NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda
Board of Trustees Compliance Committee

February 11, 2015 | 11:15 a.m. – 12:15 p.m. Pacific

The Westin San Diego
400 W Broadway
San Diego, CA 92101

Call to Order

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines—Public Announcement

Agenda

1. **Minutes* — Approve**
   a. November 12, 2014 Meeting
2. **Compliance Committee Self-Assessment Results* — Review**
3. **Risk-Based Compliance Monitoring and Enforcement Implementation* — Update**
4. **Key Compliance Enforcement Metrics and Trends* — Review**
5. **Compliance Exception and Self-Logging Report* — Review**
6. **Adjournment**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.
- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition.

Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Draft Minutes
Board of Trustees Compliance Committee

Agenda Item 1.a

November 12, 2014 | 9:45 a.m. Eastern

The Westin Buckhead Atlanta
3391 Peachtree Road NE
Atlanta, GA 30326

Bruce A. Scherr, Chair, called to order the duly noticed open meeting of the Board of Trustees Compliance Committee (the Committee) of the North American Electric Reliability Corporation on November 12, 2014 at approximately 9:45 a.m. Eastern, and a quorum was declared present. The agenda is attached as **Exhibit A**.

Present at the meeting were:

Committee Members:	**Board of Trustees Members:**
Bruce A. Scherr, Chair	Gerry W. Cauley, President and Chief Executive Officer
Janice B. Case	Paul F. Barber
Frederick W. Gorbet	Robert G. Clarke
David Goulding	Douglas Jaeger
Jan Schori	Kenneth G. Peterson
Roy Thilly	

NERC Staff:
Charles A. Berardesco, Senior Vice President, General Counsel, and Corporate Secretary
Sonia Mendonça, Associate General Counsel and Senior Director of Enforcement
Steven Noess, Director, Compliance Assurance

Regional Entity Staff:
Curtis Crews, Director, Compliance Assessments, Texas RE
Stacy Dochoda, FRCC President and Chief Executive Officer
Sara Patrick, Vice President, Enforcement and Regulatory Affairs, MRO
Marisa Sifontes, SERC General Counsel

Registered Entity Representatives
Greg Froehling, NERC Compliance Officer, Rayburn Country Electric Cooperative
Randy Crissman, Vice President – Technical Compliance Operations, New York Power Authority
Annette Johnston, Director NERC/CIPS Compliance, MidAmerican Energy Company

A listing of industry attendees is attached as **Exhibit B**.

NERC Antitrust Compliance Guidelines
Mr. Scherr directed the participants' attention to the NERC Antitrust Compliance Guidelines.

Minutes
Upon motion duly made and seconded, the August 13, 2014 meeting minutes were approved as presented at the meeting.

Reliability Assurance Initiative (RAI)
A panel of NERC and Regional Entity staff and registered entity representatives provided an update regarding the transition from design to implementation of the risk-based approach to compliance monitoring and enforcement. The presentation reviewed a variety of subjects, including the staff-training plan, the latest developments on outreach and communication, and NERC oversight during implementation.

In addition, the presentation also addressed new efforts aimed at enhancing the coordination by Regional Entities in the oversight of Multi-Region Registered Entities, and the Regional Consistency Reporting Tool aimed at collecting data on situations where lack of consistent processes within the ERO Enterprise may exist. The Tool is available through links on the websites of NERC and the Regional Entities.

A smaller registered entity, Rayburn Country Electric Cooperative, which was recently audited by the Texas Regional Entity, described its experience with the Inherent Risk Assessment and Internal Controls Evaluation.

Two other registered entities, MidAmerican Energy Company and New York Power Authority, presented on their respective experiences with the self-logging and compliance exception processes.

Key Compliance and Enforcement Metrics and Trends
Ms. Mendonça referred the Committee to the Key Compliance Enforcement Metrics and Trends material included with the agenda package.

There being no further business, and upon motion duly made and seconded, the meeting was adjourned at approximately 12:00 p.m. Eastern.

Submitted by,

Charles A. Berardesco
Corporate Secretary

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 2

Summary of 2014 Board of Trustees Compliance Committee Survey

RELIABILITY | ACCOUNTABILITY




Overview

- NERC engaged TalentQuest to conduct its annual Board of Trustees Compliance Committee survey through an online methodology
- The Compliance Committee survey was administered from November 12 to December 19, 2014, to a total of 6 Committee members
- 6 Committee members responded to the survey
  - 100% response rate

Rating Scale

- Respondents were asked to rate items on a 1 to 3 point scale to indicate their evaluation for each rated item
  - 1= Below Expectations ("performance area with opportunity for improvement")
  - 2= Meets Expectations ("meets required standard of performance")
  - 3 = Above Expectations ("exceeds the required standard of performance")
- For any item rated "1" (Below Expectations) or "No", mandatory comments were required to explain the rationale for the rating or selection

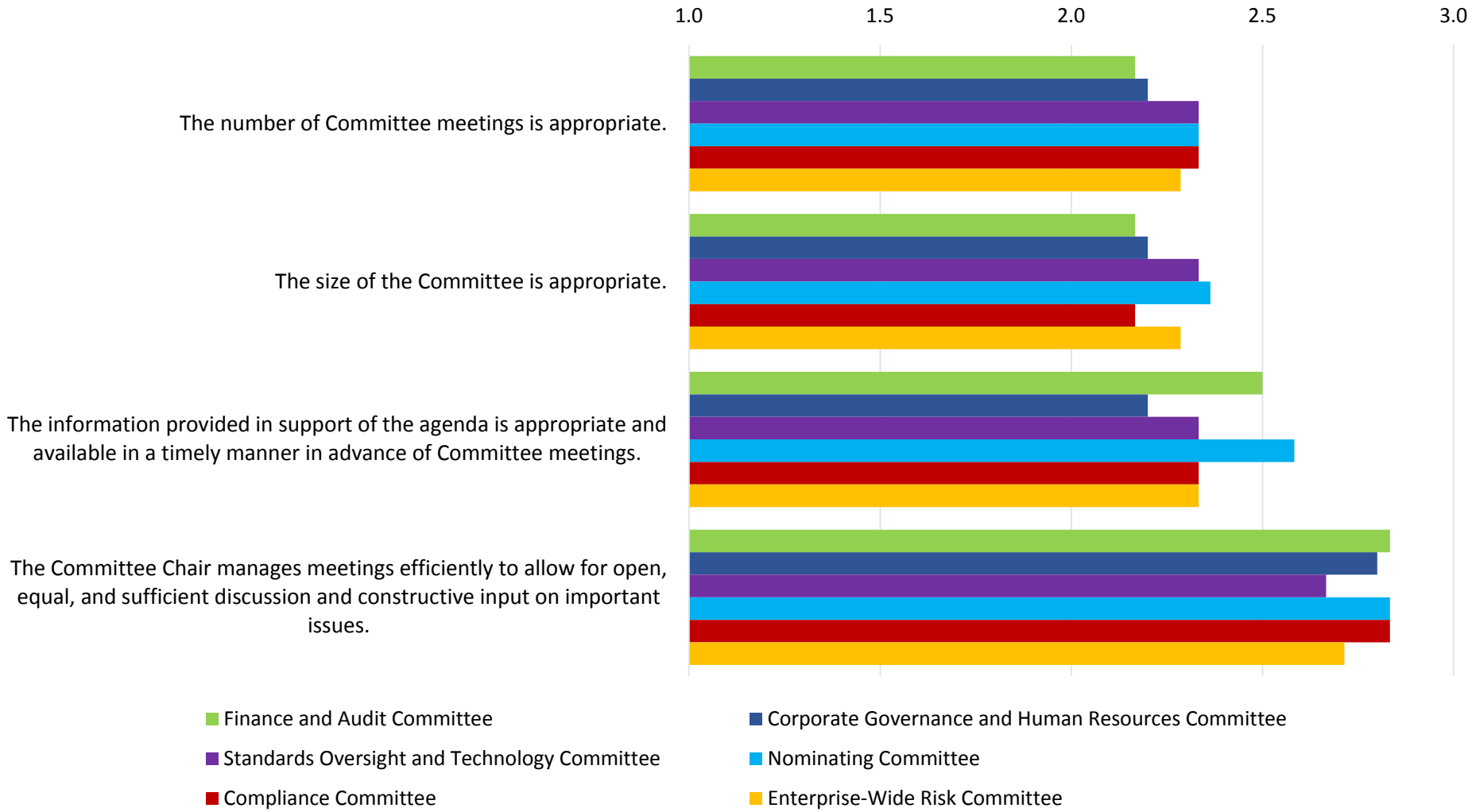
Results Summary

- The overall Compliance Committee survey average was 2.22, with item averages ranging from 2.00 to 2.83
- Given the lowest item averages are 2.00, the Compliance Committee is seen to be operating at expectations or higher
- Highest Rated Item (2.83):
  - The Committee Chair manages meetings efficiently to allow for open, equal, and sufficient discussion and constructive input on important issues.

Results Summary

- Review of cross-committee survey items finds the Compliance Committee rated the lowest on the following item:
  - The size of the Committee is appropriate. (2.17)
- Of the cross-committee survey items, the Compliance Committee rated the highest on the following items:
  - The Committee Chair manages meetings efficiently to allow for open, equal, and sufficient discussion and constructive input on important issues. (2.83)
  - The number of Committee meetings is appropriate. (2.33)

Committee Comparison



Agenda Item 3
Board of Trustees Compliance Committee
Open Session
February 11, 2015

Risk-based Compliance Monitoring and Enforcement Update

Action

Information

Completion of the Reliability Assurance Initiative and Communications Update

In 2014, through the Reliability Assurance Initiative (RAI), NERC completed the design of the various components of the risk-based Compliance Monitoring and Enforcement Program (CMEP).

In 2015, the ERO Enterprise will focus on the successful implementation of the risk-based CMEP. Consequently, in its communications, NERC will reference the risk-based CMEP rather than the initiative or "RAI." NERC is working to duplicate the information accumulated in the RAI page in the Compliance and Enforcement pages, which will also be redesigned to be more usable. The RAI page will remain in place during 2015, with all of its current content, to ensure that the information remains available to all interested parties while the Compliance and Enforcement pages are reorganized. NERC also will continue to highlight new information available regarding the risk-based CMEP in its weekly bulletins and monthly newsletter.

Ongoing Activities

The ERO Enterprise has begun implementation of all aspects of the risk-based CMEP. Oversight related to the design documents is underway, and NERC and Regional Entity management remain in close coordination to ensure successful implementation. As 2015 progresses, NERC will present the results of such implementation. In particular, NERC will regularly address the following topics:

- Continued training of the ERO Enterprise staff;
- Continued outreach efforts during 2015 (including industry-focused workshops, a small entity tabletop exercise for ERO Enterprise staff, tutorials on the use of compliance and enforcement information available online, and efforts to support and encourage information sharing among registered entities);
- Oversight of Regional Entity implementation of various risk-based processes; and
- Development and benchmarking of objective metrics to support the measures of success for the risk-based CMEP identified in November 2014.

Continued Training of the ERO Enterprise Staff

During 2015, NERC Compliance Assurance and Compliance Enforcement departments, supported by Regional Entities, will continue to develop and provide comprehensive and ongoing education and training on the transformation of compliance monitoring and enforcement for ERO

Enterprise staff. In particular, the training will focus heavily on continuing education for implementing the Inherent Risk Assessment (IRA) and Internal Control Evaluation (ICE) components of the risk-based CMEP to support successful implementation and consistency. The training plan has several goals:

- Develop training objectives for risk-based CMEP implementation and identify steps to rollout training, both short-term and long-term;
- Identify roles, responsibilities, and skillsets for regional staff under the risk-based CMEP and corresponding training needs;
- Identify training and communication needs for other target audiences such as Compliance/Enforcement Managers, Auditors, registered entities, FERC staff, and NERC staff;
- Identify and allocate resources to support the training plan; and
- Develop and conduct continued training on IRA, ICE, self-logging, and compliance exceptions.

Training Approach Overview

NERC and the Regions are working collaboratively to provide detail and input into necessary training materials (e.g., identifying who needs to be trained, what topics the training should include, and what detail the training needs to cover). In order to ensure consistency in training and approach, a core group of NERC-led presenters and trainers are overseeing the implementation of the training plan.

Specific training is being provided for both the design of the risk-based CMEP and specific components, and it is tailored in each instance to the targeted audience:

- As applicable, tailored to the "performance" role for each component (e.g., those who will actually conduct the IRA or ICE);
- Tailored to compliance monitoring and compliance enforcement staff in general for context of what is being done collectively as part of the risk-based CMEP (i.e., even if a particular regional entity staff member is not conducting the IRA or ICE, it is important for that individual to understand the risk-based approach that informs a registered entity's compliance oversight plan); and
- Possible outreach and training that may be "stakeholder" focused, which may be developed based upon input from a stakeholder-focused advisory group.

The training is being implemented in two phases, the first of which began in Q4 2014. Phase I involves a shorter-term approach to address IRA and ICE content focusing first on those regional staff that perform actual IRAs and ICEs. Phase I also includes foundational concepts using real-life scenarios and examples.

Phase II will provide further depth and will incorporate lessons learned and other examples obtained throughout actual application of IRA and ICE.

As implementation progresses, NERC will assess which other components and topics need more or less training to support development of consistency among the ERO Enterprise and will adapt and modify training material to address this input on an ongoing basis.

In addition, beginning in the first quarter of 2015, NERC and the Regional Entities will engage in one or more tabletop exercises focused on assessing internal controls for small registered entities (i.e., entities serving a load of between 75 MW and 300 MW). These exercises will assist ERO Enterprise staff in scaling application of ICE by obtaining a better understanding of how small entities identify internal controls. During these exercises, representatives from approximately five small entities will present their approach to internal controls for specific Reliability Standards and engage in discussions with regional staff to support application of ICE to small entities.

The table below illustrates the timing of the training milestones:

Table 1: Regional Entity Training

Date	Training Activity
Q4 2014	(Complete) Initial training for Phase I of Training Program. Training focus is on ERO Enterprise staff performing IRA and ICE.
Q1 2015	Conduct final training related to Phase I Training Program for ERO Enterprise staff not responsible for performing IRA and ICE.
Q1	Develop Phase I Training Report that identified observations, opportunities, and future training and education needs.
Q1	Identify competencies and skill areas for training and education activities.
Q1	Small entity tabletop exercise for ERO Enterprise staff
Q1-Q2	Phase II begins: Develop and communicate education schedule and delivery methods for identified competencies and skill areas for training and education activities. Primary delivery method will be monthly webinars for ERO Enterprise staff and in-person, instructor-led training.
Q2	Conduct in-person training on IRA and ICE, focusing on specific examples and lessons learned. Deliver training and education at Spring 2015 ERO Compliance Monitoring Workshop.
Q2-Q4	Develop and deliver Phase II training based on identified competencies and skill areas.
Q3	Deliver training and education at Fall 2015 ERO Compliance Monitoring Workshop.
Q4	Assess and evaluate future training, education, and guidance needs and provide input into the year-end report assessing consistency of IRA and ICE implementation.

Continued Outreach Efforts in 2015

Currently scheduled events for Q1 2015 include industry focused outreach events and webinars on the ERO Enterprise's approaches to risk-based CMEP activities. On March 5, 2015, a panel of participants from NERC, Regional Entities, and stakeholder companies will discuss the components of the transformed, risk-based CMEP, which includes the application of risk-based CMEP concepts to CIP Version 5. Agenda topics and discussions will incorporate feedback obtained from prior industry outreach events as well as any lessons learned during the ERO Enterprise's initial implementation and rollout. This outreach event will be held in-person in Atlanta, Georgia, and will also be available through a streaming webinar.

Additional outreach efforts will include, at minimum, quarterly webinars on lessons learned, process updates, and guidance for compliance monitoring and enforcement activities, combined with a second industry focused event in Q4 2015. Further, ERO Enterprise staff will conduct a webinar series providing guidance on Standards and Requirements associated with the 2015 Risk Elements identified for consideration for compliance monitoring.

Throughout 2015, ERO Enterprise staff will continue holding advisory group meetings to identify additional outreach and education needs as well as provide an opportunity for industry input into the rollout of the ERO Enterprise' implementation of risk-based approaches to the CMEP.

The table below illustrates selected outreach and training events for 2015. Additional events will be added as necessary.

Table 2: Outreach and Training Events

Date	Meeting	Place
Q1-Q4 2015	Industry: Webinar outreach series on Standards & Requirements associated with Risk Elements identified for compliance monitoring consideration	Webinar
January 27, 2015	Industry: Closed Advisory Group Meeting	Washington, DC
March 5, 2015	Industry: Risk-Based Compliance Monitoring and Enforcement Event	Atlanta, GA (webinar participation available)
April 1-3, 2015	Industry: Spring Standards and Compliance Workshop	Atlanta, GA
July 2015	Industry: Risk-based Compliance Monitoring and Enforcement Webinar	Webinar
October 2015	Industry: Spring Standards and Compliance Workshop	TBA
October 2015	Industry: Risk-Based Compliance Monitoring and Enforcement Event	Atlanta, GA (webinar participation available)

Oversight Approach Overview

For 2015, ensuring the successful implementation of NERC's risk-based CMEP is the priority of NERC's Compliance Assurance and Compliance Enforcement departments' oversight plans. As part of that oversight, and in support of the 2015 Enterprise and Corporate Metrics approved at the November 2014 quarterly meetings, NERC will, in addition to regular feedback to the Regional Entities, provide a report by the end of 2015 assessing consistency of Regional Entity compliance monitoring (inclusive of IRA and ICE performance) and identifying areas for improvement or promoting consistency through training, guidance, or adjustment the following year. NERC also produces an annual ERO CMEP report, which for 2015 will include assessment of risk-based CMEP implementation. That report will be published during the first quarter of 2016.

The oversight approach to risk-based CMEP implementation includes the following concepts:

- Reviewing processes and procedure documentation to assess consistency with risk-based CMEP design
- Sampling the activities related to performance of specific components of the risk-based CMEP design
- Providing feedback and recommendations on assessments to Regional Entities for improvement and training

Table 3: Oversight Schedule

Date	Oversight Activity
Q1-Q2	Phase I of Compliance Assurance Oversight (described below)
Q3 and beyond	Phase II of Compliance Assurance Oversight (described below)
Q1 and beyond	Qualitative review of enforcement processes
Each quarter	Collection of data and reporting of utilization rates of enforcement processes
Q4	Publish report assessing consistency of Regional Entity compliance monitoring
Q1 2016	Publish 2015 annual ERO risk-based CMEP report

Compliance Assurance Oversight

For Compliance Assurance, oversight activities are being conducted through a two-phased approach, and each phase's reviews include activities related to Multi-Regional Registered Entities (MRRE) to support evaluation of MRRE implementation across the ERO Enterprise.

The phases of Compliance Assurance oversight include the following:

- Phase I
  - Q1-Q2 of 2015
  - Process and procedure documentation reviews of each region to establish conceptual consistency and to identify and resolve any nonconformance to the risk-based CMEP's design
  - Feedback to the Regional Entity with recommendations
- Phase II
  - Q3 2015 and beyond
  - Evaluation of how risk-based compliance monitoring concepts are used (including determinations and application)
  - Focus on samples of compliance monitoring work
  - Review of on performance of the compliance monitoring work
  - Feedback to the Regional Entity with recommendations

Phase one began during the first quarter of 2015 and will continue into the second quarter. It is designed to establish conceptual consistency in the application of the ERO Enterprise's risk-based approach through review of each Region's risk-based process documentation to interpret and understand their conceptual intent of application and compare these concepts to the ERO Enterprise's guidance documents. This will involve dialogue and the collection and review of supporting regional process documents such as policies, procedures, narratives, and flowcharts describing the Regional Entity's execution and application of the design for the ERO Enterprise's risk-based CMEP.

As part of phase one, NERC will provide to each Regional Entity an oversight report summarizing the results of its review to identify, if any, differences or opportunities for increased consistency in regional processes versus the risk-based CMEP design. The reports will also recommend actions the Regional Entity should implement to address such feedback, if any. The reports will include best practices and improvement opportunities that can be utilized to both enhance an individual Region's IRA and ICE activities and develop training for the ERO Enterprise as a whole.

In phase two, NERC's oversight will begin to evaluate how risk-based compliance monitoring concepts are utilized, the determinations made when using these concepts, and the results of their practical application by the Regional Entities. Phase two will focus on samples of compliance monitoring work by each Regional Entity while using their risk-based concepts.

Compliance Enforcement Oversight

For Compliance Enforcement, NERC oversight of the Regional Entities' enforcement programs is performed primarily through the review of the processes, supporting evidence, and other information provided by the Regional Entities over the course of focused engagements of program areas that are appropriately scheduled throughout the year. NERC communicates the recommendations and findings to the Regional Entities to help the ERO Enterprise develop responsive strategies and solutions to potential issues and ensure uniform and consistent

implementation of the CMEP. Such recommendations and findings also help identify priority areas for training of ERO Enterprise staff during the year.

NERC Enforcement's oversight includes three main categories of activities: (a) those associated with data flow and calculation of metrics, (b) the annual spot check program, and (c) the development of feedback, guidance, and training.

- First, NERC Enforcement analyzes enforcement data to assist with monitoring of CMEP processes and to help identify trends that may affect BPS reliability. Performance indices are also computed on a regular basis to quantify the performance of the Regional Entities and NERC in processing violations and mitigation and to provide insight in determining the effectiveness of Regional Entity programs and adequacy of Regional Entity and NERC resources.

- Second, NERC spot-checks specific enforcement-related process throughout the year. As a result of such spot checks, NERC Enforcement provides feedback to the Regional Entities on areas and activities to enhance consistency and effectiveness of processes. In 2015, spot checks will focus on the new processes under the risk-based CMEP.

- Finally, NERC Enforcement provides feedback, guidance, and training to the Regional Entities. For example, NERC Enforcement provides individual feedback on areas such as opportunities to enhance consistency and effectiveness of processes. As explained above, in 2015, NERC Enforcement will provide additional training to Regional Entity staff and the industry on areas such as compliance exceptions and the self-logging program. NERC will develop this training based on early experience with implementing the programs, as well as observations from the various spot-checks.

Development and Benchmarking of Objective Metrics to Support the Measures of Success for the Risk-based CMEP Identified in November 2014

These are the preliminary objective metrics being discussed to assess the success of the implementation of the risk-based CMEP.[1] NERC is also working with the NERC Compliance and Certification Committee (CCC) to develop criteria by which it would to determine the effectiveness of each Regional Entity Compliance Monitoring and Enforcement Program. The criteria are being developed to further support the measurement of each of these success factors.

Over the course of the year, NERC will collect information related to each measurement in order to determine the appropriate benchmarks and possible targets for future years. Each metric may support more than one success factor. None of the metrics are intended to replace the qualitative evaluation that will be performed through the oversigh processes referenced above.

[1] This is also in support of the 2015 Enterprise and Corporate Metrics which specify development of such metrics for the risk-based CMEP measures of success identified at the November 2014 quarterly meetings.

Table 4: Risk-based CMEP Objective Metrics			
	Success Factor	**Activities in Support**	**Measurement**
1	ERO Enterprise Staff Competency (competency and perception): ERO Enterprise staff performing key activities are trained and competent in their areas of responsibility, such as risk assessment, audit, internal controls evaluation, and enforcement, and are regarded by registered entities as being well-qualified in their roles.	• 2015: Internal training of staff (risk, compliance and enforcement) including in person and remote opportunities • ERO Enterprise effectiveness survey • 2016: development of evaluation process for staff based on results of 2015 training and oversight activities	• Percent by identified role of ERO Enterprise staff who received training in identified competency areas for risk-based compliance and enforcement activities • Output from audit engagement exit surveys • Benchmarking of results of effectiveness survey for future comparison
2	Information and Outreach: Registered entities have the information they need—through outreach, program transparency, and sharing of best practices—to prepare for engaging with the Regional Entities and NERC in the risk-based compliance and enforcement activities.	• NERC and Regional Entity webinars, workshops, etc. (feedback from recent events suggests joint efforts are beneficial) • NERC and Regional Entity support of CCC/NATF/NAGF/Trades events, including by encouraging/mediating industry panels for sharing of best practices • Revamping of Compliance and Enforcement pages on NERC.com • Continued utilization of weekly bulletin and monthly newsletter to disseminate information and availability of resources/webinar on availability of resources and how to find/use publicly	• Frequency of events by delivery method • Benchmarking of results of effectiveness survey for future comparison

Table 4: Risk-based CMEP Objective Metrics			
	Success Factor	**Activities in Support**	**Measurement**
		available information posted by compliance and enforcement	

3	Consistency: The common tools, processes, and templates used by Regional Entities for risk-based compliance and enforcement activities with registered entities are consistent on matters where consistency is important, and NERC has adequate oversight of that interface.	• Continued coordination within ERO Enterprise
		• Continued development and implementation of oversight program
		  • Execution of Compliance Assurance and Enforcement oversight plans
		  o Assessment of consistency with risk-based CMEP design
		  o Sampling of activities
		  o Feedback to Regional Entities
			• Rates of utilization of various monitoring and enforcement methods [See example below for compliance exceptions and self-logging utilization rates]
			• Timing of various compliance monitoring and enforcement activities
			• Output and qualitative evaluation from consistency reporting tool
			• Output from audit engagement exit surveys
			• 2015 report on implementation of ICE and IRA
			• Benchmarking of results of effectiveness survey for future comparison

4	Regulator Trust: The ERO Enterprise has strengthened the trust of FERC and applicable Canadian government authorities in risk-based	• Continued coordination and collaboration with FERC and Canadian authorities at various levels	• Feedback from North American regulators on informational filing

Table 4: Risk-based CMEP Objective Metrics			
	Success Factor	**Activities in Support**	**Measurement**
	compliance and enforcement.		
5	Balanced Transparency: An appropriate level of transparency has been determined for various facets of risk-based compliance and enforcement, balancing efficiency and the confidentiality needs of a registered entity with the needs of industry as a whole to learn from others (e.g., transparency of compliance exceptions and aggregation logs, as well as feedback to each entity regarding inherent risk or internal controls evaluation).		• Annual and quarterly reports on compliance exceptions and self-logging [For example, see the report for fourth quarter posted as part of this agenda package] • 2015 report on implementation of ICE and IRA • Summary information to registered entity on IRA/ICE results • Benchmarking of results of effectiveness survey for future comparison
6	Metrics Identified: Metrics are identified for key expected results from risk-based compliance and enforcement and benchmarked for 2015.	• Review and evaluation of existing enforcement and compliance metrics (including compliance metrics already in use at the Regional Entity level)	• Rates of utilization of various monitoring and enforcement methods • Timing of various compliance monitoring and enforcement activities
7	Recognized Value: The value of risk-based compliance and enforcement of registered entities is of demonstrable value to the consuming public	• Continued analytical work and dissemination of results (example: analysis of violation information by risk level)	• Correlation of ERO performance metrics regarding reliability results, assurance effectiveness, and risk mitigation effectiveness

Table 4: Risk-based CMEP Objective Metrics			
	Success Factor	**Activities in Support**	**Measurement**
	and can be clearly and publicly articulated.		• Benchmarking of results of effectiveness survey for future comparison

To illustrate some of the above metrics, please see below (these graphs are fully discussed and explained in the Compliance Exception and Self-Logging report included in this package).

This graphs shows the rate of utilization of compliance exceptions (shown in yellow) by the various Regional Entities during the limited application of the program in 2014. In 2015, use of the compliance exception disposition track will be more even and, for the most part, replace the use of FFT for disposition of issues posing a minimal risk to the reliability of the BPS.

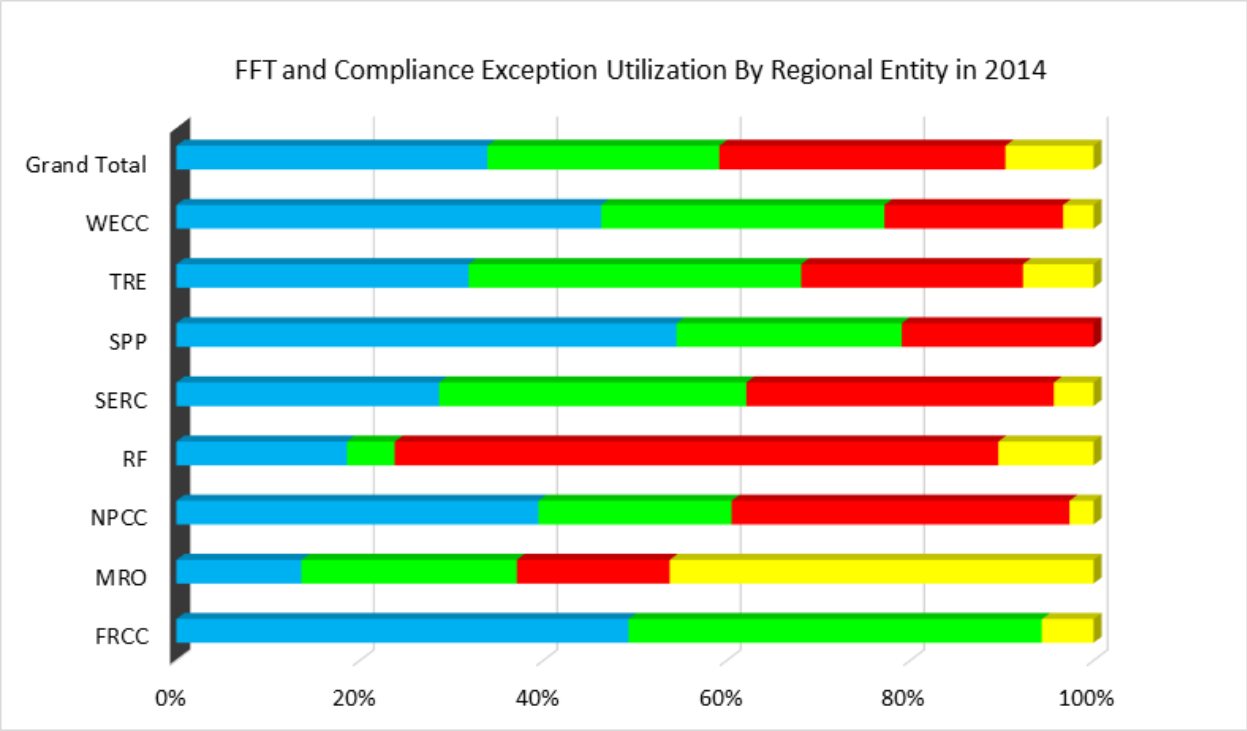


Figure 1: FFT and Compliance Exception Utilization

This graph shows the use of the self-logging program by Regional Entity during the limited application of the program in 2014. The program is open to any registered entity that qualifies based on the requirements of the program. See http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Self-logging%20of%20Minimal%20Risk%20Issues%20Program%20Overview.pdf.

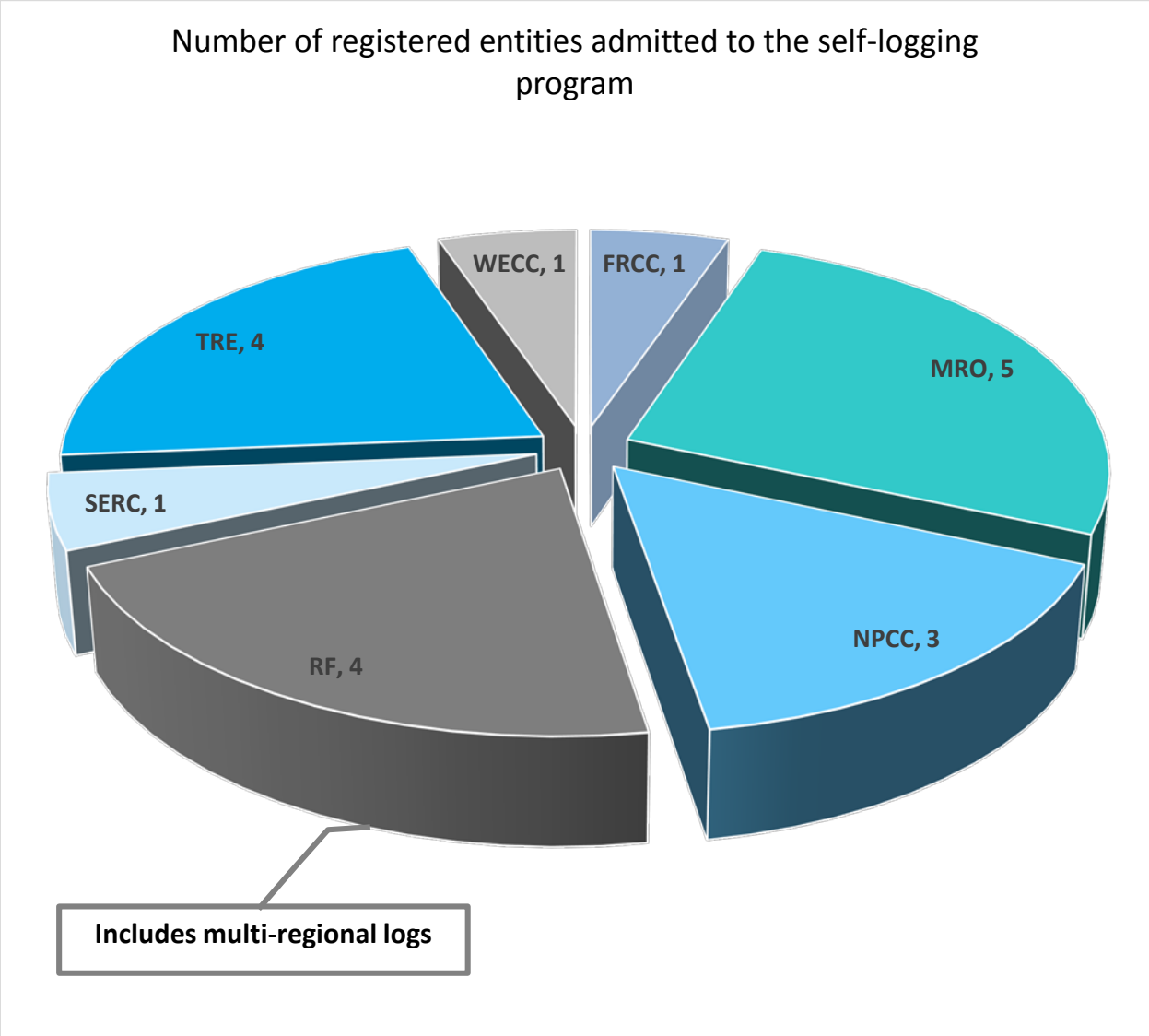


Figure 2: Registered Entities and Self-Logging

Agenda Item 4
Board of Trustees Compliance Committee
Open Session
February 11, 2015

Key Compliance Enforcement Metrics and Trends

Action
Information

Introduction
On a quarterly basis, NERC provides the Board of Trustees Compliance Committee an update on key compliance enforcement metrics and trends. This report focuses on the ERO Enterprise's performance on the Enforcement goals and metrics in 2014. The report also covers other relevant trends pertaining to enforcement activities.

ERO Enterprise 2014 Goals—Compliance Enforcement
In 2014, the ERO Enterprise adopted the following compliance enforcement goals:

- Timeliness and transparency of compliance results (measured through the caseload index and reduction of the caseload discovered prior to January 1, 2013);
- Promotion of self-identification of noncompliance (measured as a percentage of noncompliance discovered in 2014);
- Timeliness of mitigation (measured as percentage of matters with completed mitigation per year of discovery); and
- RAI enforcement reforms (measured as the average time for noncompliance discovered in 2014 to go through triage).

The sections below show the performance of the ERO Enterprise in 2014 and provide additional information.

Timeliness and Transparency of Compliance Results

ERO Enterprise and Regional Caseload Indices[1]
The ERO Enterprise caseload index is the sum of the average Regional Entity and NERC caseload indices. The average Regional Entity caseload index for the end of 2014 was 6.3 months and the NERC caseload index was 0.8 months.

The ERO Enterprise caseload index began and ended the year at approximately 7.2 months. The 2014 target for this metric was 7 months and the threshold was 8 months.

[1] The caseload index is a predictive metric forecasting the time it would take to eliminate the noncompliance inventory based on the processing rate of the past 12 months. It is calculated based on the inventory of active noncompliance being processed (excluding any noncompliance being held as a result of an appeal, a regulator, or a court) and dividing it by the processing rate over the past 12 months.

The incoming noncompliance during 2014 increased the inventory, requiring review and processing during 2014, which resulted in the rise of the caseload index in Q2 and Q3. NERC and the Regional Entities' efforts associated with the processing of noncompliance resulted in a decrease in the caseload index in Q4. These efforts included close monitoring of enforcement processing metrics, project planning, and use of streamlined disposition mechanisms, including compliance exceptions and FFTs.

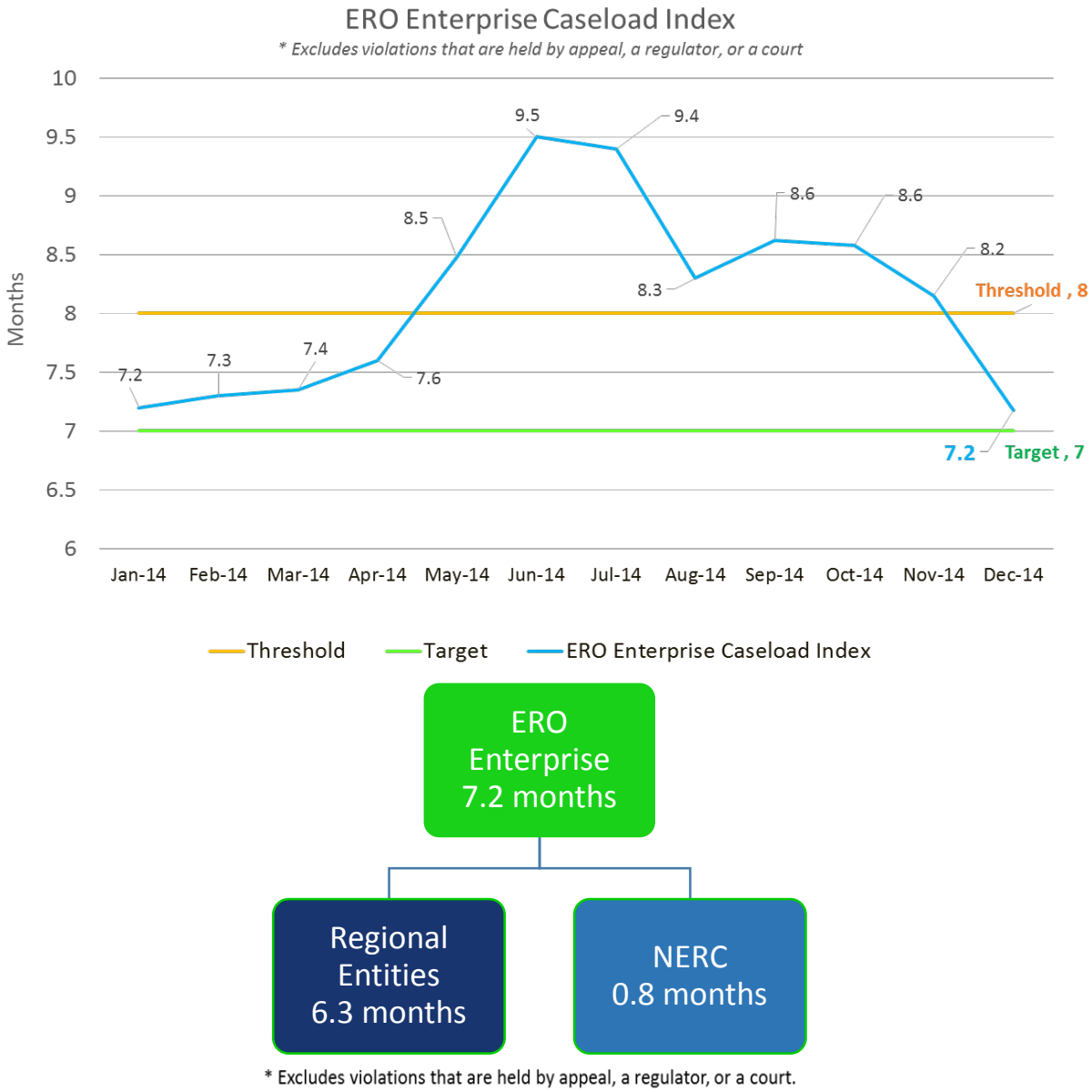


Figure 1: ERO Enterprise Caseload Index

Results in Caseload Reduction

As of January 1, 2015, there are 35 pre-2013 active instances of noncompliance in the ERO Enterprise inventory.[2] The threshold for this metric was to end the year with 65 or fewer instances of noncompliance in the ERO inventory, and the goal was to process fully all of such instances of noncompliance.

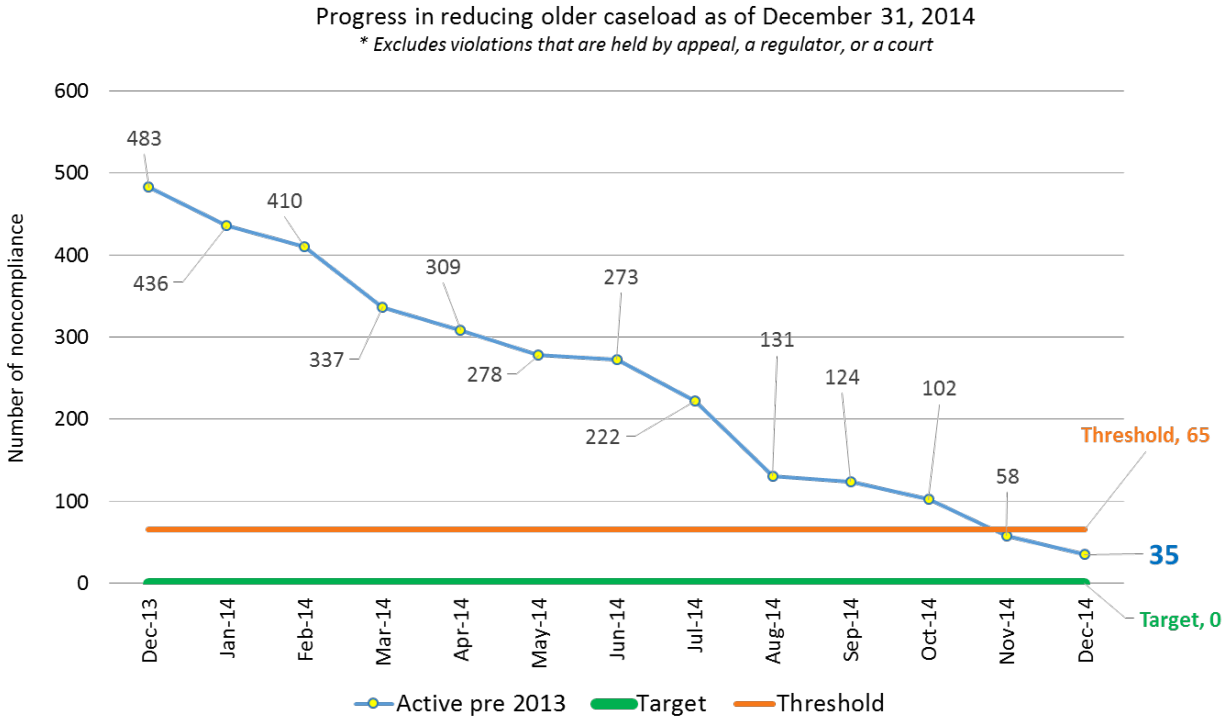
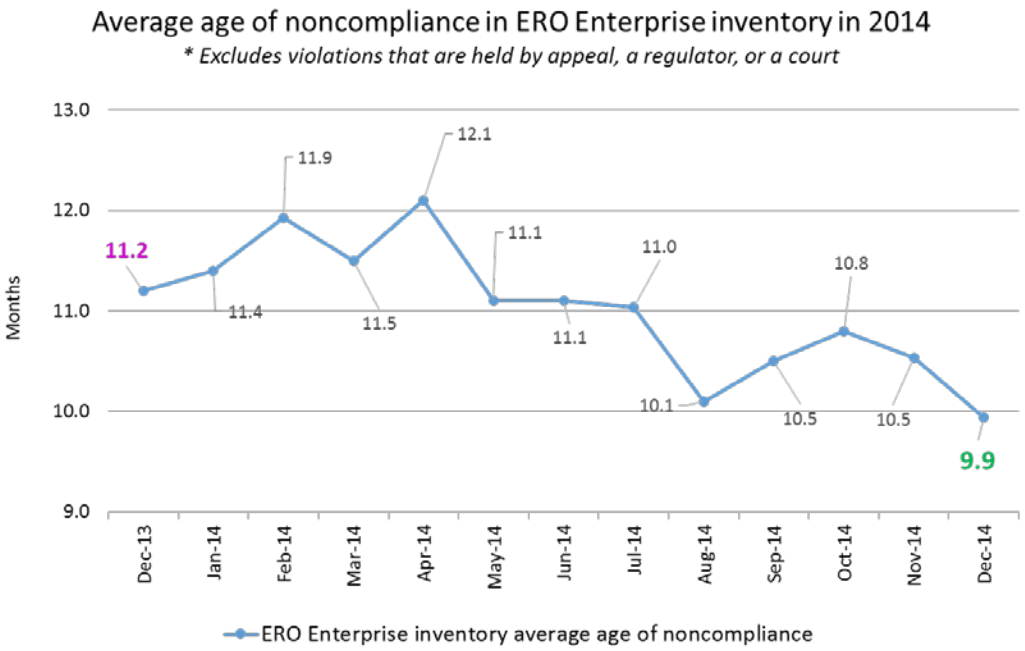


Figure 2: Progress in Reducing Older Caseload

Violation Age in the ERO Enterprise

The significant reduction in the active caseload discovered prior to 2013 in addition to utilization of new disposition mechanisms helped reduce the average age of noncompliance in the ERO Enterprise inventory to 9.9 months. Currently 68% of the cases in the Enterprise inventory are less than a year old. Four percent of the inventory consists of noncompliance discovered before 2013.

[2] The active caseload does not include approximately 350 instances of noncompliance that have been on-hold and not available for processing pending a court decision on the applicability of monetary penalties to federal entities. In August 2014, the court issued a decision holding that monetary penalties are not applicable to federal entities and the ERO Enterprise has developed a plan to resolve a majority of these items during 2015. The processing of these items will continue to be reported separately from the processing of active cases. Despite the on-hold status, a majority of these instances of noncompliance has been mitigated.



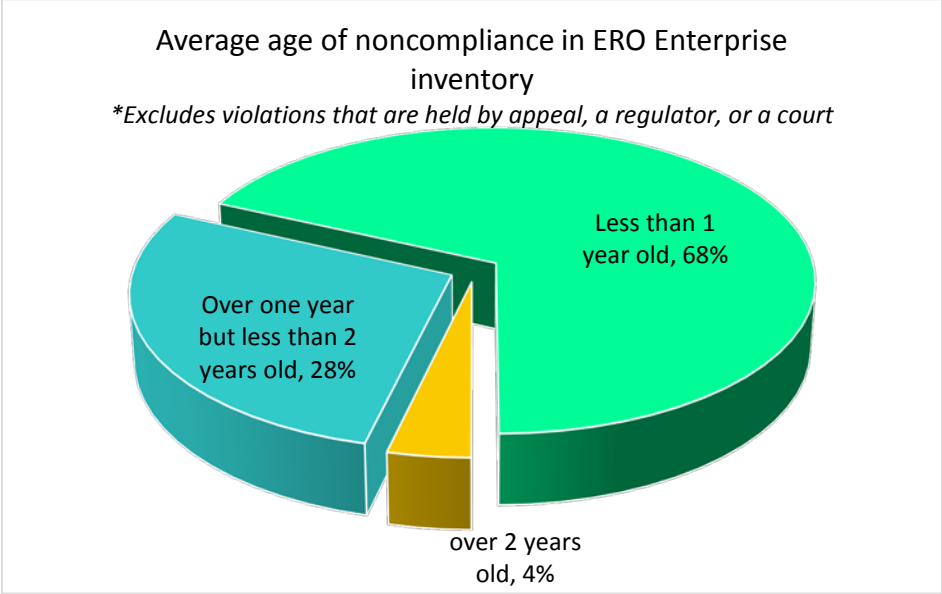


Figure 3: Average Age of Noncompliance in ERO Enterprise Inventory

Promoting Self-Identification of Noncompliance

The ERO Enterprise promoted internal identification of noncompliance in 2014 resulting in 76% of the noncompliance identified in 2014, being self-identified. The target for self-identification of noncompliance was 75%.

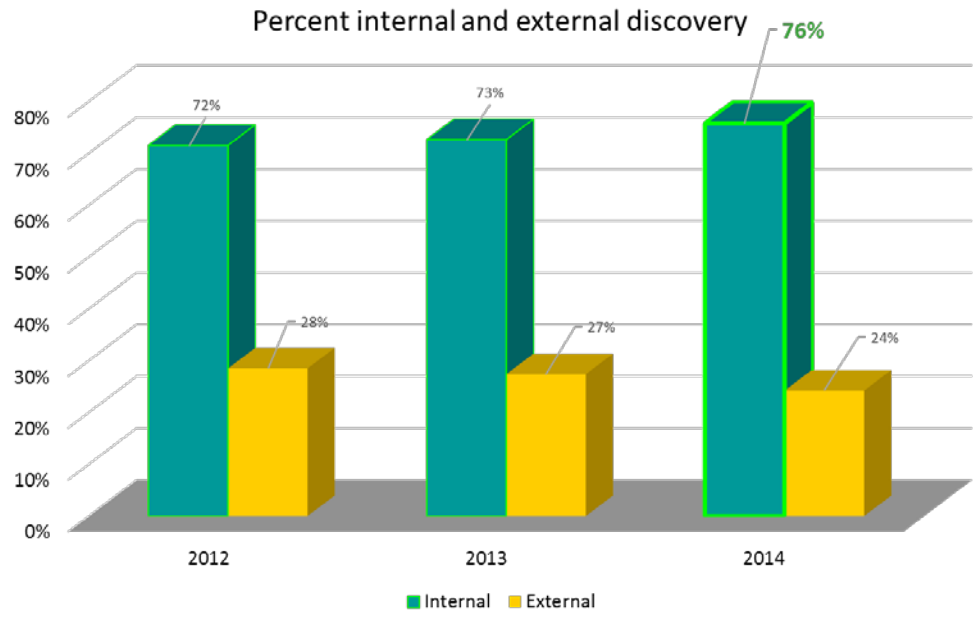


Figure 4: Internal and External Discovery Percentages

The following graph shows the variation of the percentages of internal and external discoveries by quarter during 2014.

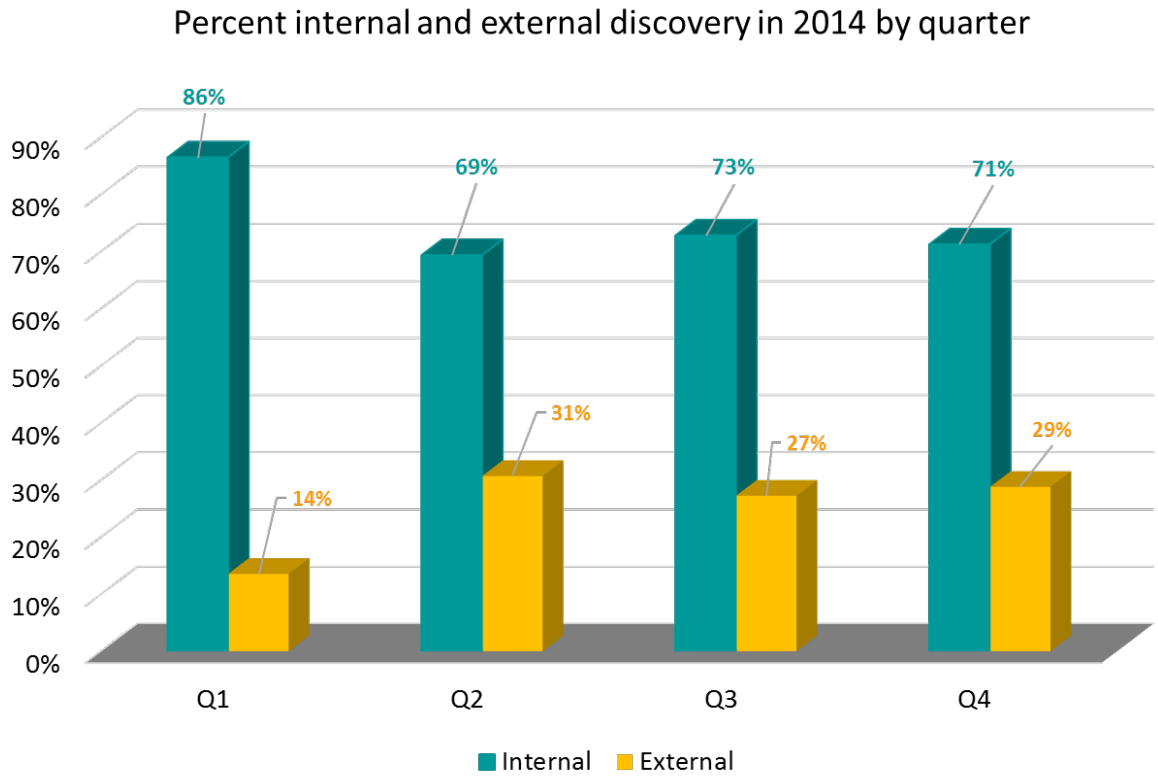


Figure 5: Internal and External Discovery by Quarter

Timeliness of Mitigation

Monitoring Mitigation Completion

NERC carefully monitors mitigation completion time. The objective of this metric is to promote timely mitigation of all noncompliance, which reduces risk to the BPS. The table below shows the ERO Enterprise's targets and thresholds for mitigation completion by discovery year. In all cases, the metric's thresholds have been met. For noncompliance discovered in 2013, the ERO Enterprise exceeded the target by 2%.

Table 1: Mitigation Completion

Discovery year	Progress toward the goal	Threshold	Target
2013	82%	75%	80%
2012	93%	90%	95%
2011	96%	95%	98%
2010 and older	99%	98%	100%

The following graph shows the progress in completion of mitigation plans and activities for cases discovered before 2014. NERC, in collaboration with the Regional Entities, will continue to monitor timely completion of formal mitigation plans and mitigating activities in 2015.

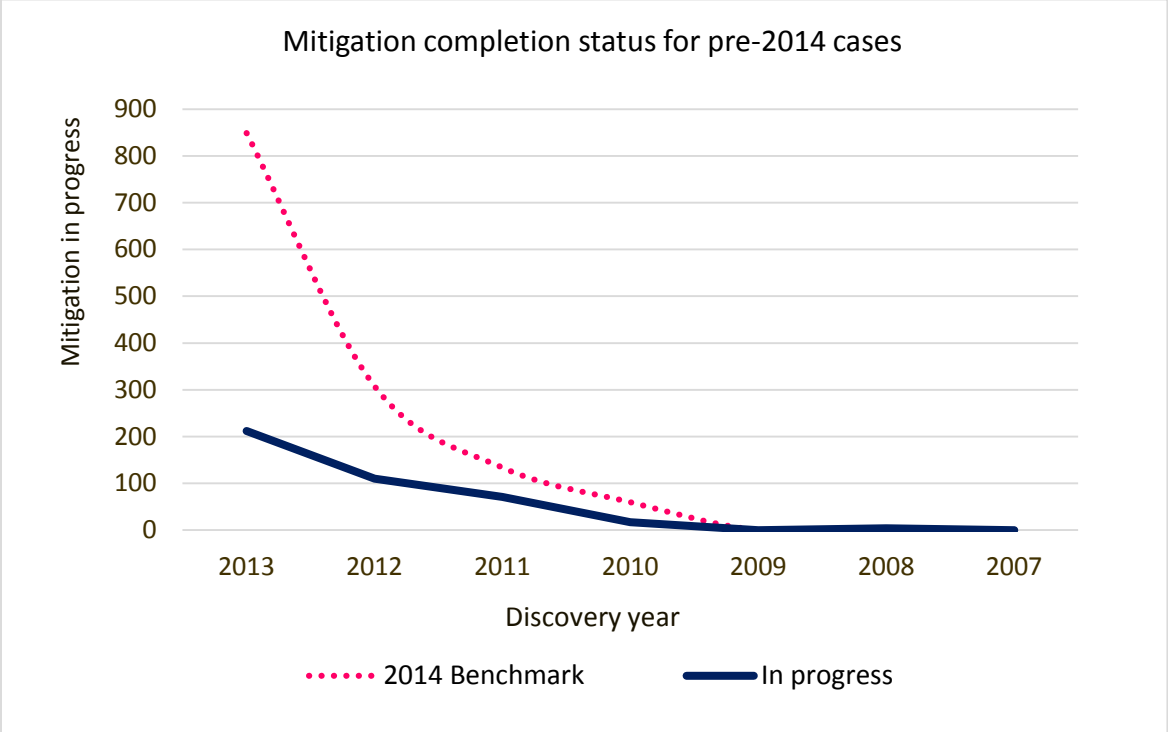


Figure 6: Mitigation Completion Status

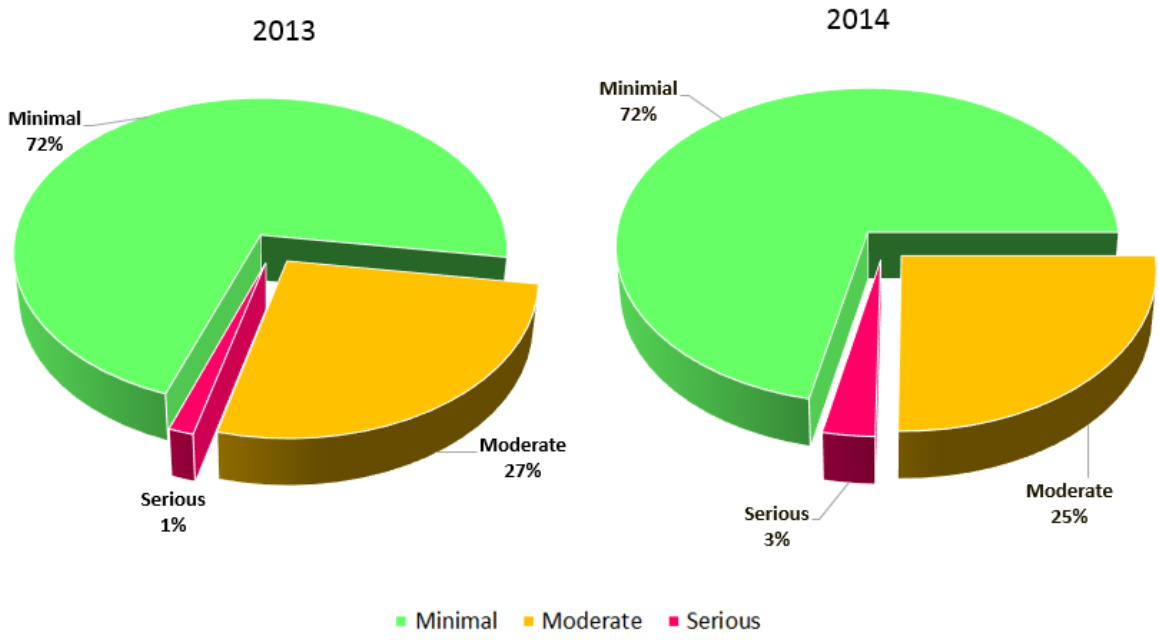
Triage of Incoming Noncompliance

Ninety-six percent of the noncompliance discovered in 2014 completed triage on average within 46 days. This means that Regional Entities contacted the registered entity to request additional information necessary for the disposition of the noncompliance or determined the processing path of the submission by (a) issuing a notice of possible violation (enforcement path), (b) issuing a notice of compliance exception (enforcement discretion) or (c) issued a notice of dismissal. Currently less than 4% of the noncompliance discovered in 2014 is under the triage process (primarily those discovered within the last two months of 2014). In 2015, NERC will perform a spot check of the implementation of the triage process and will analyze the process from a qualitative perspective.

Risk Assessment and Trends by Reliability Standard

The majority of cases resolved in 2014 and 2013 posed a minimal or moderate risk to the reliability of the BPS. As noted in the graph below, the trend of assessed risks in both years is similar.

Figure 7: Requirements Associated with Violations



The table below shows the Reliability Standards and Requirements associated with violations processed in 2013 and 2014 that were deemed to pose a serious or substantial risk to the BPS. Additional information regarding these cases is available at NERC's Enforcement and Mitigation page, at http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx.

Table 2: 2013 and 2014 Serious or Substantial Risk											
Standard	**R1.**	**R2.**	**R3.**	**R4.**	**R5.**	**R6.**	**R7.**	**R8.**	**R12.**	**R15.**	**Grand Total**
FAC-009	1										1
CIP-003					1						1
CIP-004			1								1
TOP-007				1							1
PRC-001		1									1
IRO-009			1								1
TOP-002	1										1
EOP-008	1										1
TOP-004						1					1
IRO-008		2									2
EOP-003	1							1			2
EOP-001			2								2
TOP-001	1	1									2
IRO-001		1	2								3
IRO-002							2	1			3
COM-002		3									3
CIP-005	1	2		1							4
PRC-005	1	3									4
CIP-006	3	2									5
CIP-002	1		5								6
IRO-005	2			2	1	1		1	1	1	9
CIP-007	1	3	3		2			2			11
Grand Total	**14**	**18**	**14**	**4**	**4**	**2**	**2**	**5**	**1**	**1**	**65**

Additional Analysis in 2015

In 2014, the ERO Enterprise developed additional risk-based processes to bring closure that is more expedient to noncompliance posing a minimal risk to the reliability of the BPS. NERC and the Regional Entities continue to monitor all reported noncompliance regardless of its disposition method.

During the course of 2015, NERC will monitor the implementation of the new processes in order to identify areas of excellence and lessons learned.

Agenda Item 5
Board of Trustees Compliance Committee
Open Session
February 11, 2015

Compliance Exception and Self-Logging Report Q4 2014

Action

Information

Introduction

Beginning in November 2013, NERC and the Regional Entities began exercising their inherent discretion whether to initiate a formal enforcement action by identifying minimal risk noncompliance that does not warrant a penalty and which would be recorded and mitigated without triggering an enforcement action. Noncompliance that is not pursued through an enforcement action by the ERO Enterprise is referred to as a "compliance exception."[1]

The compliance exception disposition track builds on the success of the Find, Fix, Track, and Report (FFT) program, which was the first step in implementing a risk-based strategy that recognizes that not all instances of noncompliance require the same type of enforcement process.

In 2013 and 2014, the use of compliance exceptions (as the alternative disposition for noncompliance posing a minimal risk to the reliability of the bulk power system) was limited to allow the testing of the new process. In 2015, this disposition track became available throughout the ERO Enterprise. Utilization of compliance exceptions as a disposition track has increased steadily, as shown in the following graphs.

On a quarterly basis, NERC will provide information regarding the utilization of the compliance exception disposition track, as well as relevant information that could be used by registered entities to understand the types of issues being treated as compliance exceptions and avoid similar noncompliance. Information on the utilization of the self-logging program will also be included.

[1] For more information about compliance exceptions, please visit http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Compliance%20Exception%20Overview.pdf

Utilization of Compliance Exceptions

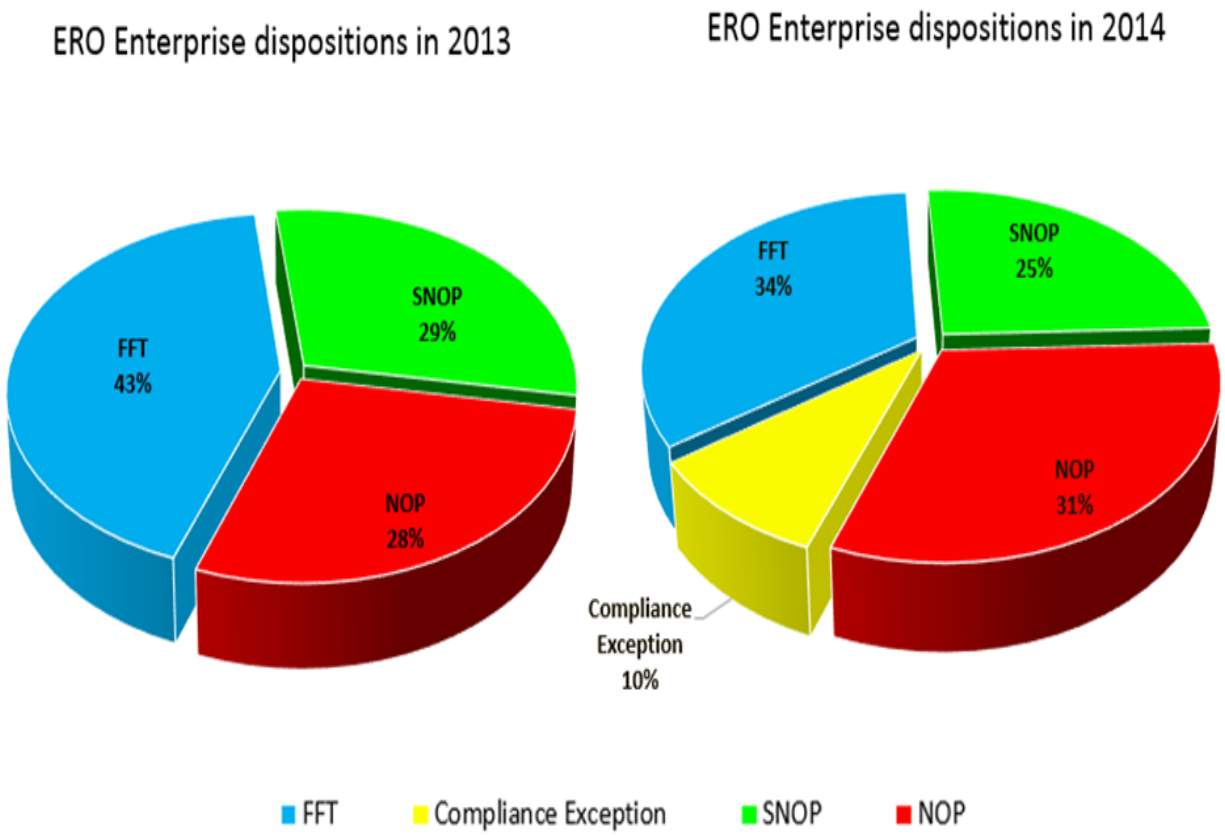


Figure 1: ERO Enterprise Disposition Methods 2013 vs. 2014

In 2013, 43% of noncompliance was disposed through the FFT process. In 2014, 34% of noncompliance was disposed through the FFT process, and 10% were provided compliance exception treatment (see Figure 1). The utilization of streamlined disposition tracks for lesser risk issues remains steady and reflects the continued use of these tracks as well as an initial shift of usage of compliance exceptions in lieu of FFTs. The small increase in the percentage of matters disposed of through an NOP in 2014 reflects the natural variation of the caseload as well as a minor increase in the number of serious violations processed in 2014 compared to 2013.[2]

Figure 2 shows the utilization of compliance exceptions at the Regional Entities. In cases where Regional Entities coordinated the processing of compliance exceptions such that one Regional Entity was responsible for processing them, these items will not appear in the percentages of the other Regional Entities involved. This is the case, for example, of certain compliance exceptions processed by RF on behalf of SPP RE and Texas RE.

[2] See breakdown of violations by risk in the Key Compliance Enforcement Metrics and Trends update, item 4 in this same package.

This data reflects the end of the pilot phase for compliance exceptions. Staff expects that the full-year 2015 data will show a more even distribution of the utilization of the compliance exception disposition track. It should also, consistent with the initial data in Table 1, show an increase in utilization of compliance exceptions and a corresponding reduction of minimal risk issues processed as FFTs, compared to 2014.

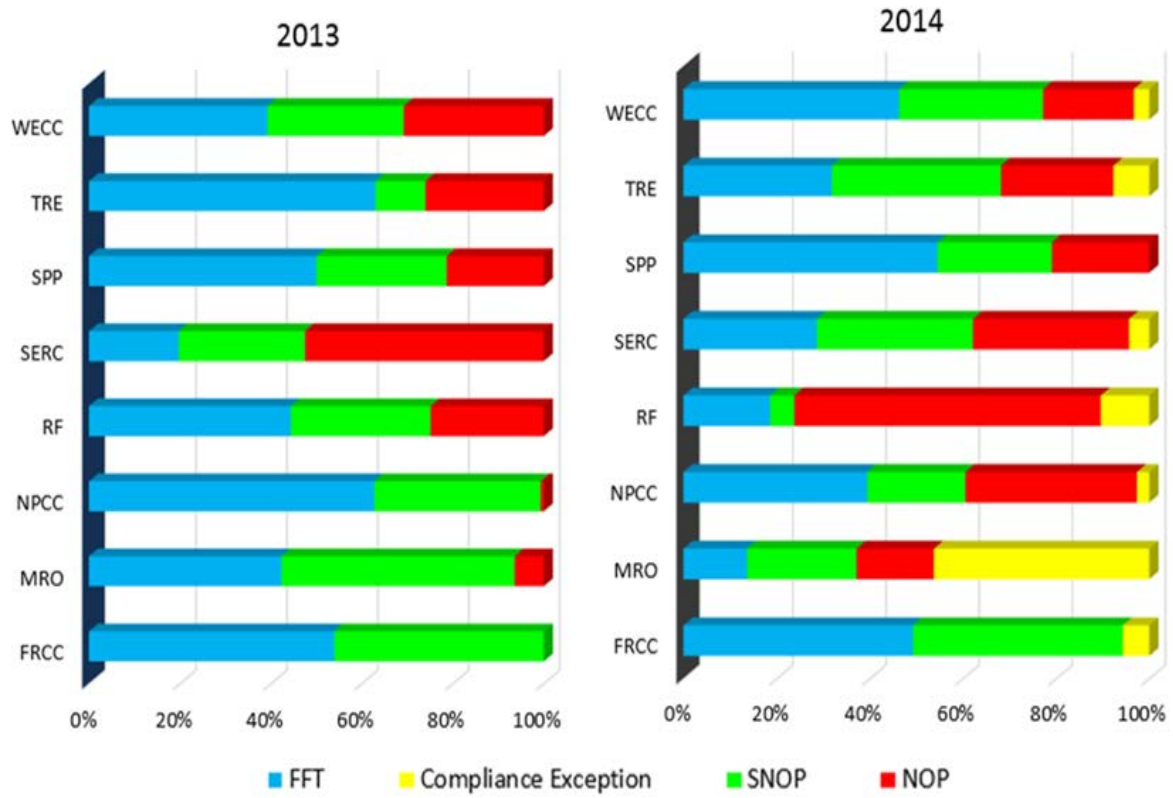


Figure 2: Disposition Methods Used by the Regional Entities 2013 vs. 2014

Utilization of Self-Logging

As of January 1, 2015, 19 registered entities have been permitted to self-log minimal risk noncompliance (see Figure 3 below). The self-logging program (formerly known as the aggregation program) allows any registered entities that have demonstrated effective management practices to keep track of minimal risk noncompliance (and related mitigation) on a log that is periodically reviewed by the Regional Entity. Minimal risk noncompliance added to the log is presumed to be disposed of as a compliance exception.

The program is now available to any registered entity that would like to be evaluated by its Regional Entity in accordance with the program requirements.[3]

[3] For more information about self-logging of minimal risk issues, including program requirements, please visit http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Self-logging%20of%20Minimal%20Risk%20Issues%20Program%20Overview.pdf

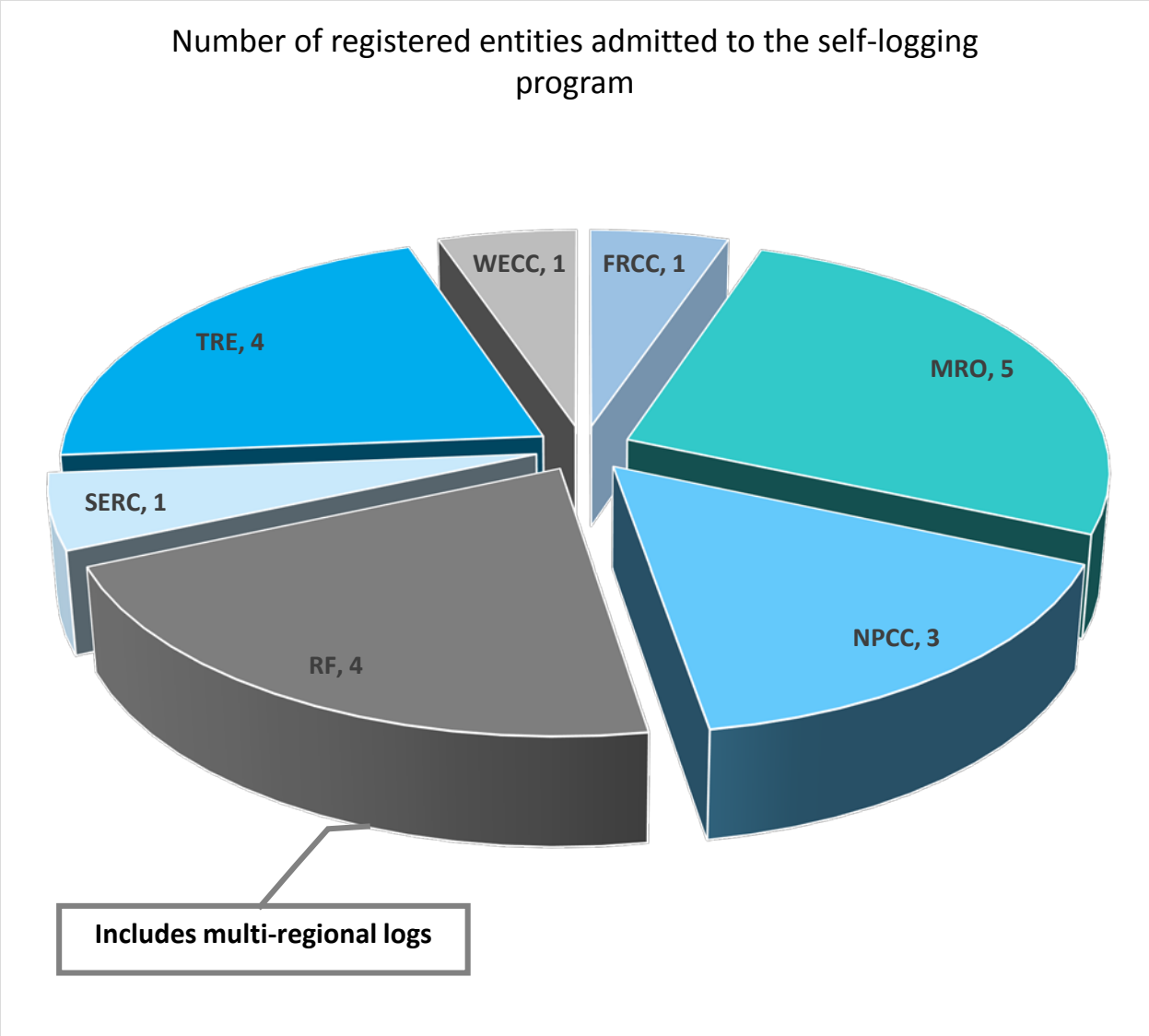


Figure 3: Number of Registered Entities Participating in Self-Logging By Regional Entity

Compliance Exception Trends

The ERO Enterprise disposed of 116 instances of noncompliance as compliance exceptions in 2014. The Regional Entities used the discretion path for issues discovered in 2014 as well as those discovered in past years (see Figure 4).

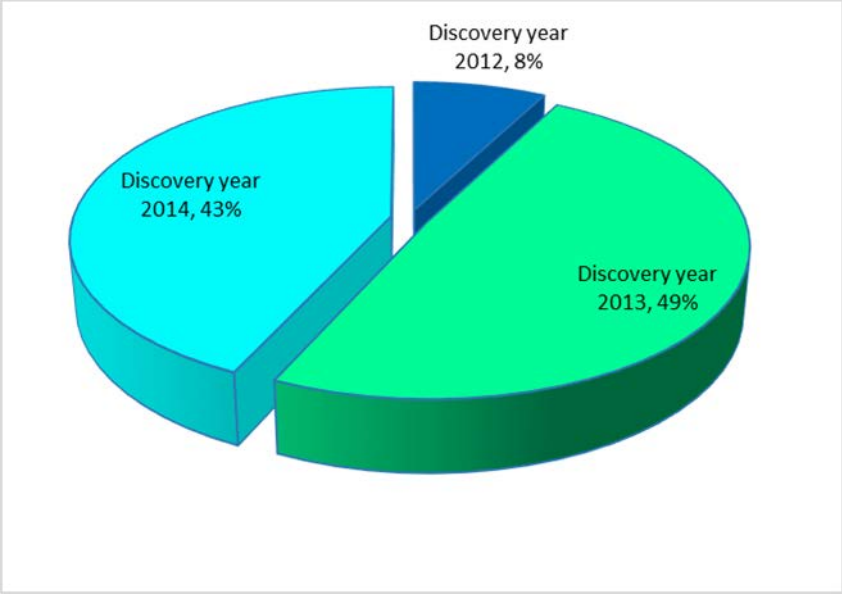


Figure 4: Compliance Exceptions by Discovery Year

Compliance exceptions may come from any of the Reliability Standards. Fifty-three percent of the compliance exceptions related to non-CIP Reliability Standards. Forty-seven percent of the compliance exceptions related to CIP Reliability Standards. Most of the compliance exceptions were internally discovered by the registered entity (see Figure 5 below).

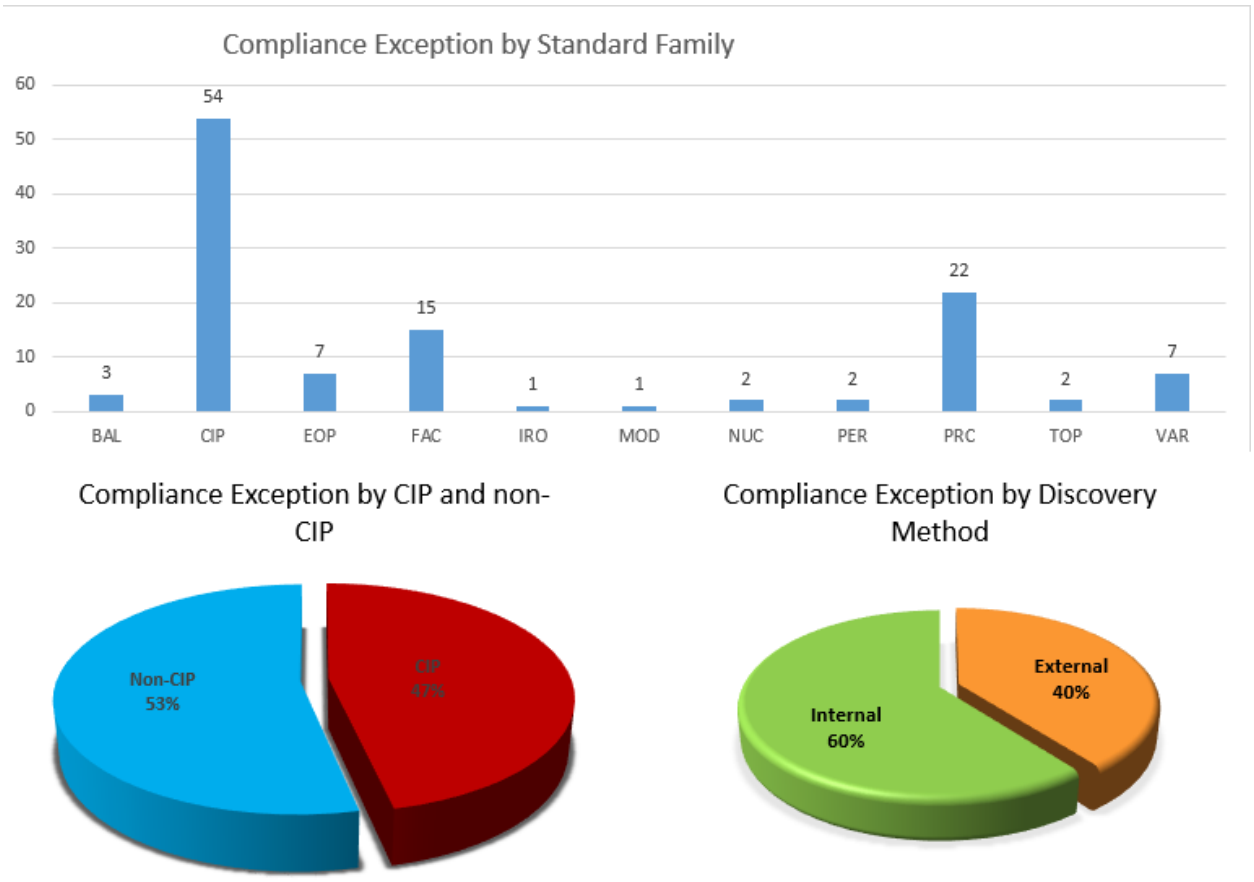


Figure 5: Compliance Exception by Standard Family and Discovery Method

Table 1 below shows a list of the Reliability Standards most frequently involved in noncompliance disposed of as compliance exceptions. The list is similar to the list of Reliability Standards most frequently involved in noncompliance disposed of as FFTs in the past.

A significant number of compliance exceptions relate to CIP-007, CIP-006, and CIP-005. For that reason, NERC is providing some observations related to those compliance exceptions.[4]

[4] CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets (CCAs), as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). CIP-006 is intended to ensure the implementation of a physical security program for the protection of CCAs. CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all CCAs reside, as well as all access points on the perimeter.

Table 1: Count of Compliance Exceptions by Reliability Standard	
Standards	**Number of Compliance Exceptions**
CIP-007	16
PRC-005	16
CIP-006	12
CIP-005	11
CIP-004	9
FAC-008	9
VAR-002	6
CIP-003	4
EOP-008	4
FAC-009	4

Observations and Examples

Below are a number of examples of compliance exceptions processed by the ERO Enterprise. These are grouped into two primary themes: documentation issues and isolated issues.

The Registered Entity had Documentation Issues

A CIP-007-3a R4 related compliance exception involved the registered entity's failure to update a Technical Feasibility Exception (TFE) in a timely manner.[5] The registered entity maintained TFEs for devices that do not support anti-virus or antimalware technologies; however, the registered entity self-discovered that it did not include a complete list of Cyber Assets as amendments to its TFEs. Specifically, the registered entity failed to include 11 Cyber Assets on its antivirus and malware device list. The registered entity was required to update its existing TFE document but failed to do so on time. The registered entity had compensating measures in place.

The compliance exception involved a documentation issue and posed a minimal risk to the BPS. Some of the compensating measures in place included the following: (a) access to the devices was restricted to authorized personnel, (b) malware prevention was installed at all access points to the Electronic Security Perimeter (ESP), and (c) the devices were within a Physical Security Perimeter (PSP).

The Mitigation Activities involved training staff on the TFE process, updating the TFEs, and updating the change control and configuration management form.

In a CIP-006-3c R2-related compliance exception, the registered entity did not update its physical access control (PAC) system account management procedure within 30 days as required by the

[5] **R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

Reliability Standard.[6] The registered entity self-discovered that it did not update its PAC system procedure as required by the Reliability Standard. The noncompliance involved a delay in removing steps from the PAC procedure and could not have resulted in granting of unwanted physical access privileges. To mitigate this issue, the registered entity revised and approved a new procedure.

A CIP-007-3a R3 compliance exception involved the registered entity's failure to document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades for four patches.[7] The four patches were not evaluated within the 30-calendar-day window as required.

The registered entity self-discovered the issue within two months of the start date of the noncompliance through its internal controls. The registered entity concluded that a system administrator failed to evaluate four security patches within the 30-day time requirement because of failed oversight to verify the four security patches were evaluated within the 30-day time requirement. To date, all patches released have been evaluated. Additionally, all patches identified as relevant through evaluation have been applied, and the registered entity is now compliant with the evaluation of patches. In addition to self-discovering the noncompliance in a timely manner via controls, the registered entity had compensating measures in place.

The registered entity has several other physical and electronic access controls in place to provide supplemental measures to prevent potential exposure to any Critical Cyber Assets (CCAs), curtailing any possible or actual adversities to the system. The registered entity's CCAs are protected by a PAC system that creates the PSP per CIP-006; its CCAs have electronic access points that are created and managed by a separate system that creates the ESP per CIP-005; and The CCAs that reside inside the ESPs use additional authentication mechanisms per CIP-007.

In a CIP-005-3a R1.5-related compliance exception, the registered entity did not follow its change management process in the completion of a checklist when it replaced a Cyber Asset used in electronic access control and monitoring (EACM).[8] The new Cyber Asset was previously tested and configured on the ESP network. However, the registered entity reconnected the device to

---

[6] **R2.** Protection of Physical Access Control Systems — Cyber Assets that authorize and log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
R2.1. Be protected from unauthorized physical access.
R2.2. Be given the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

[7] **R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all Cyber Assets within the Electronic Security Perimeter(s).

[8] **R1.** Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

the ESP to replace another device and did not complete the add/remove checklist as required by its policy. The registered entity had compensating measures in place.

The risk was reduced as the new EACM Cyber Asset was given all the required protections of the Reliability Standards before connection to the production network. Furthermore, the device did not have control of any BPS asset. This was a documentation error in not completing the procedural checklist until after the EACM was connected to the production ESP network and elevated to a production status.

The registered entity mitigated the noncompliance by completing the checklist, updating the coversheet on the checklist to clarify expectations, and trained support staff.

The Registered Entity Self-Reported an Isolated Instance of CIP Noncompliance

In another compliance exception, the registered entity self-discovered a noncompliance with CIP-006-3c R1.[9] The registered entity detected a series of invalid access attempts at a site when staff was alerted by alarms from the facility's PAC system. Security personnel who were requested to investigate the alarm gained unescorted access to a PSP without prior approval. While investigating the alarm, the security personnel discovered a door that was not secure. The security personnel entered the PSP, unescorted, to verify that no suspicious activity was taking place.

The registered entity personnel immediately discovered the unescorted access because it was actively monitoring closed-circuit television of the area. The registered entity personnel asked the security personnel at the site to leave the area. The security personnel secured the control room door and exited the PSP within five minutes. Although the registered entity demonstrated

[9] **R1.** Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
R1.2. Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.
R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.
R1.7. Update of the physical security plan within 30 calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.
R1.8. Annual review of the physical security plan.

quick identification of the noncompliance, it failed to implement its visitor control program for visitors to a PSP as required by the Reliability Standard; however, as detailed above, the visitors were security personnel who were there to investigate an alarm. The registered entity demonstrated appropriate usage of controls that served as compensating measures.

The registered entity immediately detected and corrected the noncompliance, which limited its duration to approximately five minutes. Although the security personnel failed to follow certain procedures, the deviation occurred under the circumstances because the security officers had determined the door lock was not secure and the investigation of the suspicious activity was time-sensitive.

To mitigate the noncompliance, the registered entity updated its emergency response procedure to declare a response to an alert from the PACS an emergency so that armed security personnel may respond accordingly.

For another CIP-006-3c R1 and R1.6.2-related compliance exception, the registered entity self-reported that it failed to provide continuous escorted access of a visitor within the PSP as required by its visitor control program.

At a monthly meeting, a presenter who was an employee of the registered entity did not have unescorted access privileges in the area where a meeting was being held, which was also within a PSP. Upon completing the presentation, the employee left the PSP unescorted and proceeded to leave the building. The visitor was unescorted for approximately three minutes. The registered entity had compensating measures in place.

The employee did not have access to areas that contain ESPs. In addition, additional badge access is required to enter any areas where an ESP exists. In addition, the employee in question had a background check performed approximately three years before the issue.

In a similar compliance exception, the registered entity self-reported an issue with CIP-006-3c R1 because it had failed to provide continuous escorted access to visitors within a PSP. Specifically, the registered entity did not escort a visitor within a PSP for 13 minutes.

The mitigating factors concerning the noncompliance included the short duration of the violation and the unescorted visitor who was in the training room and not a more sensitive location.
To mitigate the issue, the registered entity investigated the event and trained staff. Specifically, it investigated to ensure that no harm occurred by reviewing PSP access records, login records of the equipment in the training room, and interviewed the individuals involved to understand the facts and circumstances of the noncompliance. In addition, the registered entity retrained staff on its security procedures.

Additional Resources

- Analyzing Enforcement Data
- Violation Statistics
- Compliance Exception Overview
- Self-logging Overview