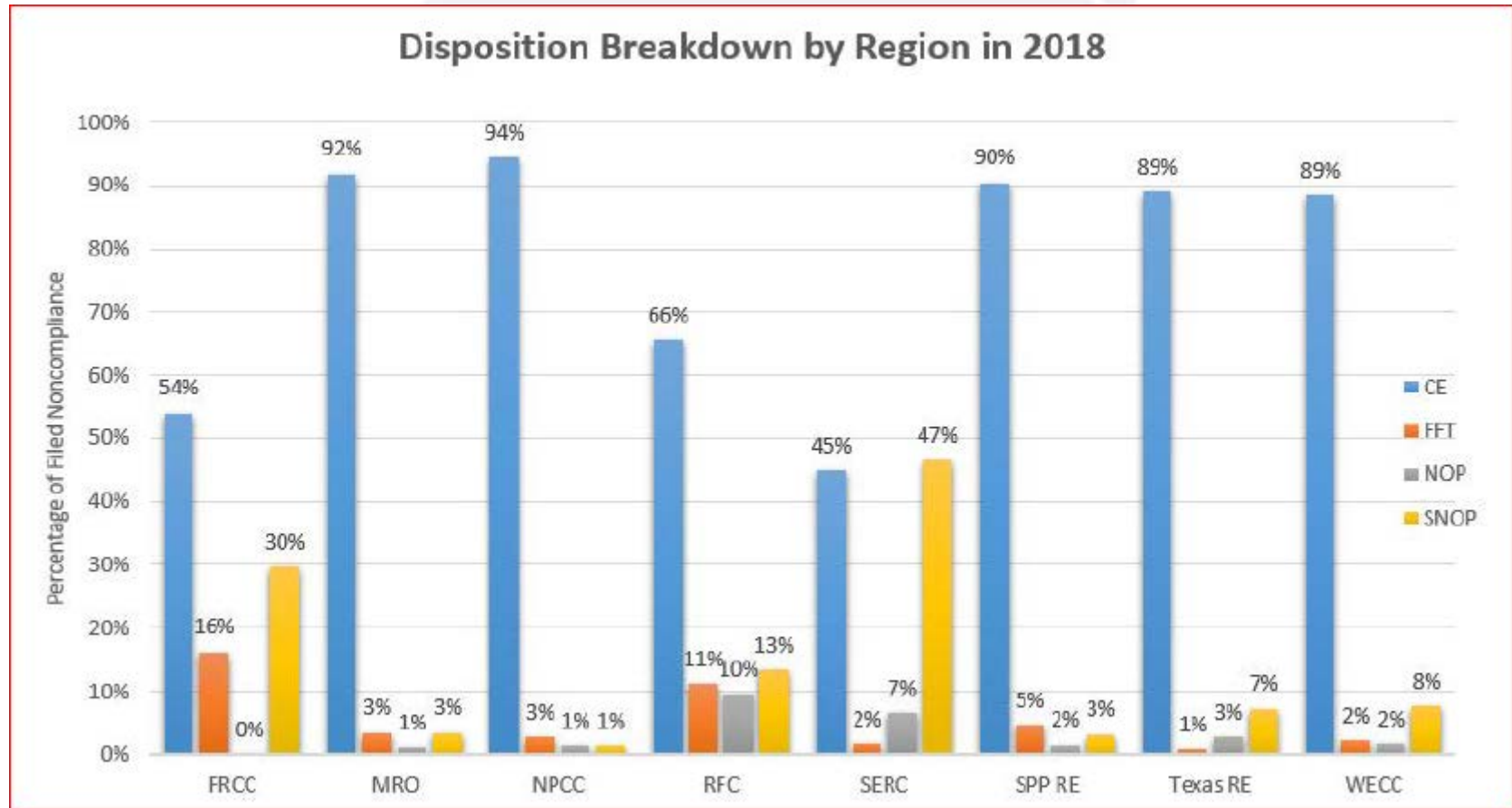
Total Noncompliances by Discovery Method



2018 Disposals



2018 Disposition by Region



Leading O&P Non-Compliance Factors

- Implementation Plan dates
- Incorrect Assumptions
 - Facility, Component, Entity, NYISO D9 and D10 program
- Lack of Awareness/Obligation/Understanding
 - MOD-025 Real/Reactive
 - PRC-024 Freq and Voltage Operational Curves
 - PRC-019 Voltage Regulating System Control Verification
- Lack of proper controls

MOD-025

- Use the NERC form...or provide the same data as on the NERC form.
- For NERC Compliance, your ISO cannot dictate to you to use their form. If you provide them the data fields on the NERC form in some fashion, you are compliant.
- ISO Market Rules are a different story

PRC-024 Misconceptions

- Facility – What is a Facility in this Standard?
 - 2 curves: Freq and Voltage
 - UF is trumped by PRC-006-NPCC-01
 - Voltage Protection Systems and POI
- Forgot about including V/Hz in the review
- Solar Invertors – WECC Events
 - Current from invertors to grid cannot stop while within either curve.
 - “Trip” is not a defined term

PRC-019 Voltage Regulating Control Verification

- Need some sort of analysis
- Show your lines on the D Curve
- Need documentation that it was verified before the due date. Still a PNC if no changes are needed without proper documentation.

New and Old: Industry Focus

- 7/1/18, R2: MOD-026-1 and MOD-027-1
 - Verification of Gen Excitation Control System
 - Verification of Turbine/Governor and Load Control
 - Implementation Plan: 30% of NCR applicable gross MVA by Interconnection completed and the data supplied to TP
- FAC-003-4
 - 2003 Blackout, not looked upon lightly, keep up your guard
- FAC-008-3
 - Issues uncovered in ERO
 - Field verification visits will start during TO, GO audits
 - Will check for most limiting series element that makes up the Facility Rating

In Depth Understanding and Proper Mitigation

- Identify the full scope/extent of the Non Compliance issue 5W/1H
- Identify the Root Cause of the issue
- Evaluate/Harden internal controls
 - Determine: Which controls worked? Which didn't?
 - Preventative, Detective, Corrective
 - Determine effectiveness of mitigation activities over time
- Feedback and Communication

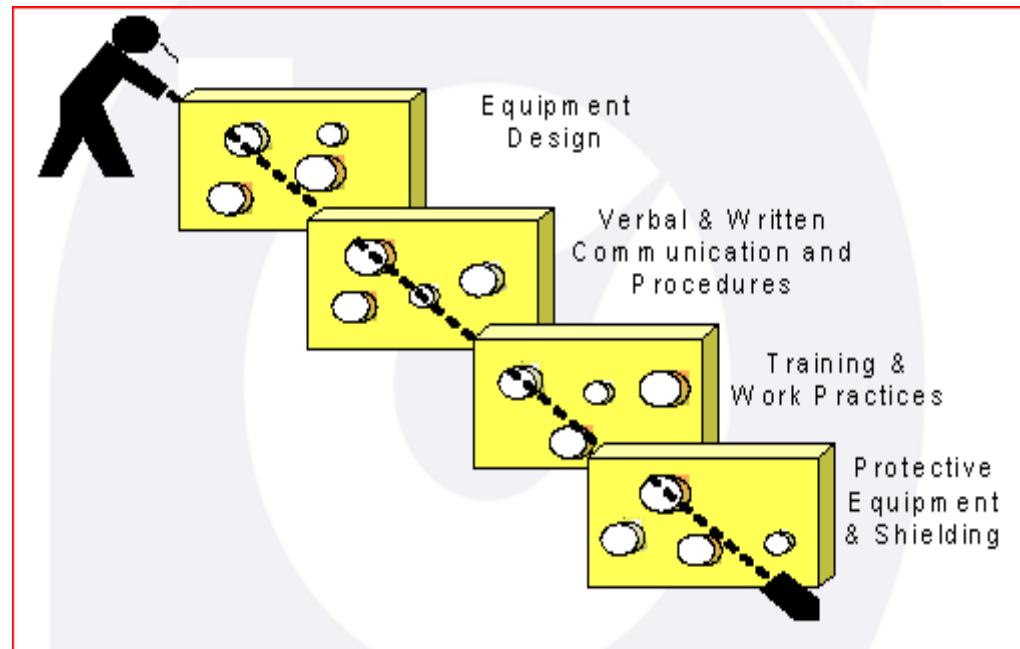
Humans and Root Cause

- Dig deeper than just assigning “Human Error”
- Majority of issue is due to lack of preventative controls
- Humans will make mistakes
- Change/adjust the conditions that humans work
- Majority issues: Management failures and/or failures in the program/process to foresee the forthcoming error

Determine:

- Which controls worked? Which didn't?

Opportunities to Defend



- Line Sag into tree
- State Estimator not working
- Operator Situational Awareness Lacking
- Lack of Communication to Neighbor System