

February 18, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

**Re: North American Electric Reliability Corporation, Docket No. RR15-2-000
Annual Compliance Monitoring and Enforcement Program Filing**

Dear Ms. Bose,

The North American Electric Reliability Corporation submits this annual Compliance Monitoring and Enforcement Program filing in Docket No. RR15-2-000.

Please contact the undersigned if you have any questions concerning this filing.

Respectfully submitted,

/s/

Sonia C. Mendonca

Counsel for the North American Electric
Reliability Corporation

TABLE OF CONTENTS

I.	EXECUTIVE SUMMARY	2
II.	RISK-BASED CMEP PROGRESS AND OBSERVED TRENDS	3
	A. Progress	4
	B. Observed Trends	5
	1. General Trends	5
	2. Compliance Exception Trends	6
	C. Risk-based CMEP Enhancements	7
III.	INTERPLAY BETWEEN CMEP AND OTHER PROGRAM AREAS	7
	A. Feedback Loop between CMEP and Reliability Standards Development	10
	B. Analysis of BPS Events	13
IV.	INTERNAL CONTROLS EVALUATION	16
V.	USE OF LEARNING TOOLS	20
VI.	NERC OVERSIGHT	22
	A. Oversight of Compliance Monitoring Activities	24
	1. Phase I Assessment	24
	2. Other Oversight Activities	24
	B. Oversight of Enforcement Activities	27
VII.	METRICS	29
	A. Effect of Risk-Based CMEP on Reliability	31
	B. Implementation of Risk-Based CMEP	32
VIII.	CONCLUSION	35

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

NORTH AMERICAN ELECTRIC) Docket No. RR15-2-000
RELIABILITY CORPORATION)

**NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION'S
ANNUAL COMPLIANCE MONITORING AND ENFORCEMENT PROGRAM FILING**

Sonia C. Mendonca
Vice President of Enforcement and Deputy
General Counsel
Shamai Elstein, Senior Counsel
Arthur L. Brown, Counsel
North American Electric Reliability
Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net
shamai.elstein@nerc.net
arthur.brown@nerc.net

*Counsel for the North American Electric
Reliability Corporation*

February 18, 2016

**UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION**

NORTH AMERICAN ELECTRIC) Docket No. RR14-5-000
RELIABILITY CORPORATION)

**NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION’S
ANNUAL COMPLIANCE MONITORING AND ENFORCEMENT FILING**

The North American Electric Reliability Corporation (“NERC”) submits this annual Compliance Monitoring and Enforcement Program (“CMEP”) filing in accordance with the Federal Energy Regulatory Commission’s (“FERC” or the “Commission”) February 19, 2015, *Order on Electric Reliability Organization Reliability Assurance Initiative and Requiring Compliance Filing*¹ and its November 4, 2015, *Order Conditionally Accepting Compliance Filings*.²

This annual CMEP filing is organized as follows:

- **Section I – Executive Summary**
- **Section II – Risk-based CMEP Progress and Trends:** Describes the progress of the risk-based CMEP and discusses observed trends. Incorporates the attached [2015 ERO Enterprise Compliance Monitoring and Enforcement Program Annual Report](#) (“Annual

¹ *North American Electric Reliability Corporation*, 150 FERC ¶ 61,108 (2015) (“February 19 Order”). In the February 19 Order, the Commission conditionally approved the implementation of the risk-based CMEP, finding that the “overall goal of focusing ERO and industry compliance resources on higher-risk issues that matter more to reliability is reasonable.” *Id.* at P 2. The Commission also directed NERC, among other things, to submit an annual informational filing, within one year from the date of the issuance of the order, to review the progress of the risk-based CMEP and to address a number of other specific topics regarding oversight processes and implementation assessment.

² *North American Electric Reliability Corporation*, 153 FERC ¶ 61,130 (2015) (“November 4 Order”). The November 4 Order conditionally accepted NERC’s May 20 and July 6 compliance filings and directed NERC to, among other things, include additional information in this filing addressing NERC’s risk-based CMEP oversight and the metrics designed to track risk-based CMEP performance.

Report”) and references relevant information contained in prior quarterly updates issued by NERC throughout 2015.

- **Section III – Interplay between Risk-based CMEP and Other Program Areas:** Discusses the interplay between the risk-based CMEP and other NERC program areas, including the feedback loop to the Reliability Standards development process.
- **Section IV – Internal Controls Evaluation:** Addresses the Commission’s directive to discuss whether a baseline audit is needed to properly evaluate a registered entity’s internal controls when performing an Internal Control Evaluation (“ICE”).
- **Section V – Use of Learning Tools:** Addresses the Commission’s directive to discuss how a Regional Entity assesses and factors into a registered entity’s risk assessment and audit scope that entity’s use of NERC Alerts, Lessons Learned, Reliability Guidelines, and other NERC learning tools.
- **Section VI – Oversight:** Describes NERC’s oversight processes and assessment of the implementation of the risk-based CMEP.
- **Section VII – Metrics:** Discusses the metrics NERC will track to measure the success of the risk-based CMEP.

I. EXECUTIVE SUMMARY

In 2015, NERC and the eight Regional Entities made significant progress implementing the risk-based CMEP. This annual CMEP filing addresses the key activities that occurred in 2015, which are further discussed in the attached Annual Report. As indicated in the Annual Report, the risk-based CMEP has allowed the ERO Enterprise to focus on issues that matter more to reliability.

This filing also discusses how the interplay between CMEP and other program areas is being enhanced through the risk-based approach adopted by the ERO Enterprise.³ As discussed further below, the risk-based CMEP promotes the information flow between compliance monitoring and enforcement activities to various ERO Enterprise programs and departments. This enhanced communication framework is central to identifying and managing Bulk Power System (“BPS”) risks, establishing ERO Enterprise priorities to focus compliance resources on higher-risk issues, and identifying and implementing lessons learned.

In 2015, NERC transitioned its oversight activities to align with the risk-based CMEP. Through oversight activities, NERC found that all eight Regional Entities are actively engaged in risk-based CMEP activities. Among other things, NERC found that compliance monitoring activities had a clear focus on reliability risks and minimal risk noncompliance categorized as Compliance Exceptions received consistent and appropriate treatment.

Lastly, the ERO Enterprise has begun to develop a number of ways to measure the effect of risk-based CMEP on BPS reliability and the success of the ERO Enterprise’s implementation of the risk-based CMEP. These metrics, which are described herein, will continue to be refined in collaboration with FERC staff.

II. RISK-BASED CMEP PROGRESS AND OBSERVED TRENDS

In the February 19 Order, the Commission accepted NERC’s commitment to submit an annual informational filing to FERC “reviewing the progress of the [risk-based CMEP] and

³ The ERO Enterprise refers to the affiliation between NERC and the eight Regional Entities for the purpose of coordinating goals, objectives, metrics, methods, and practices across statutory activities. The operation of the ERO Enterprise does not conflict with obligations of each organization through statutes, regulations, and delegation agreements. The activities discussed in this report relate to compliance monitoring and enforcement performed in connection with United States registered entities. ERO Enterprise activities outside of the United States are not specifically addressed.

considering any enhancements or expansions that may be necessary...[T]he informational filing would include observed trends by standard, region or other categories, as well as examples of matters treated as compliance exceptions.”⁴

A. Progress

The implementation of the risk-based CMEP and the progress made in 2015 are described in greater detail in the attached Annual Report. The Annual Report highlights key CMEP activities that occurred in 2015, provides information and statistics regarding those activities, and previews the ERO Enterprise’s 2016 CMEP priorities. The topics addressed in the Annual Report that are relevant to this filing are discussed here in summary form. The entire Annual Report is attached as Appendix A.

As noted in the Annual Report, the risk-based CMEP involves the use of an oversight plan framework⁵ focused on identifying, prioritizing, and addressing risks to the BPS to enable the ERO Enterprise to allocate resources where they are most needed and likely to be the most effective. After completing the risk-based CMEP design in early 2015, the ERO Enterprise began initial implementation activities. Specifically, the ERO Enterprise (1) conducted **Inherent Risk Assessments** (“IRAs”) to review the inherent risks posed by individual registered entities to BPS reliability; (2) performed ICEs to evaluate whether registered entities have implemented effective internal controls; and (3) used various methods to process noncompliance based on risk (including the **Self-Logging** program and **Compliance Exceptions**). For example, during 2015, the ERO Enterprise conducted 331 IRAs and 51 ICEs. The ERO Enterprise resolved nearly 70% of minimal

⁴ February 19 Order at P 49.

⁵ A visual representation of the risk-based framework is available at <http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Risk-Based%20Compliance%20Monitoring%20and%20Enforcement%20Program%20Visual%20Overview.pdf>.

risk noncompliance in 2015 as Compliance Exceptions.⁶ In addition, by the end of 2015, 42 registered entities had been approved to self-log. These registered entities represent nearly all of the reliability functions.

The ERO Enterprise also continued to maintain a consolidated Implementation Plan that provides guidance and implementation information common among NERC and the eight Regional Entities, including risks to the BPS (referred to as risk elements) to focus compliance monitoring. Overall, these activities supported compliance monitoring planning, focused the oversight of registered entities, and provided greater efficiency in enforcement activities. Other major milestones include training and educating ERO Enterprise staff regarding risk-based CMEP processes.

B. Observed Trends

1. General Trends

Over the course of 2015, NERC tracked noncompliance with the Reliability Standards at all risk levels to identify patterns, trends, and areas of focus. The review of this information helps to identify practices to assist in preventing similar noncompliance. As an example, in its [CMEP Quarterly Update for Q3 2015](#) (“Q3 2015 Update”), NERC reviewed serious risk violations occurring from 2007 on, and identified the Reliability Standards and Requirements most prevalent in such violations. In addition, NERC reviewed the non-Critical Infrastructure Protection (“CIP”) portion of the serious risk violations (93 violations) and identified high-level initial trends regarding common causes of such violations.

In the Q3 2015 Update, as well as in its Annual Report, NERC also reported on mitigation completion trends. NERC regularly tracks completion of mitigation associated with all

⁶ Additional detail on the use of various disposition tracks for noncompliance is also found in the Annual Report at pp. 13-16.

noncompliance to identify and understand any outstanding risks to the reliability of the BPS due to noncompliance with Reliability Standards. As indicated in those documents, registered entities continue to complete timely mitigation for the vast majority of noncompliance.⁷

Finally, NERC continues to track, in quarterly updates and in the Annual Report, levels of self-identification of noncompliance by registered entities. In 2015, registered entities self-identified 84% of the noncompliance.⁸

2. Compliance Exception Trends

The use of Compliance Exceptions allows the ERO Enterprise to dispose of noncompliance posing a minimal risk to the reliability of the BPS efficiently, and enhance its focus on noncompliance posing a moderate or serious risk to BPS reliability. Throughout 2015, the ERO Enterprise has appropriately treated minimal risk noncompliance as Compliance Exceptions. Indeed, out of 741 instances of minimal risk noncompliance processed in 2015, the ERO Enterprise disposed of 514 as Compliance Exceptions. Other instances of noncompliance posing a minimal risk were processed through different disposition tracks based on the underlying facts and circumstances. For examples of instances of noncompliance posing a minimal risk that were not treated as Compliance Exceptions, please see the [CMEP Quarterly Update for Q1 2015](#) (“Q1 2015 Update”).⁹ As a general matter, this resulted from the aggregated risk of the subject violations. The Q1 2015 Update also includes illustrative examples of matters treated as Compliance Exceptions involving CIP and Operations and Planning issues. As noted therein, and as can be

⁷ Annual Report at p. 34.

⁸ *Id.* at p. 35.

⁹ See also the CMEP Quarterly Update for Q2 2015 at <http://www.nerc.com/pa/comp/CE/Compliance%20Violation%20Statistics/Compliance%20Violation%20Statistics%20-%20Second%20Quarter%202015.pdf>. All of the quarterly updates published in 2015 can be found at <http://www.nerc.com/pa/comp/CE/Pages/Compliance-Violation-Statistics.aspx>.

seen in subsequently posted Compliance Exceptions, those matters posed a minimal risk to the reliability of the BPS.

C. Risk-based CMEP Enhancements

There are no specific changes to the risk-based CMEP design or NERC Rules of Procedure being requested at this time. The ERO Enterprise continues to learn from its experience in implementing risk-based CMEP and may identify enhancements in a future filing to FERC. For example, it may be appropriate, in the future, to afford greater flexibility with respect to requirements applicable to monitoring of certain types of entities. It may also be appropriate to consider enhancements to the Self-Logging program that may be identified through the review process to be initiated in 2016.

III. INTERPLAY BETWEEN CMEP AND OTHER PROGRAM AREAS

In the February 19 Order, the Commission stated that “[t]he annual report should also address the interplay between the RAI program and other NERC program areas.”¹⁰ The Commission highlighted two areas of focus: (1) the feedback loop between the CMEP and the Reliability Standards development process, and (2) the analysis of BPS events. Below is a description of the relationship between the risk-based CMEP and the standard development process and Events Analysis.

Importantly, the interplay between the CMEP and other program areas, including Reliability Standards development and Events Analysis, is part of a broader ERO Enterprise-wide effort to promote the information flow between the various programs and departments in the ERO Enterprise. A robust communication framework throughout the ERO Enterprise is essential for, among other things, identifying and managing BPS risks, establishing ERO Enterprise priorities

¹⁰ February 19 Order at P 50.

to ensure that the ERO Enterprise and industry focus their resources in the appropriate places, and identifying and implementing lessons learned across ERO Enterprise programs and departments. Identified risks may be addressed through various means, including but not limited, to guidelines, Reliability Standards, or training.

There are a number of mechanisms or feedback loops across the ERO Enterprise that facilitate the exchange of information across programs. These feedback loops occur both at the strategic level as well as at the operational level. At the strategic level, for example, the Reliability Issues Steering Committee (“RISC”), an advisory committee of the NERC Board of Trustees (“Board”), uses data and information from ERO Enterprise programs to assist the Board by identifying risks. The RISC also sets priorities and goals for the development of solutions to address risks of strategic importance to BPS reliability. The RISC draws feedback from CMEP activities, and from the technical committees of the Board (e.g., the Operating Committee, the Planning Committee, and the Critical Infrastructure Protection Committee), as well as research and analysis conducted by NERC staff. The RISC also provides recommendations to the Board on the strategic approach that NERC should take to enhance reliability and manage identified risks.¹¹ The Board and NERC staff use the RISC’s recommendations to inform the setting of priorities throughout the ERO Enterprise. These reports are part of the strategic framework for steering, developing, formalizing, and organizing recommendations to help NERC and industry effectively focus their resources on the critical issues needed to best improve the reliability of the BPS.

¹¹ The most recent RISC report is available at http://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO_Reliability_Risk_Priorities_RISC_Recommendations_to_the_Board.pdf.

As an example of how the feedback loops work at the operational level, the development of the annual ERO CMEP Implementation Plan is illustrative. To develop the CMEP Implementation Plan, NERC follows the Risk Elements Guide, which outlines the process by which the ERO Enterprise will identify and prioritize continent-wide risks to the reliability of the BPS, as well the Reliability Standards and registration functional categories related to those risks.¹² Under the Risk Elements Guide, NERC identifies and prioritizes risks to reliability of the BPS by taking into account data and information from other ERO Enterprise departments, such as the Reliability Assessment and System Analysis group and the Reliability Risk Management group, which includes NERC's Bulk Power System Awareness, Event Analysis, and Performance Analysis departments. NERC also uses the expert judgment of the ERO Enterprise staff and the associated technical committees and their subcommittees.

Specifically, in addition to using compliance and enforcement data to inform the CMEP Implementation Plan, NERC staff collects and analyzes the available ERO Enterprise data, reports and publications that identify reliability risks. These additional sources of data include: the State of Reliability Report; the Long-Term Reliability Assessment; publications from the RISC; special assessments or reports from NERC's Reliability Assessment and System Analysis group or NERC technical committees; the ERO Enterprise Strategic Plan; ERO Event Analysis process insights; significant occurrences noted by NERC and Regional Entity Situational Awareness and Event Analysis staff; and other relevant documents pertaining to risks to the reliability of the BPS. All of this information helps identify and prioritize risk and inform the development of the CMEP Implementation Plan.

¹² The Risk Elements Guide is available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/2016%20CMEP%20IP_v_2_11172015_ForPosting.pdf.

These types of feedback loops also exist between CMEP and Reliability Standards development and Event Analysis, as discussed below.

A. Feedback Loop between CMEP and Reliability Standards Development

The feedback loop between the CMEP and Reliability Standards development does not consist of a single process; instead, it consists of various mechanisms for ERO Enterprise compliance and enforcement staff to provide input into the Reliability Standards development process. Specifically, where ERO Enterprise compliance and enforcement staff identify a risk that should be addressed through a Reliability Standard, there are available mechanisms for the ERO Enterprise to initiate a Reliability Standard development project, or for NERC and Regional Entity compliance staff to provide input on Reliability Standards already in development. ERO Enterprise staff provide input to Standards under development through, among other things, participation during standard drafting team meetings and the development of Reliability Standard Audit Worksheets (“RSAWs”), as discussed further below.

The most direct feedback loop between the CMEP and the Reliability Standards development process is the mechanism for NERC and Regional Entities to propose a new Reliability Standard, modifications to an existing Reliability Standard, or the retirement of an existing Reliability Standard, based on, among other things, risks identified from their compliance monitoring and enforcement activities. The Regional Entity or NERC may submit a Standards Authorization Request (“SAR”) to propose a new or modified Reliability Standard or retire an existing Reliability Standard where staff concludes changes are necessary. This conclusion to submit a SAR may be based on a BPS risk not being adequately addressed in the Reliability Standards, an existing Reliability Standard being ambiguous, or an existing Reliability Standard providing little to no benefit to reliability, among other things.

A recent illustrative example of this feedback loop involves the flow of information from the Midwest Reliability Organization (“MRO”) IRA process, analyzed in conjunction with a diverse group of registered entities, including a Transmission Owner/Operator, two Generator Owner/Operators, a Canadian entity, and a vertically integrated cooperative, to the NERC Reliability Standards development process. Specifically, in 2015, the MRO Board of Directors tasked the MRO Standards Committee with creating a sub-committee to review a list of Reliability Standard requirements identified as low risk through MRO’s IRA process to determine whether such requirements were unnecessary for BPS reliability, consistent with Commission precedent.¹³

As a result of this analysis, a diverse group of MRO registered entities submitted a SAR to the NERC Standards Committee proposing the retirement of Requirement R3 of Reliability Standard VAR-001-4 (Voltage and Reactive Control) based on the results of IRAs performed within the MRO region. The analysis identified several other requirements that are candidates for retirement, but it was determined that the others were being addressed by existing standard development projects. The Standards Committee merged the SAR for the retirement of Reliability Standard VAR-001-4, Requirement R3 with the enhanced periodic review for Reliability Standards VAR-001 and VAR-002, NERC Project 2016-EPR-02 - Enhanced Periodic Review of Voltage and Reactive Standards. The enhanced periodic review team for Project 2016-EPR-02 will address the issues raised in the SAR.

The CIP V5 Transition Program is also an example of how compliance and enforcement matters inform and influence the Reliability Standards development process. Following the issuance of Order No. 791, which approved new and modified CIP Reliability Standards, referred

¹³ In the February 19 Order, the Commission noted that “[t]he adoption of the streamlined RAI programs to process lower risk compliance matters suggest that there may be provisions of Reliability Standards that provide little protection to the reliable operation of the Bulk Power System, and we support NERC’s efforts to identify such provision for proposed retirement.” February 19 Order at n. 47.

to as the CIP Version 5 Reliability Standards (the “CIP V5 Standards”), the ERO Enterprise’s compliance monitoring group initiated a program to support industry’s transition to the CIP V5 Standards. Among other things, NERC conducted an implementation study and formed a transition advisory group, consisting of representatives from NERC, Regional Entities, and registered entities,¹⁴ to issue guidance regarding possible methods to achieve compliance to support industry’s implementation activities. The guidance documents are intended to help entities implement the CIP V5 Standards effectively and mitigate risks associated with inadequate implementation approaches. Further, because certain issues identified during the implementation study and discussed with the transition advisory group could not be resolved through implementation guidance, the transition advisory group is referring certain issues to the NERC Standards department, the Standards Committee, and the existing CIP Standards drafting team for evaluation in future standards development. The transition advisory group is currently drafting a document outlining each of these issues for approval by the Standards Committee to provide to the CIP standard drafting team.

ERO Enterprise staff also provide feedback during the Reliability Standards development process. Regional Entities have, since the formation of the ERO, been able to vote and comment on proposed Reliability Standards, providing them a mechanism to influence standards development based on, among other things, data points from their compliance monitoring and enforcement activities. Further, NERC and Regional Entity staff participate in standard drafting team meetings and can use those venues to raise lessons learned from the CMEP. For example, compliance staff will continue to provide feedback into the development of the modifications to the CIP Standards referenced above during the standards process. The feedback will provide

¹⁴ Commission staff attended certain in-person meetings and conference calls of the transition advisory group.

information to the standards drafting team regarding risks seen in the field, particularly as it relates to the guidance documents referenced above. ERO Enterprise CMEP staff will be able to provide information on how current Standards address existing risks, as well as information regarding the impact of the guidance documents, to the drafting team.

Regional Entities have historically provided this type of in-development input from the perspective of individual Regional Entities. This opportunity is being enhanced in 2016 as the ERO Enterprise CMEP staff has set up mechanisms, through existing working groups, to provide an ERO Enterprise CMEP staff perspective to the drafting teams. Lastly, NERC and Regional Entity compliance staff draft and comment on RSAWs for each new or modified standard being developed, which provides another opportunity to identify CMEP-related issues.

As noted above, the CMEP and Reliability Standards development feedback loops are part of a larger communication framework at the ERO Enterprise. There are many other inputs into the Reliability Standards development process from other ERO Enterprise program areas. For instance, to identify any reliability issues not adequately addressed by NERC's existing Reliability Standards, the ERO Enterprise, through NERC's Reliability Risk Management department, performs an assessment of all Category 3 and above events to determine whether the Reliability Standards can be improved to help prevent similar events from occurring in the future. If the assessment indicates standard development is necessary, NERC will work through the proper procedures to initiate a project.

B. Analysis of BPS Events

As noted above, in the February 19 Order, the Commission also focused on the relationship between the CMEP and events analysis. The Commission stated, "NERC has previously stated that '[t]he anatomy of major disturbances, such as the August 2003 Blackout, reveals it is often a

combination of relatively lesser mistakes and problems occurring simultaneously that precipitate a major disturbance.”¹⁵ The February 19 Order directed NERC to “address how [risk-based CMEP] enables NERC to focus attention on such events as indicators of this type of reliability risk and identify resulting actions taken to identify and mitigate the types of minor mistakes or problems known to be causal of major events.”¹⁶

One of the benefits of the risk-based CMEP is an enhanced ability for the ERO Enterprise to work with registered entities to identify and mitigate minimal risk noncompliance before potential escalation into a major event. To help identify such areas of focus for the CMEP, the ERO Enterprise compliance and enforcement staff look at data resulting from events analysis. Under NERC’s [Cause Code Assignment Process](#) (“CCAP”), the analysis of BPS events involves a systematic process to assign cause codes after an event based on the principle that many events can be avoided proactively by understanding the reasons mistakes occur and the active application of remedies and strategies to prevent them. A thorough event analysis is necessary to determine the cause sequence leading to a larger event and to recommend corrective actions, including active defenses, to prevent reoccurrence. The CCAP involves a three-step analysis by the event investigator: (1) investigation and analysis; (2) event analysis report; and (3) cause coding for trending and expanded analysis.¹⁷

¹⁵ February 19 Order at P 50.

¹⁶ *Id.*

¹⁷ The NERC Cause Code Assignment Process is available at http://www.nerc.com/pa/rrm/ea/EA%20Program%20Document%20Library/CCAP_Manual_rev201503__Final_for_posting.pdf. In 2015, NERC conducted an analysis of nearly 100 serious risk, non-CIP compliance violations using the CCAP (not for an event, but for the understanding of how the entity became noncompliant with the Reliability Standard). By using the CCAP, NERC identified five major trends in the causes of serious risk violations: (1) Management or Organization, (2) Individual Human Performance, (3) Equipment or Material Problems, (4) Communication, and (5) Training Deficiency. This analysis allows NERC to focus attention on such causes as indicators of this type of reliability risk and identify resulting actions taken to identify and mitigate the types of minor mistakes or problems known to be causal of major events.

As it relates to the risk-based CMEP, ERO Enterprise compliance and enforcement staff evaluate the results of the CCAP to help inform the scope of CMEP activities. If, for instance, the CCAP identifies a seemingly minimal risk issue as having the potential to have severe consequences if left unaddressed, the ERO Enterprise can appropriately focus their compliance monitoring resources on those issues by including it in the CMEP Implementation Plan. Further, if the risk is specific to a particular Regional Entity footprint, the Regional Entity can use the events analysis data in developing its Regional Risk Assessment (“RRA”). An RRA, which is based on an identification and analysis of trends within a specific Regional Entity footprint and a determination of how best to mitigate potential risks, informs the scope of compliance monitoring activities for that Regional Entity.

NERC also assesses all Category 3 and above events, as mentioned above. Following an event, the applicable registered entities and Regional Entities coordinate to capture all relevant data. The impacted entity(ies) then submits a draft Event Analysis Report to NERC that addresses the sequence of events as they happened, the identified causal factors, and the appropriate corrective actions. Next, selected technical groups and NERC staff review the drafts for completeness and appropriateness prior to publication to the industry. Lessons learned could include the adoption of operating procedures, the identification of generic equipment problems, or even the need for enhanced personnel training.

Further, NERC performs a gap analysis of all Category 3 and above events to identify gaps in Reliability Standards and compliance monitoring within 90 days of receipt of the impacted entity’s Event Analysis report and compliance self-assessment. Based on the lessons learned from the events analysis process, the Implementation Plan may be adjusted to account for those lessons learned and focus on any newly identified risks. In 2016, NERC will expand this gap analysis by

sampling five additional lower-level events that occurred between 2014 and 2016, and develop a program that will explore potential gaps in NERC’s Reliability Standards and compliance monitoring activities. The purpose of this activity is to expand the current program to include more events, thus providing a feedback mechanism to assure compliance and standards are addressing the risks to reliability.

IV. INTERNAL CONTROLS EVALUATION

In the February 19 Order, the Commission also directed that the annual report “address whether a baseline audit is needed to properly evaluate a registered entity’s internal controls” when performing an ICE.¹⁸ The Commission stated that it was unclear “whether the review of internal controls under [the] ICE [process] is based only on a review of program documents, or whether the review also examines the effectiveness of the program, i.e., a baseline evaluation of actual compliance performance under the entity’s internal controls.”¹⁹ Lastly, the Commission noted, “a process that reviews both program documentation and the actual effectiveness of a program may be appropriate to ensure adequate compliance with the risk-based oversight under RAI.”²⁰

NERC and the Regional Entities agree that in evaluating a registered entity’s internal controls under the ICE process, it is important to review both program design as well as the actual effectiveness of that program. Fundamentally, a review of internal controls under the ICE process consists of two primary elements:

- An evaluation of the design of a registered entity’s compliance program (i.e., an evaluation of governance practices, policies, and procedures); and

¹⁸ February 19 Order at P 51.

¹⁹ *Id.*

²⁰ *Id.*

- An analysis of the implementation and effectiveness of an entity's internal controls (i.e., an evaluation of how well the registered entity self-monitors compliance by proactively identifying potential violations, assesses the risks posed by those potential violations, and takes corrective actions to prevent re-occurrence.)

As discussed below, however, requiring a baseline audit in addition to, or separate from, the other compliance monitoring activities the Regional Entities already perform is unnecessary to accomplish the objectives of the ICE process.

The goal of the ICE process is to evaluate whether an entity's internal controls provide reasonable assurance of compliance with mandatory NERC Reliability Standards. The outcome of that evaluation helps to determine the appropriate depth of testing necessary during compliance monitoring activities. While reviewing program documentation is one step in the evaluation, Regional Entities do not rely solely on program documentation. Determining whether the registered entity has implemented the program and the controls are effective is essential to obtaining reasonable assurance of compliance.

As noted above, to start the ICE process, Regional Entities may request internal compliance program documentation and information about program design. The Regional Entity will evaluate the entity's governance practices and its compliance program policies and procedures to determine whether the construct of the program will prevent, detect, or correct actions that could pose a risk for noncompliance. The Regional Entity will also test the implementation and efficacy of the entity's program by looking at compliance with particular Reliability Standards, along with how well the registered entity prevents potential noncompliance, identifies potential noncompliance, and takes corrective actions to mitigate any potential risk and modify compliance processes or controls to prevent future occurrences of noncompliance. When conducting an ICE, Regional

Entities may use information from past work with the registered entity, such as past audits, mitigation plans, and previous internal compliance program reviews, or from doing an assessment of internal controls outside of the regular compliance monitoring activities, or a combination of the two.²¹

In performing ICEs during 2015, Regional Entities reviewed the effectiveness of specific internal controls in the following circumstances: (1) testing internal controls during compliance monitoring activities; (2) conducting periodic assessment of internal controls outside of compliance monitoring activity; and (3) working with entities on enforcement and mitigation matters.

For example, in performing an ICE of an entity, Texas Reliability Entity, Inc. (“Texas RE”) tested, among other things, the controls surrounding Reliability Standard EOP-005-2, Requirements R1 and R4 related to system restoration from Blackstart Resources. After reviewing the entity’s documented processes and practices, Texas RE sought to verify the registered entity’s implementation of those processes and practices. Texas RE confirmed that the registered entity implemented the documented controls, including:

- Actively tracking deadlines for Reliability Coordinator approval with planned communication milestones on restoration plan approval status;
- Conducting project meetings focused on determining if the restoration plan needs changes;

²¹ GAO-12-331G Government Auditing Standards, Chapter 6, Section 6.18, Internal Controls (December 2011): “Auditors may obtain an understanding of internal control through inquiries, observations, inspection of documents and records, review of other auditors’ reports, or direct tests. The nature and extent of procedures auditors perform to obtain an understanding of internal control may vary among audits based on audit objectives, audit risk, known or potential internal control deficiencies, and the auditors’ knowledge about internal control gained in prior audits.”

- Maintaining a project manager checklist that includes questioning restoration plan revisions in project (with subsequent notification efforts regarding noted changes in the project);
- Participation in the Regional Entity working group focused on collaboration and coordination of restoration plans;
- Using a document repository for restoration plan revision(s) and communications;
- Implementing procedural steps for updating and notification efforts if an unplanned change occurs; and
- Implementing a requirement for a compliance executive to approve any restoration plan revisions.

Texas RE rated the documented controls as “Largely Implemented” because the registered entity took sufficient action to demonstrate process and internal control implementation, which provided reasonable assurance of compliance with the requirements. As a result of the focused internal controls evaluation, Texas RE modified the scope of its audit of the entity.

Whether a Regional Entity performed an assessment of internal controls outside of compliance monitoring activities or used compliance monitoring and enforcement activities to measure the effectiveness of an internal compliance program, the outcome was the same: the Regional Entity obtained an understanding of the internal controls used by the registered entity and the effectiveness of those controls. Regional Entities should have the flexibility to use whatever processes to perform an ICE that best accomplish the goals of the ICE process efficiently and effectively, whether that is conducting a new, separate assessment or relying on compliance monitoring activities.

Importantly, the ICE program is a work in progress for the ERO Enterprise. Currently the ICE program is voluntary and, if a registered entity chooses to participate, the results factor into the development of the registered entity's compliance oversight plan. Specifically, the results of the internal controls assessment provide the Regional Entity with a level of confidence regarding the registered entity's ability to achieve and maintain compliance with Reliability Standards. Regional Entities will use this information to determine the depth of testing that is necessary for each Reliability Standard or requirement to provide a reasonable assurance of compliance, and projection of continued compliance. The ICEs performed in 2015 are in effect a snapshot in time to provide reasonable assurance of compliance. While the ICE program is voluntary, ERO Enterprise compliance monitoring staff will also obtain an understanding of registered entity internal controls that are significant within the context of the compliance monitoring objectives.²² Entities that can demonstrate effective internal controls may derive benefit, specifically in regards to the depth of testing necessary for the Reliability Standards within the scope of its compliance monitoring activity. It is important to note that Reliability Standards vary; some are in and of themselves essentially internal controls, some have internal controls included within the requirements of the standard (e.g., FAC-003), and some require compliance activities for which registered entities can develop internal controls.

V. USE OF LEARNING TOOLS

The Commission stated that the annual report should “address and provide examples of how a Regional Entity assesses and factors into a registered entity's risk assessment and audit scope that entity's use of NERC Alerts, Lessons Learned, Reliability Guidelines, and other NERC

²² GAO-12-331G Government Auditing Standards, Chapter 6, Section 6.16, Internal Controls (December 2011).

learning tools.”²³ The core of the IRA is a consideration of the entity’s assets, the nature of its systems, geography, interconnectivity, functions performed, prior compliance history, and overall culture of compliance. Other information about the registered entity, such as what risk management activities it conducts, the quality of the entity’s compliance program, the effectiveness of its internal controls, and its consideration of learning tools, may mitigate its inherent risks. Regional Entities may gather information on the use of these learning tools through various methods, including interviews with entity staff during on-site visits, informal conversations, and formal questions on this issue in the risk assessment survey. There may be situations where an entity, after review and consideration of a learning tool, determines not to use or apply it, for a variety of valid reliability-based reasons. Therefore, when a Regional Entity considers a registered entity’s use of NERC Alerts, Lessons Learned, Reliability Guidelines and other NERC learning tools in this context, the Regional Entity first seeks to understand whether the registered entity is aware of the learning tools and makes conscious determinations whether the learning tools provide pertinent or applicable information for its specific circumstances.

For example, Western Electricity Coordinating Council (“WECC”) considers the registered entities’ use of Lessons Learned and Reliability Guidelines on a case-by-case basis during the risk assessment and audit processes. Depending on the registered entity, its registered functions, previous events, and the potential applicability of Lessons Learned or other learning tools, WECC audit and risk staff may examine the entity’s use of learning tools. Any consideration of such learning tools is done in the context of the entity’s system design, configuration, and compliance program. In addition, WECC audit staff may consider the use of learning tools in a similar manner. One example is related to Energy Management System (“EMS”) outages. NERC

²³ February 19 Order at P 52.

has issued two advisories on EMS outages that recommend actions involving an entity's loss of partial or full visibility of its systems. Where an entity has had EMS outages, auditors may ask if the entity is aware of the advisories and if so, how the entity improved its processes for managing these outages. Currently, this is an informal process, but WECC anticipates formalizing this as the relevant compliance processes are periodically reviewed and updated.

Consistent with WECC's case-by-case approach, as guidelines and lessons learned are identified, ReliabilityFirst will evaluate whether the entities within its footprint are aware of the information and appropriately disseminating it. After release of the winter preparedness reports in response to the polar vortex, ReliabilityFirst created its own cold weather analysis and then conducted on-site visits to ensure entities were reacting to the information.

Although it is important to understand whether and how an entity uses these learning tools, it is not necessarily a determinative factor in assessing risk and determining a compliance oversight plan. It is additional information for the Regional Entity to include in the overall assessment, and may be a factor to provide the Regional Entity confidence that the registered entity is managing its inherent risks.

VI. NERC OVERSIGHT

The Commission's February 19 Order directed NERC to "address and provide an update on NERC's oversight of the RAI Program."²⁴

Throughout 2015, NERC began to transition its own oversight to align with a risk-based environment. This included engaging frequently with Regional Entities and developing an IRA analysis team, in addition to collecting and reviewing IRA and ICE summary reports, as discussed

²⁴ February 19 Order at P 52.

below. Compliance monitoring oversight activities also included observing Regional Entity audits of registered entities and analyzing post-audit feedback.

Through these oversight activities, NERC confirmed that the Regional Entities made significant progress in developing processes and tools to implement risk-based compliance activities. By mid-year, all eight Regional Entities were generally in line with the IRA and ICE alignment criteria reviewed during the Phase 1 assessment activities referenced below. NERC staff also found that Regional Entity audits of registered entities were focused on high-risk areas and tailored to include Reliability Standards that specifically address the entity's characteristics. NERC staff did not identify any concerns relating to any Regional Entity evaluation of a registered entity's compliance with the NERC Reliability Standards. Further, NERC staff's review of registered entity post-audit feedback surveys indicated that most audits had a clear focus of monitoring efforts on reliability risk. As risk-based compliance monitoring continues to mature, specifically in the selection of tools and frequency of monitoring activities within compliance oversight plans, NERC will continue to transition oversight activities. At full maturity, NERC activities will oversee process as well as results—specifically whether compliance monitoring plans for individual entities address necessary risks.

NERC's oversight of Regional Entity enforcement processes found that the Regional Entities appropriately used streamlined enforcement disposition methods. NERC and FERC staff jointly reviewed the Find, Fix, Track, and Report ("FFT") program in 2015 and found no instance of inappropriate FFT treatment for noncompliance. The 2016 joint review, by NERC and FERC staff, of FFTs and Compliance Exceptions is underway. In addition, NERC found that minimal risk noncompliance categorized as Compliance Exceptions received consistent and appropriate treatment.

The following sections describe NERC's compliance monitoring and enforcement oversight activities and findings in more detail.

A. Oversight of Compliance Monitoring Activities

1. Phase I Assessment

NERC's May 20, 2015 compliance filing described the Phase 1 assessment and the associated first quarter activities that were completed. In the November 4 Order, the Commission directed "NERC to provide the results of that assessment, as well as future assessments, in its annual reports."²⁵ At the June 2015 conclusion of the Phase 1 oversight activities, NERC completed a Phase One NERC Oversight Closeout Report ("Closeout Report"), attached as Appendix B. The Closeout Report provides a summary of Phase 1 oversight activities, initial implementation accomplishments, current alignment efforts, and ERO Enterprise improvement recommendations, in addition to next steps and phase two NERC oversight.

2. Other Oversight Activities

In 2015, NERC began collecting summary reports of IRA results to monitor Regional Entity progress toward completing IRAs for registered entities, to gather data on risks being identified and associated NERC Reliability Standards and requirements monitored, and to understand how significant BPS reliability risks are being monitored. On a periodic basis, NERC samples IRA summary reports and requests supporting documentation of IRA activities. The purpose of sampling and reviewing supporting IRA documentation is to gain further understanding, on an ERO Enterprise-wide basis, of Regional Entity processes and procedures being used to complete implementation of risk-based compliance monitoring. Through this

²⁵ November 4 Order at P 21.

activity, NERC can monitor progress and identify other opportunities for improved program consistency.

With 2015 being an implementation year, NERC's primary focus of this monitoring activity was on establishing a repeatable process for collection of IRA summary reports, creating mechanisms to maintain and track information contained within IRA summary reports, and identifying registered entities involved in initial IRAs. As the compliance monitoring program evolves in 2016, NERC staff will gather and analyze data to further assess how significant BPS reliability risks are being monitored across the ERO Enterprise.

NERC also samples a selection of ICE results and requests supporting documentation of ICE activities. The purpose of sampling and reviewing supporting ICE documentation is to enhance understanding of, on an ERO Enterprise-wide basis, Regional Entity processes and procedures being used to complete implementation of risk-based compliance monitoring. This monitoring activity allows NERC to identify opportunities for program consistency and improvement.

In addition, NERC samples a selection of Regional Entity audits of registered entities to observe and review. Through audit observations, NERC monitors both the audit process, including audit-scoping determinations, and assesses the Regional Entities' evaluations of registered entity compliance with NERC Reliability Standards. Audit observations also help NERC to assess the implementation of significant ERO Enterprise activities, such as risk-based compliance monitoring, CIP Version 5 transition, physical security implementation, and the Coordinated Oversight Program of multi-region registered entities ("MRREs"), and to identify program development needs, training, and outreach.

In 2015, NERC observed seven audits, including both CIP and Operations and Planning, and some involving registered entities within the Coordinated Oversight Program for MRREs. NERC staff identified positive observations, as well as lessons learned and opportunities for consistency and overall improvements.

For example, NERC staff noted that Regional Entity staff continues to provide registered entities updates on the audit status to keep the entity informed and hold open and timely discussions around possible areas of noncompliance. Registered entities also confirmed that their audits were focused on high-risk areas and tailored specifically to their entity characteristics. Opportunities for improvement involve the Coordinated Oversight Program for consistent and efficient processes are occurring, and continued improvements for identification, documentation, and incorporation of new or refined risk areas into the entity's IRA and overall compliance monitoring activities. For instance, NERC and the Regional Entities recognize that events or other triggers, including CMEP activities, may identify additional information that can help refine or affect IRAs. Incorporation of this information is an important component of understanding and properly assessing the entity's impact on the BPS in order to tailor and determine appropriate monitoring activities.

NERC's ultimate goal in connection with the oversight of compliance monitoring activities is to focus its oversight on the review of customized Compliance Oversight Plans ("COP") tailored to each registered entity's risks. As processes mature, the ERO Enterprise will continue to develop appropriate COPs through identification of the entity's specific areas of risk and its effective risk mitigation activities. Based on the identified risks and other relevant factors, the COP will identify Reliability Standards and requirements to be monitored, identify the monitoring tools that will be used, and detail monitoring frequency.

Further, following every audit, Regional Entities provide registered entities post-audit feedback surveys to complete and return to both NERC and the respective Regional Entity. Since transitioning to risk-based compliance monitoring, the feedback survey now includes questions relating to all steps within the risk-based compliance monitoring framework leading up to the actual audit. NERC collects and reviews the surveys to help consider industry stakeholder perception, as well as understanding of risk-based compliance monitoring activities. Post-audit feedback surveys also provide a feedback loop back to NERC and the Regional Entities by identifying successes and opportunities of program development, and education and training opportunities for ERO Enterprise staff.

In 2015, NERC and the Regional Entities collected 70 post-audit feedback surveys, which represents a 35% response rate of the total number of 2015 audits. Overall, survey respondents indicated a continued support by registered entities for the risk-based compliance monitoring approach, noting most audits had a clear focus of monitoring efforts on reliability risk.

NERC's ultimate goal in connection with the oversight of compliance monitoring activities is to focus its oversight on the review of customized Compliance Oversight Plans ("COP") tailored to each registered entity's risks. As processes mature, the ERO Enterprise will continue to develop appropriate COPs through risk identification activities, including IRAs, the Risk Elements Guide, among others, in addition to identifying effective risk mitigation activities. Based on the identified risks and other relevant factors, the COP will map to Reliability Standards and requirements, identify the monitoring tools that will be used, and detail monitoring frequency.

B. Oversight of Enforcement Activities

NERC engages in regular oversight of Regional Entity enforcement activities to evaluate the appropriateness of disposition methods, including assessment of a penalty or sanction,

particularly in comparison with previous resolutions of similar noncompliance involving like circumstances. The NERC Board of Trustees Compliance Committee considers the recommendations of NERC staff regarding approval of Full Notices of Penalty and monitors the handling of noncompliance through the streamlined disposition methods of Spreadsheet Notice of Penalties, FFTs, and Compliance Exceptions.

In 2015, NERC conducted a joint review with FERC staff of Regional Entities' use of the FFT program. The review indicated that the program remains successful. While there are opportunities for further streamlining in the areas of mitigation documentation and verification, the review indicated that the ERO Enterprise continues to implement the program appropriately. The full results of the review are available in the [Annual Report on the FFT Program](#). The information collection for a joint NERC-FERC staff review of the FFT and Compliance Exception programs is underway.

1. Self-Logging

In the November 4 Order, the Commission directed NERC to:

[P]rovide in its annual reports an analysis of self-logging data provided by each Regional Entity to measure the quality and consistency of self-logging across regions. This analysis should include information quantifying the number of applicants and successful applicants to receive self-logging authority, and information on the quality and disposition of self-logs, including whether they included all elements required by NERC's self-logging program.²⁶

NERC will conduct a review of the self-logging program in 2016 to encompass 2015 activities to ensure they align with the self-logging program document, including the self-logging assessment methodology developed by the ERO Enterprise and approved by FERC in the November 4 Order. NERC will coordinate closely with FERC staff during this review.

²⁶ November 4 Order at P 22.

There are currently 42 registered entities self-logging throughout the ERO Enterprise. Since FERC approval, in late 2015, of the self-logging assessment methodology, NERC expects greater interest in the program. The 2016 program review will address the areas required in the November 4 Order. NERC also expects to consider whether there are any barriers to increased levels of participation in the program. NERC understands that the self-logging program may not offer a significant efficiency gain for all entities. For example, entities with very few identified instances of noncompliance may find it is just as efficient to self-report the noncompliance without undergoing the required process to obtain approval to self-log. Nevertheless, NERC will seek to understand whether any other factors are affecting the growth of the program. Such considerations will be included in the analysis of self-logging across Regions to be conducted as part of the 2016 program review.

VII. METRICS

In the February 19 Order, the Commission directed NERC to provide details in a compliance filing on “how it intends to measure the success of the risk-based approach to compliance monitoring and enforcement, to include the types of data-driven metrics it will track as the RAI program develops.”²⁷ The Commission also directed that “the annual report should address and provide an update on the metrics that NERC has or will employ to measure the effectiveness of the [risk-based CMEP].”²⁸ In the November 4 Order, the Commission conditionally accepted NERC’s preliminary success factors and related metrics to measure the success of initial implementation of the risk-based CMEP during 2015, subject to NERC providing revised success factors and metrics in its annual report.²⁹

²⁷ February 19 Order at P 32.

²⁸ February 19 Order at P 52.

²⁹ November 4 Order at PP 32-34.

The ERO Enterprise continues to refine the metrics it uses to measure the success of the risk-based CMEP going forward.³⁰ The attached Annual Report discusses the preliminary success factors and metrics used to measure success of the risk-based CMEP during its initial implementation in 2015. As discussed therein, a review of the ERO Enterprise's CMEP implementation in relation to the preliminary success factors and metrics indicates that it was a successful year for the CMEP and the transition to a robust, risk-based approach to compliance monitoring and enforcement.

The metrics described below are designed to enable NERC and the Commission to properly evaluate the success of the risk-based CMEP and identify whether there are areas for improvement. Conceptually, the metrics divide into two categories: (1) those used to measure the effect of the risk-based CMEP on the reliability of the BPS; and (2) those used to measure the ERO Enterprise's implementation of the risk-based CMEP. As the ERO Enterprise continues to implement the risk-based CMEP in 2016 and beyond, it may develop additional metrics to enhance its understanding of the effectiveness of the program and its impact on reliability.

It is important to recognize that the CMEP metrics represent only one component of the metrics that the ERO Enterprise evaluates to determine the overall success of the ERO Enterprise and its effect on BPS reliability. Among other things, the ERO Enterprise tracks the frequency and severity of events on the BPS, analyzes the comprehensiveness of its Reliability Standards following any Category 3 or above events, and measures the mitigation of identified risks.³¹ As the implementation of risk-based CMEP matures, an array of metrics will communicate whether the ERO Enterprise is operating from a process framework to ensure non-discriminatory practices,

³⁰ NERC staff held a brief, initial meeting with Commission staff on January 13, 2016. Additional meetings are being scheduled and NERC staff will continue to consult with Commission staff on enhancing the CMEP metrics.

³¹ The 2016 ERO Enterprise and Corporate Metrics are available at <http://www.nerc.com/gov/Pages/default.aspx>.

whether compliance monitoring plans are addressing the appropriate risks for each registered entity, and whether reliability of the BPS is improving.

A. Effect of Risk-Based CMEP on Reliability

As previously discussed, a primary benefit of the risk-based CMEP is to create a compliance and enforcement program that properly focuses ERO Enterprise and industry resources to higher risk issues that matter more to reliability. The end goal is to create an oversight program that ultimately improves the reliability of the BPS by identifying, prioritizing, and addressing risks to the BPS to enable the ERO Enterprise and industry to allocate resources where they are most needed and likely to be the most effective in preventing and mitigating events on the BPS. To help measure the success of the risk-based CMEP in accomplishing that objective, the ERO Enterprise is tracking the following items:

- The number of new violations;
- The risk of those violations to the reliability of the BPS;
- The timeliness of mitigation of those violations; and
- The percentage of violations that are self-identified.³²

By tracking these issues over time, the ERO Enterprise is developing a better understanding of whether the risk-based CMEP is having its intended effect. For instance, a trend towards fewer violations with lower risk to the BPS that are timely mitigated and self-identified suggests that the move to a risk-based CMEP is succeeding in identifying and addressing higher risk issues, properly focusing ERO Enterprise and industry resources on identifying and correcting instances of non-compliance, and, in turn, improving the reliability of the BPS. In contrast, if there is an increase

³² The most recent data for these four items was presented to the NERC Board of Trustees Compliance Committee at its February 10, 2016 meeting. The presentation is available at http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/CC_Open_Presentations_Feb_2016.pdf.

in violations that present severe risk to the BPS and entities are neither timely mitigating nor self-identifying these violations, it is an indication that the risk-based CMEP is not having its intended effect and needs improvement.

Importantly, in any given year, there may be factors unrelated to the implementation of the risk-based CMEP that may sway these numbers to one side or another. As such, evaluation of the success of the risk-based CMEP on reliability may not be apparent in any one-, two-, or even three-year period. The ERO Enterprise and the Commission should have a long view in measuring the success of the risk-based CMEP. As the ERO Enterprise tracks these metrics over time, it will evaluate, in consultation with Commission staff, ways to assess the causal relationship between the various processes and procedures in the CMEP and improved reliability of the BPS.

B. Implementation of Risk-Based CMEP

To determine the success of the risk-based CMEP, it is also important to collect and analyze data on the implementation of the various risk-based processes and procedures. Such data enables the ERO Enterprise to understand how the various processes and procedures are being used, identify areas for improvement, understand trends, develop lessons learned, and begin to correlate the implementation of the risk-based CMEP with improvement to reliability, as measured by the four metrics tracked above. The following is a discussion of the metrics the ERO Enterprise will use to track the implementation of the CMEP, both the compliance monitoring components and the enforcement components.

To measure the ERO Enterprise's progress in implementing the compliance monitoring components of the risk-based CMEP, the ERO Enterprise has tracked the following on an annual and quarterly basis:

- The total number of IRAs conducted;³³
- The total number of IRAs conducted for registered entities on the audit schedule for a particular year compared to the total number of registered entities on the audit schedule;
- The total number of IRAs conducted for registered entities not on the audit schedule;
- The total number of ICEs conducted as compared to the total number of registered entities that have requested an ICE;
- The total number of ICEs conducted for registered entities on the audit schedule for a particular year compared to the total number of registered entities on the audit schedule;
- and
- The total number of ICEs conducted for registered entities not on the audit schedule.

In 2016, the ERO Enterprise will also track those Reliability Standards (and requirements therein) that are the focus of compliance monitoring activities from year to year to analyze: (1) the manner in which the ERO Enterprise is identifying and evaluating BPS risks over time; and (2) the industry response to those areas of focus.

To measure the ERO Enterprise's progress in implementing the enforcement components of the risk-based CMEP, the ERO Enterprise has tracked the following on an annual and/or quarterly basis:

- The number of serious risk violations;
- The most commonly violated Reliability Standards, focusing on those associated with serious risk violations;

³³ During 2016, the goal is to complete IRAs for all Reliability Coordinators, Balancing Authorities, and Transmission Operators.

- The number of instances of noncompliance discovered internally by the registered entity versus externally by the ERO Enterprise;³⁴
- The average age of noncompliance (i.e., the age of a violation from discovery to closure);³⁵
- The timeliness of mitigation of instances of noncompliance;
- Registered entities that are self-logging, including total number of registered entities self-logging by Regional Entity and by reliability function;
- Use of Compliance Exceptions for minimal risk issues, including the percentage of minimal risk issues processed under each disposition method by Regional Entities. This includes a review of trends in Compliance Exceptions.
- The percentage of Notices of Penalty approved by the Commission; and
- The number of older violations in a Regional Entity's inventory.

Tracking the metrics outlined above will help measure the ERO Enterprise's success in rolling out the new processes and procedures (e.g., number of IRAs, use of Compliance Exceptions), whether registered entities are using risk-based tools (e.g., requesting an ICE, use of Self-Logging), and whether the registered entities are focusing resources appropriately (e.g., increase in self-identification of noncompliance, increased timeliness of mitigation, and decrease in serious risk violations).

As the ERO Enterprise continues to implement the risk-based CMEP, it may develop additional metrics to help determine the effectiveness of risk-based CMEP implementation.

³⁴ The target for self-identification of noncompliance in 2016 is 75%.

³⁵ The target is for the average age of noncompliance in the ERO Enterprise's inventory not to exceed 12 months.

VIII. CONCLUSION

NERC respectfully requests that the Commission accept this filing as compliant with the Commission's February 19 Order and November 4 Order issued in Docket No. RR15-2-000.

Respectfully submitted,

/s/

Sonia C. Mendonca
Vice President of Enforcement and Deputy
General Counsel
Shamai Elstein, Senior Counsel
Arthur L. Brown, Counsel
North American Electric Reliability
Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net
shamai.elstein@nerc.net
arthur.brown@nerc.net

*Counsel for the North American Electric
Reliability Corporation*

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in Docket No. RR15-2-000.

Dated at Washington, D.C. this 18th day of February, 2016.

Respectfully submitted,

/s/

Arthur L. Brown

*Counsel for the North American Electric
Reliability Corporation*

APPENDIX A

2015 CMEP Annual Report

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2015 ERO Enterprise Compliance Monitoring and Enforcement Program Annual Report

February 10, 2016

RELIABILITY | ACCOUNTABILITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface.....	iv
Executive Summary	1
Key Activities.....	1
Risk-Based Compliance Monitoring and Enforcement Implementation Activities.....	1
Regional Entity Coordination of Multi-Region Registered Entities	2
Regional Consistency Reporting Tool.....	2
Transition to Version 5 of the Critical Infrastructure Protection Standards.....	2
Physical Security Reliability Standard	2
Success Factors and Metrics	3
Risk-based Compliance Monitoring and Enforcement.....	4
Risk-based Compliance Monitoring	4
2015 ERO Enterprise CMEP Implementation Plan	4
Inherent Risk Assessments and Internal Control Evaluations.....	6
Regional Entity Compliance Monitoring	9
Risk-based Enforcement	10
Background	10
ERO Enterprise Core Values and Guiding Principles	10
2015 Enforcement Results	12
Disposition of Noncompliance in 2015.....	13
Compliance Exceptions	13
Find, Fix, Track, and Report (FFT).....	14
Spreadsheet Notice of Penalty (SNOP)	14
Full Notices of Penalty (NOP)	15
Self-Logging Use.....	16
ERO Enterprise CMEP Training, Education, and Outreach	18
ERO Enterprise Staff Training and Education	18
Industry Stakeholder Information and Outreach	19
NERC Oversight of the Regional Entities	23
Risk-based Compliance Monitoring Oversight	23
Oversight of Initial Implementation of Risk-based Compliance Monitoring	23
Registered Entity Audit Observations and Reviews.....	23
IRA Results Summary Collection	24
Review of Registered Entity Post-Audit Feedback Surveys.....	24

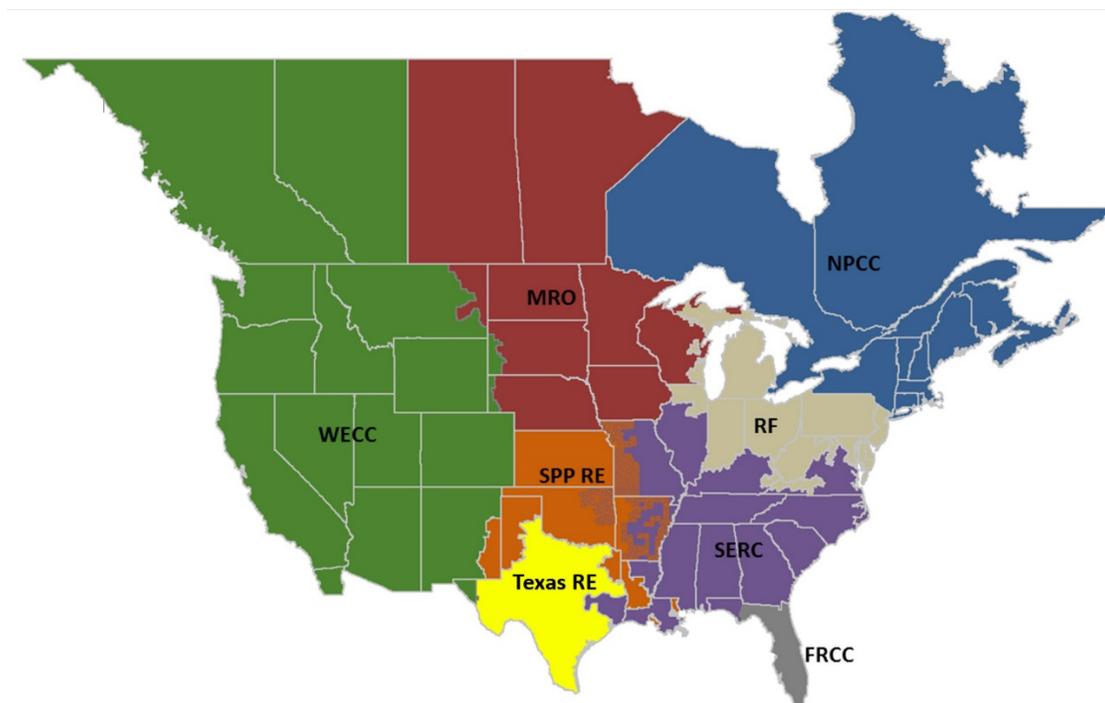
Table of Contents

Risk-based Enforcement Oversight.....	25
Annual Reviews Conducted in 2015.....	25
Other Significant 2015 Activities	26
Managing the Transition to Version 5 of the CIP Standards.....	26
Physical Security Reliability Standard Implementation	28
Regional Entity Coordinated Oversight of Multi-region Registered Entities	29
Regional Consistency Tool	31
Looking Ahead to 2016.....	33
Appendix.....	34
Mitigation Completion Status.....	34
Self-Assessment and Identification of Noncompliance	35
Noncompliance Processing Metrics.....	36
ERO Enterprise’s Pre-2014 Caseload.....	36
Average Age of Noncompliance in the ERO Enterprise by Month.....	38

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC’s area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC’s jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into several assessment areas within the eight Regional Entity boundaries, as shown in the map and corresponding table below.



The regional boundaries in this map are approximate. The highlighted area between SPP RE and SERC denotes overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Executive Summary

This report highlights key ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) activities that occurred in 2015, provides information and statistics regarding those activities, and provides a look forward to the ERO Enterprise's 2016 CMEP priorities.¹ As discussed further below, 2015 was a demanding yet transformative and highly successful year for enhancing the efficiency and effectiveness of the ERO Enterprise's CMEP. Most significantly, after a collaborative, multi-year effort among NERC, the Regional Entities, and industry stakeholders to identify and test risk-based compliance monitoring and enforcement concepts, processes, and programs; the ERO Enterprise successfully commenced implementation of a risk-based CMEP designed to focus ERO Enterprise and industry compliance resources on higher-risk issues that matter more to reliability. The ERO Enterprise also continued its commitment to enhance other features of the CMEP and work with stakeholders to help ensure a successful and effective implementation of new Critical Infrastructure Protection (CIP) Reliability Standards. The following is a brief overview of these activities and the factors and metrics the ERO Enterprise used to measure the success of the CMEP during 2015, which are discussed in greater detail throughout this report.

Key Activities

Risk-Based Compliance Monitoring and Enforcement Implementation Activities

A primary focus of the ERO Enterprise during 2015 was fully implementing the risk-based CMEP. The risk-based CMEP involves the use of an oversight plan framework² focused on identifying, prioritizing, and addressing risks to the BPS to enable the ERO Enterprise to allocate resources where they are most needed and likely to be the most effective. After completing the risk-based CMEP design in early 2015, the ERO began initial implementation activities. Specifically, the ERO Enterprise (1) conducted [Inherent Risk Assessments](#) (IRAs), which is a review of inherent risks posed by an individual registered entity to BPS reliability, (2) performed [Internal Control Evaluations](#) (ICEs) to evaluate whether the registered entity has implemented effective internal controls, and (3) used various methods to process noncompliance based on risk (including the [Self-Logging](#) program and [Compliance Exceptions](#)). In addition, the ERO Enterprise continued to maintain a consolidated Implementation Plan that provides guidance and implementation information common among NERC and the eight Regional Entities, including risks to the BPS (referred to as risk elements) to focus compliance monitoring. Overall, these activities supported compliance monitoring planning, focused the oversight of registered entities, and provided greater efficiency in enforcement activities.

In 2015, the ERO Enterprise made a significant shift in how it conducts compliance monitoring activities. Previously, audit schedules primarily drove interactions with registered entities without emphasis on risk to reliability. In addition, the scope of compliance monitoring activities was driven by a relatively static list of Reliability Standards on the Actively Monitored List. The ERO Enterprise is now using the analysis of risks to drive interactions with registered entities and conduct compliance monitoring activities. Registered entities are not all similarly situated; there are numerous differences in technology, geographical location, voltages, and inter-ties that require a more risk-informed method. Recognizing the unique characteristics of registered entities and using the analysis of risks, Regional Entities tailor the monitoring activities to address the appropriate risks. The ERO Enterprise has also changed the manner in which it engages with certain registered entities. In some cases,

¹ The "ERO Enterprise" refers to the affiliation between NERC and the eight Regional Entities for the purpose of coordinating goals, objectives, metrics, methods, and practices across statutory activities. The operation of the ERO Enterprise does not conflict with obligations of each organization through statutes, regulations, and delegation agreements. The activities discussed in this report relate to compliance monitoring and enforcement performed in connection with United States registered entities. ERO Enterprise activities outside of the United States are not specifically addressed.

² A visual representation of the risk-based framework is available at:
<http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Risk-Based%20Compliance%20Monitoring%20and%20Enforcement%20Program%20Visual%20Overview.pdf>.

registered entities that historically were monitored through an audit are now being monitored through a spot check or even a self-certification because of the focused, tailored scope of risk-based monitoring.

In 2015, enforcement activities throughout the ERO Enterprise reflected the full implementation of the risk-based approach introduced in 2013 through the Reliability Assurance Initiative. The risk-based approach aligns the outcome of any noncompliance to the risk the particular noncompliance posed to the reliability of the BPS. In that sense, the outcome could range from a significant monetary penalty to a streamlined disposition outside of the enforcement process. This approach, and the high usage of streamlined methods described in this report, are predicated on a significant level of cooperation by registered entities. In this context, cooperation is evidenced in part by high levels of self-identification of noncompliance and prompt mitigation of issues. These historical trends regarding self-identification and mitigation continued in 2015, as discussed below. Maintaining trends of high self-identification and prompt mitigation is essential to the effectiveness of the risk-based program.

This report discusses the results achieved in 2015 with a focus on two streamlined programs in particular: Self-Logging and Compliance Exceptions. Included in the Appendix are processing efficiency results, which indicate how these programs have allowed the ERO Enterprise to operate more efficiently.

Regional Entity Coordination of Multi-Region Registered Entities

In June 2015, the ERO Enterprise opened the [Coordinated Oversight Program](#) of multi-region registered entities (MRREs) to all registered entities. This program is intended to make risk assessments, compliance monitoring and enforcement, and event analysis activities more efficient for the registered entities that use, own, or operate assets in areas covering more than one Regional Entity territory. Under the Coordinated Oversight Program for MRREs, Regional Entities coordinate their oversight responsibilities over MRREs by designating one or more Lead Regional Entity (LRE) to each MRRE or group of MRREs. By the end of 2015, 152 entities throughout the ERO Enterprise – by individual NERC Compliance Registry number – were participating in the program.

Regional Consistency Reporting Tool

To improve consistency among the Regional Entities and drive continuous improvement in day-to-day operations, the Regional Entities also developed the [Regional Consistency Reporting Tool](#) as an additional channel of communication for registered entities and relevant industry stakeholders. The tool allows the public to report any perceived inconsistencies among Regional Entities, including perceived inconsistencies with compliance monitoring and enforcement processes, procedures, or rules. In 2015, 20 reports of perceived inconsistencies were submitted through the Regional Consistency Reporting Tool. These 20 reports represent a diverse category of issues involving, among others, compliance monitoring, CMEP tools, event analysis, organization registration, and BES asset identification. The majority of these reports involve substantive issues—with a handful involving administrative issues, such as inconsistent data transmittal methods from registered entities to Regional Entities. Out of these 20 reports, 13 have been successfully investigated and resolved, three have been assigned to ERO staff working groups for longer-term tracking and resolution, and four cases are in-process.

Transition to Version 5 of the Critical Infrastructure Protection Standards

To support registered entities' transition to the CIP Version 5 Reliability Standards, most of which become effective in the United States on April 1, 2016, NERC focused its 2015 efforts on three key areas: written guidance and Reliability Standard Audit Worksheets completion, stakeholder outreach, and ERO Enterprise CMEP staff training. The CIP Version 5 transition program involved significant stakeholder participation and helped address several challenging issues to enable an efficient and effective transition to the CIP Version 5 standards.

Physical Security Reliability Standard

The Physical Security Reliability Standard became effective on October 1, 2015. Throughout 2015, NERC and the Regional Entities focused on implementation readiness. At the start of 2015, NERC released formal guidance on implementation requirements. By the fall of 2015, the ERO Enterprise began engaging with registered entities

through a variety of outreach activities and coordinated site visits to discuss and understand their Physical Security Reliability Standard plans. NERC will continue to monitor compliance with this Reliability Standard with emphasis on assessing and supporting effective implementation.

Success Factors and Metrics

The ERO Enterprise identified the following preliminary factors and related metrics to measure the success of initial implementation of the risk-based CMEP during 2015:

1. *ERO Enterprise Staff Competency*: 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.
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.
3. *Consistency*: The common tools, processes, and templates used by Regional Entities for risk-based compliance activities with registered entities are consistent on matters where consistency is important, and NERC has adequate oversight of that interface.
4. *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.
5. *Preliminary Metrics*: Metrics were identified for key expected results from risk-based compliance and enforcement and benchmarked for 2015.
6. *Recognized Value*: The value of risk-based compliance and enforcement of registered entities is apparent to the public and can be clearly and publicly articulated.

This report identifies, throughout, the activities that were performed in 2015 in support of each of these success factors. This report also addresses how the implementation of the risk-based CMEP compared to the [criteria](#) proposed by the Compliance and Certification Committee (CCC) for evaluating Regional Entity CMEP effectiveness (referred to as the CCC Criteria).³

As discussed below, while 2015 presented a number of challenges for the ERO Enterprise, a review of the ERO Enterprise's CMEP implementation in relation to these factors and metrics indicates that it was a successful year for the CMEP and the transition to a robust, risk-based approach to compliance monitoring and enforcement. This report also describes lessons learned during 2015 for all CMEP activities and, based on those lessons learned, highlights the ERO Enterprise's CMEP priorities for 2016 and expectations. Additional metrics are being developed to continue assessing the ERO Enterprise's CMEP activities in 2016.

³ The CCC is a NERC Board-appointed stakeholder committee serving and reporting directly to the NERC Board of Trustees. In accordance with Section 402.1.2 of the NERC Rules of Procedure, the CCC is responsible for establishing criteria for NERC to use to evaluate annually the goals, tools, and procedures of each Regional Entity Compliance Monitoring and Enforcement Program to determine the effectiveness of each such program.

Risk-based Compliance Monitoring and Enforcement

Throughout 2015, the ERO Enterprise made significant progress in its evolution to a robust risk-based CMEP. Some highlights and accomplishments of the evolution to risk-based compliance monitoring and enforcement include the following: completing the design of the risk-based CMEP in early 2015, conducting IRAs of registered entities, performing ICEs, and using risk based methods to process noncompliance. These activities helped to support compliance monitoring planning, focus oversight for registered entities, and provide greater efficiency in enforcement activities.

Risk-based Compliance Monitoring

In 2015, the ERO Enterprise made a significant shift in how it conducts compliance monitoring activities. Previously, audit schedules primarily drove interactions with registered entities without emphasis on risk to reliability. In addition, the scope of compliance monitoring activities was driven by a relatively static list of Reliability Standards on the Actively Monitored List. The ERO Enterprise is now using the analysis of risks to drive interactions with registered entities and conduct compliance monitoring activities. Registered entities are not all similarly situated; there are numerous differences in technology, geographical location, voltages, and inter-ties that require a more risk-informed method. Recognizing the unique characteristics of registered entities and using the analysis of risks, Regional Entities tailor the monitoring activities to address the appropriate risks. The ERO Enterprise has also changed the manner in which it engages with certain registered entities. In some cases, registered entities that historically were monitored through an audit are now being monitored through a spot check or even a self-certification because of the focused, tailored scope of risk-based monitoring.

Risk-based compliance monitoring involves three main activities: the identification of BPS risk elements and associated areas of focus in the ERO Enterprise CMEP Implementation Plan, the assessment of a registered entity's inherent risk through an IRA, and the determination of the appropriate scope, frequency, and tools to use for specific compliance monitoring of each registered entity. In support of success factor 4 (on balanced transparency), the ERO Enterprise publicly posted information on how the ERO Enterprise carries out these activities in the 2015 ERO Enterprise Implementation Plan, the IRA and ICE Guides, and documents associated with Regional Entities' risk-based CMEP processes.⁴ The following is an overview of risk-based compliance monitoring activities and the ERO Enterprise's implementation progress during 2015.

2015 ERO Enterprise CMEP Implementation Plan

The first step of the risk-based framework is identification and prioritization of continent-wide risks, which results in an annual compilation of risk elements applicable across the ERO Enterprise. Through the identification of risk elements, NERC, with input from the Regional Entities, maps a preliminary list of applicable NERC Reliability Standards and responsible registration functional categories to the risk elements, known as areas of focus. The areas of focus represent an initial list of NERC Reliability Standards on which the ERO Enterprise focuses compliance monitoring efforts.

Next, Regional Entities further consider local risks when developing region-specific risk elements. These risk elements are included in the Implementation Plan as region-specific appendices. When developing the region-specific risk elements, Regional Entities consider the CCC Criteria on risk elements.⁵ In developing risk elements

⁴ The 2015 ERO Enterprise Implementation Plan, IRA Guide, and ICE Guide are available at <http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx>.

⁵ CCC Criteria on Risk Elements: The Regional Entity takes into account Regional BES Risks. The Regional Entity has defined and accounted for Regional BES risks in its CMEP Implementation Plan. (1) The Regional Entity used a documented process and provided a justified basis for addition, deletion, or modification of NERC Risk Elements and Standards in Focus. (2) Identify the criteria (including, but not limited to information sources) the Regional Entity used to add/subtract from NERC's Risk Elements and Standards in Focus for developing its Regional Implementation Plan. (3) The Regional Entity has provided a rationale for the removal of a NERC risk element identified by NERC in the NERC CMEP IP as not applicable to their Region.

during 2015, Regional Entities performed a Regional Risk Assessment, identifying risks specific to the region that could potentially impact the reliability of the BPS. As part of this assessment, Regional Entities gathered and reviewed Regional Entity-specific risk reports and operational information (e.g., interconnection points and critical paths, system geography, seasonal/ambient conditions, etc.) and prioritized potential Regional Entity-specific risks. Next, after determining region-specific risks, Regional Entities also identified the related Reliability Standards and requirements associated with those risks. These Reliability Standards and requirements become inputs into a registered entity's IRA, and ultimately the compliance oversight plan, however, these Reliability Standards and requirements are not intended to be a static list that must be examined during all compliance monitoring activities. The Implementation Plan includes further detail on the Regional Entities' risk element development process in the Regional Entity appendices.⁶

Further, in 2015, NERC and the Regional Entities collaborated to create NERC criteria for the development of 2016 Regional Entity Implementation Plans. NERC reviewed and approved the 2016 Regional Entity Implementation Plans for conformance to this established review criteria. Some example criteria considerations include the following: appropriate justification to explain the Regional risk elements and areas of focus for both expansions of ERO Enterprise risk elements and region-specific risk elements; and clarifications around 2016 compliance monitoring activities. The 2016 Regional Entity Implementation Plan reviews were the first time NERC and the Regional Entities considered the review criteria, which incorporates the CCC Criteria on risk element development. Through the review process, NERC and the Regional Entities identified opportunities for criteria improvements going into 2016 and beyond, and the ERO Enterprise will continue to improve and develop the review criteria in support of consistency and content. Ultimately, the Regional Entity Implementation Plans intend to reflect regional operations and provide insight regarding compliance monitoring to registered entities within their footprints; therefore, differences will exist within the Regional Entity Implementation Plans, and the ERO Enterprise does not intend to alleviate such differences.

The ERO Enterprise CMEP Implementation Plan (Implementation Plan) provides the foundation for the risk-based CMEP through its identification of BPS risk elements and areas of focus. The Implementation Plan includes risks to the overall BPS as well as regional risks. The 2015 Implementation Plan marks continued progress in implementing the risk-based CMEP. This Implementation Plan incorporated Regional Entity risk elements in appendices whereas before 2014, NERC and the Regional Entities had separate implementation plans. Previously, compliance monitoring, including audits, was performed in a prescriptive manner through the annual implementation plans. These annual implementation plans also included pre-set frequencies and scopes for compliance monitoring based on a global assessment of risks. The more precise risk-based approach used today is improved because, in addition to the risk elements, it considers more localized and regional risks posed to the broader interconnected system. It also provides greater flexibility in the deployment of resources allowing Regional Entities to engage with registered entities through risk-based, entity-specific compliance monitoring activities that better and more explicitly accommodate the differences in risks resulting from geography, technology, location, and other unique characteristics. Table 1 lists the 2015 continent-wide risk elements.⁷

⁶ The 2015 Regional Entity Implementation Plans are appended to the ERO Implementation Plan, *available at* [http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_2015%20CMEP%20IP_V_1.2%20\(Posted_08172015\).pdf](http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_2015%20CMEP%20IP_V_1.2%20(Posted_08172015).pdf).

⁷ The Risk Elements Guide for Development of the 2015 CMEP IP is available at http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_RiskElementsGuide_090814.pdf.

Table 1: 2015 ERO Enterprise Risk Elements	
Infrastructure Maintenance	Uncoordinated Protection Systems
Protection System Misoperations	Workforce Capability
Monitoring and Situational Awareness	Long Term Planning and System Analysis
Threats to Cyber Systems	Human Error
Extreme Physical Events	

Inherent Risk Assessments and Internal Control Evaluations

Throughout 2015, the ERO Enterprise focused risk-based compliance monitoring implementation on refining the IRA and ICE processes and performing IRAs, and ICEs as requested, for registered entities on the 2015 audit schedule. The ERO Enterprise prioritized performing IRAs for registered entities on the audit schedule to ensure Regional Entities’ most time-intensive engagements incorporated risk-based concepts. During these engagements, the ERO Enterprise also learned from initial implementation to incorporate in processes and further promote consistency in IRAs across the ERO Enterprise.

Regional Entities perform an IRA of a registered entity to identify areas of focus and the level of effort needed to monitor compliance with NERC Reliability Standards for a particular registered entity. The IRA is a review of risks posed by an individual registered entity to the reliability of the BPS. An IRA considers factors such as assets, systems, geography, interconnectivity, functions performed, prior compliance history, and culture of compliance, among other inputs, and is performed on a periodic basis. The frequency of updating an IRA may vary based on occurrence of significant changes to reliability risks or emergence of new reliability risks.

In developing more specific monitoring plans for registered entities in their footprints, the Regional Entities also take into account any information obtained through the ICE process. Registered entities have an opportunity to do the following: provide, on a voluntary basis, information to their respective Regional Entity about their internal controls that address the risks applicable to the entity and for identifying, assessing, and correcting noncompliance with Reliability Standards; and demonstrate the effectiveness of such controls. As a result of the ICE, the Regional Entity may further focus the compliance assurance activities for a given registered entity. For example, the depth of any particular area of review may be modified.⁸ Registered entities may elect not to participate in an ICE. In that case, the Regional Entity would use the results of the IRA to determine the appropriate compliance oversight strategy, including frequency and tools within the scope. Regional Entities will also continue to review internal controls while conducting audits.

Registered entities are expected to maintain compliance with all requirements. The IRA and ICE processes are intended to appropriately scope compliance monitoring activities or engagements in method, range, frequency and depth. These rigorous processes may lead to either reduced or increased time on site. For example, one entity with an IRA and ICE may have 6% of the applicable requirements for its registered functions identified in its audit scope. While another entity with an IRA, but not an ICE, may have an audit scope that includes 42% of applicable requirements. In any event, the Regional Entity Audit Team Lead is authorized and obligated to expand scope if there are indications of further risk.

⁸ For example, if a registered entity demonstrates effective internal controls for a given Reliability Standard during the ICE, the Regional Entity may determine that it does not need to audit the Registered Entity’s compliance with that Reliability Standard as frequently, or may select a different monitoring tool.

The entity-specific IRA is a living document, which results in the longer range compliance oversight plan. It is reviewed after engagements and then used to inform future compliance monitoring efforts, such as targeted self-certifications, spot checks, or data submittals.

Regional Entities completed 230 IRAs for registered entities on the 2015 audit schedule. Of those 230 IRAs, 31 registered entities elected to have an ICE. Regional Entities have completed 101 IRAs and 20 ICEs for registered entities that are not scheduled for an audit in 2015. Ongoing ICE-related activities also continue for registered entities who opt-in for an ICE or who are interested in having an ICE performed. To begin an ICE, Regional Entities may hold initial discussions with registered entities or send internal control questionnaires to registered entities to begin the ICE process.

Table 2 summarizes the overall IRA and ICE activities related to both the annual 2015 audit schedule and overall IRA and ICE activities.

Table 2: Summary of Overall Risk-based Compliance Monitoring Activities	
Risk-based Compliance Activities	Count
IRA	
IRAs Conducted for Registered Entities on 2015 Audit Schedule	230
IRAs Completed for Registered Entities not on 2015 Audit Schedule	101
Total IRAs Completed within the ERO Enterprise	331
IRAs Remain to be Completed for all Registered Entities within the ERO Enterprise	1,122
ICE	
ICEs Conducted for Registered Entities on 2015 Audit Schedule	31
ICEs Completed for Registered Entities not on 2015 Audit Schedule	20
Total ICEs Completed within the ERO Enterprise	51

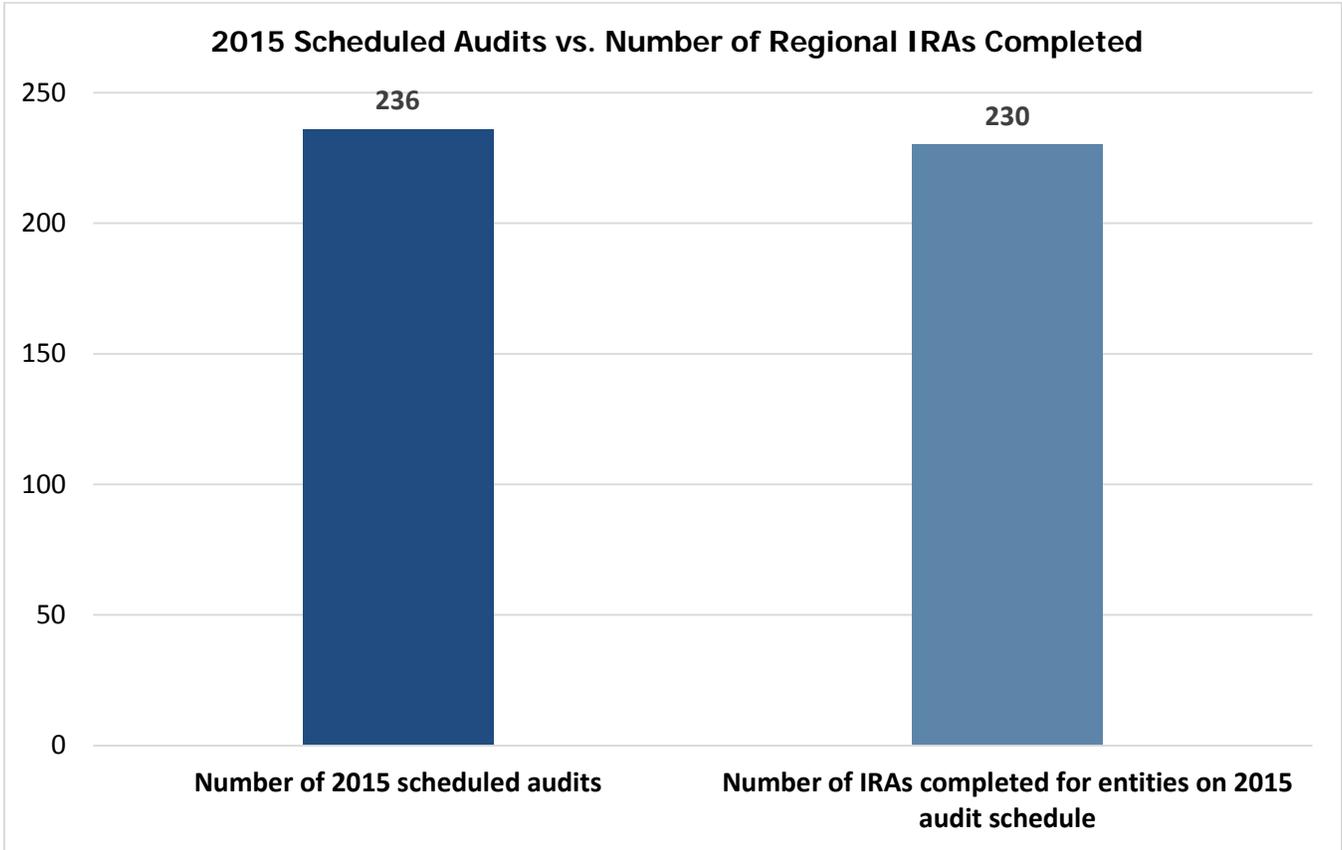


Figure 1: 2015 Scheduled Audits⁹ vs. Number of IRAs Completed¹⁰

The above figure indicates the progress of the ERO Enterprise in support of consistency among the common tools, processes, and templates used by Regional Entities (success factor 3). Regional Entities performed IRAs on 97% of registered entities on the 2015 audit schedule. To support completion of these IRAs, the ERO Enterprise focused on collaboration, sharing of best practices, and incorporating refinements based on lessons learned during the first part of 2015.

⁹ The number of scheduled audits changed from earlier reports in 2015 due to the de-registration of a registered entity on the audit schedule and the rescheduling of some audits for logistical purposes.

¹⁰ WECC performed off-site audit activities for 21 registered entities identified on its annual audit schedule. WECC identified these off-site audits based on the regional risk assessment outlined in its 2015 CMEP Implementation Plan. Scope of the compliance monitoring activities for six out of the 21 registered entities was based on the regional risk assessment and WECC’s regional risk elements and areas of focus. For the remaining 33 audits, WECC performed IRAs or preliminary IRAs for scoping the audit.

In further efforts to promote consistency, the ERO Enterprise incorporated the CCC Criteria on IRAs¹¹ and ICEs¹² into its review of IRA and ICE processes. During NERC's engagements with Regional Entities in Q1 of 2015, NERC and the Regional Entities reviewed the Regional Entities' use of information and risk factors in the IRA process. In addition, NERC and the Regional Entities discussed the Regional Entities' communication of IRA results to registered entities, registered entity feedback and understanding of IRA results, and the timing of the IRA development. Furthermore, NERC and the Regional Entities discussed initial activities involving internal controls and potential impacts these assessments may have on compliance monitoring activities. During these initial oversight engagements, there was very limited, if any, participation in ICE at the Regional Entities. These discussions informed NERC's conclusion that the Regional Entities were conceptually aligned on risk-based concepts. The Risk-based Compliance Monitoring Oversight section of the instant report provides further detail on the NERC and Regional Entity engagements.

For 2016, the ERO Enterprise will shift from schedules driving IRA completion to risk-driving IRA completion. To that end, the ERO Enterprise will focus on completing IRAs for all entities registered as a Reliability Coordinator, Balancing Authority, or Transmission Operator by 2016. This will represent a significant milestone in the implementation of risk-based compliance monitoring. Additionally, the ERO Enterprise will focus on ensuring certain registered entities will have completed compliance oversight plans (COP) that allocate compliance monitoring resources based on risk. Ultimately, the Regional Entity will determine the type and frequency of the compliance monitoring tools (e.g., off-site or onsite audits, spot checks, or self-certifications) that are warranted for a particular registered entity based on reliability risks. Additionally, the Regional Entity may modify the scope of NERC Reliability Standards reviewed as part of a Compliance Audit or pursue compliance assurance through any monitoring considerations. For Compliance Audits, auditors are authorized and obligated to expand scope should there be indications of failed controls or noncompliance of one Reliability Standard that may link to another Reliability Standard.

Regional Entity Compliance Monitoring

For 2015, Regional Entities performed compliance monitoring activities using various methods outlined in the CMEP and according to their 2015 Annual CMEP Implementation Plans. As the ERO Enterprise progresses in the implementation of risk-based CMEP, stakeholders can expect a greater use of other compliance monitoring tools, in addition to audits and spot checks. Additionally, the traditional methods used to conduct compliance monitoring needed to be re-evaluated. For example, in some cases, more detailed and instructive self-certifications could be used instead of more costly audits. These self-certifications, while requiring more review

¹¹ CCC Criteria for IRAs: The RE's Inherent Risk Assessment results in tailored approaches to monitoring compliance for similarly registered functional entities, based on differing profiles and operating characteristics. (For example, does the Regional Entity monitor all Transmission Owners within its footprint the same, or does the use of IRA criteria result in distinct monitoring plans?) (1) The Regional Entity's IRA takes into consideration the relationship of an entity's Information Attributes and Risk Factors, see IRA Program Module, in a manner that tracks regional BES risks. (2) In accordance with the IRA guide, the Regional Entity's IRA process allows for sharing of already available IRA information, discussion with the registered entity in the event of the need to clarify or correct information, and feedback provided to the registered entity so that there is an understanding of the Regional Entity's perception of the registered entity's risk. (3) Through responses to the results of post-audit questionnaires, the registered entity indicates that it understands the results of the IRA. (4) The timing of the IRA allows for adjustment to the Audit scope before sending the 90-day detail letter. (5) What is the sequencing and timing between the Regional Entity's administration of Risk-Based Compliance Monitoring and Enforcement Program Modules?

¹² CCC Criteria for ICEs: When does the Regional Entity conduct the ICE and how does the Regional Entity take into account the results to adjust the scope of the monitoring approach. (1) ICE impacts the depth and focus of the monitoring scope determined after the IRA. (2) Does the Regional Entity conduct the Internal Controls Assessment after developing the scope of Standards to audit? When the Regional Entity administers the ICE, the scope of the ICE is related to Standards and Requirements that have a relationship to regional BES risks. If the scope of the ICE does not align with these Standards and Requirements, is the deviation adequately justified, including all supporting information and data? (3) What types of guidance, process, or templates does the Regional Entity provide registered entities in its footprint about the form and manner for providing information about internal controls? (4) How far in advance of compliance monitoring engagement (e.g., audit, spot check) does Regional Entity initiate ICE and how much time is the registered entity given to respond? (5) What are the use rates for ICE engagements? (5a) For RC/BA/TOPs, the percentage that agreed/declined ICE engagement. (5b) For each other type of Registered Entity, the percentage that agreed/declined ICE engagement.

by the ERO Enterprise, do not require the cost of travel and preparation by the registered entity. As part of risk-based CMEP, Regional Entities may choose to use self-certifications in lieu of an audit, for example, depending on the risk of the registered entity. As a result, the risk-based CMEP provides for more flexibility on the methods to be used in compliance monitoring. In 2015, the ERO Enterprise conducted approximately 250 compliance audits and spot checks.

Risk-based Enforcement

Background

The ERO Enterprise's enforcement jurisdiction is drawn from the Energy Policy Act of 2005 (the Act), which added section 215 to the Federal Power Act (FPA). Section 215 made compliance with electric Reliability Standards mandatory, and authorized the creation of an ERO and Regional Entities to establish and enforce Reliability Standards. Under section 215(e)(1) of the FPA, NERC or a Regional Entity may impose a penalty on a user, owner, or operator of the BPS for a violation of a Reliability Standard approved by FERC. As the ERO, NERC has set forth Sanction Guidelines outlined in its Rules of Procedure that govern the ERO Enterprise's penalties and non-monetary sanctions for Reliability Standard violations. This document provides information on the ERO Enterprise's enforcement philosophy, i.e., the ERO Enterprise's approach for assessing and resolving noncompliance while continuing to work to bring entities into compliance with applicable Reliability Standards.

ERO Enterprise Core Values and Guiding Principles

The ERO Enterprise's 2016-2019 Strategic Plan¹³ promotes the ERO Enterprise's core values and guiding principles, which are based on accountability and independence, responsiveness, fairness and inclusiveness, adaption and innovation, excellence, efficiency, and integrity. These core values and guiding principles support the four pillars of the ERO Enterprise's efforts, namely, reliability, assurance, learning, and a risk-based approach.

Strategic Goals Related to Enforcement

Strategic goal 2 provides that the ERO Enterprise shall:

Be a strong enforcement authority that is independent, without conflict of interest, objective and fair, and promote a culture of reliability excellence through risk-informed compliance monitoring and enforcement. The ERO Enterprise retains and refines its ability to use standards enforcement when warranted and imposes penalties and sanctions commensurate with risk. The ERO Enterprise retains and refines its ability to use Reliability Standards enforcement when warranted and imposes penalties and sanctions commensurate with risk.

The risk-based enforcement approach allows for the appropriate allocation of resources to the issues that pose a higher level of risk to the reliability of the BPS.

Guiding Enforcement Principles

The following principles serve as guidelines for the conduct and behavior of all involved in the ERO Enterprise enforcement program to ensure alignment with strategic goal 2 and the ERO Enterprise's core values.

Compliance Enforcement Authorities are independent, without conflict of interest, objective, and fair.

The ERO Enterprise strives to be a strong enforcement authority that is independent, without conflict of interest, objective, and fair. NERC and each of the Regional Entities has a code of conduct addressing the professional and ethical standards applicable to its personnel. Foremost among these standards is the requirement that no person work on a matter where that work may affect the person's financial interest. The ERO Enterprise also expects its personnel to conduct themselves professionally and respectfully when engaging with registered entities or other

¹³ Available at <http://www.nerc.com/AboutNERC/Documents/ERO%20Enterprise%20Strategic%20Plan%202016-2019.pdf>.

stakeholders. Personnel who do not meet these standards are subject to discipline, up to and including termination.

Enforcement program promotes culture of reliability excellence through a risk-based approach.

The ERO Enterprise's risk-based enforcement philosophy generally advocates reserving enforcement actions under section 5.0 of the Compliance Monitoring and Enforcement Program for those issues that pose a higher risk to the reliability of the BPS. The risk of a noncompliance is determined based on specific facts and circumstances, including any controls in place at the time of the noncompliance. The ERO Enterprise works with registered entities to ensure timely remediation of potential risks to the reliability of the BPS and prevent recurrence of noncompliance. The enforcement process allows parties to address risks collaboratively and promote increased compliance and reliability through improvement of programs and controls at the registered entities.

The ERO Enterprise applies a presumption of non-enforcement treatment of minimal risk noncompliance to entities with demonstrated internal controls who are permitted to self-log such minimal risk issues. Regarding other issues posing a minimal risk, NERC and the Regional Entities may exercise appropriate judgment whether to initiate a formal enforcement action or resolve the issue outside of the formal enforcement processes. The availability of streamlined treatment of minimal risk noncompliance outside of the formal enforcement process encourages self-inspection by registered entities. When self-identified minimal risk noncompliance is more than likely not going to be subject to a financial penalty, registered entities are encouraged to establish more robust internal controls for the detection and correction of noncompliance. This approach allows the ERO Enterprise to oversee the activities of registered entities in a more efficient manner and to focus resources where they result in the greatest benefit to reliability. In this context, efficiency does not necessarily mean less time or effort. Rather, it is using the requisite time, knowledge, and skills required for each circumstance. In addition, this approach allows the ERO Enterprise to continue to provide clear signals to registered entities about identified areas of concern and risk prioritization, while maintaining existing visibility into potential noncompliance and emerging areas of risk. Outcomes for noncompliance are based on the risk of a specific noncompliance and may range from streamlined, non-enforcement processes, to significant monetary penalties.

Enforcement actions are used and penalties are imposed when warranted, commensurate with risk.

An element of a risk-based approach to enforcement is accountability of registered entities for their noncompliance. No matter the risk of the noncompliance, the registered entity still bears the responsibility of mitigating that noncompliance. Based on the risk, facts, and circumstances associated with that noncompliance, the Regional Entity decides on an appropriate disposition track, inside or outside of an enforcement action, as described above and whether a penalty is appropriate for the noncompliance.

Penalties are generally warranted for serious risk violations (e.g., uncontrolled loss of load, CIP program failures) and for when repeated noncompliance constitutes an aggravating factor. In addition to the use of significant penalties to deter undesired behavior, the ERO Enterprise also incents desired behaviors.¹⁴ Specifically, Regional Entities may offset penalties to encourage valued behavior. Factors that may mitigate penalty amounts include registered entity cooperation, accountability (including admission of violations), culture of compliance, and self-identification of noncompliance.

Regional Entities may also grant credit in enforcement determinations for certain actions undertaken by registered entities for improvements in addition to mitigating factors. For example, Regional Entities may consider significant investments in reliability made by registered entities, beyond those otherwise planned and required,

¹⁴ The Sanction Guidelines, Appendix 4B to the NERC Rules of Procedure, in alignment with Section 215, establish a general rule that penalties and sanctions imposed for the violation of a Reliability Standard shall bear a reasonable relation to the seriousness of the violation while also reflecting consideration of the other factors specified in the Sanction Guidelines. The Sanction Guidelines are available at http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4B_SanctionGuidelines_20140701.pdf.

as an offset for proposed penalties in enforcement determinations. Regional Entities do not award credits or offsets for actions or investments undertaken by a registered entity that are required to mitigate noncompliance.

NERC engages in regular oversight of Regional Entity enforcement activities to confirm that the Regional Entities have followed the CMEP. This oversight evaluates the consistency of disposition methods, including assessment of a penalty or sanction, with previous resolutions of similar noncompliance involving similar circumstances. The NERC Board of Trustees Compliance Committee (the Compliance Committee) considers the recommendations of NERC staff regarding approval of Full Notices of Penalty and monitors the handling of noncompliance through the streamlined disposition methods of Spreadsheet NOPs, FFTs, and Compliance Exceptions.

Actions are timely and transparent.

The ERO Enterprise maintains an elevated level of transparency regarding enforcement matters. NERC's Rules of Procedure (including the CMEP and Sanction Guidelines) and program documents are available to the public.¹⁵ NERC also posts information on enforcement actions on a monthly basis.¹⁶ Moreover, information on the efficiency of the enforcement program is available to the public on a quarterly basis.¹⁷

Noncompliance information is used as an input to other processes.

When developing risk elements, NERC annually identifies and prioritizes risks to the reliability of the BPS, taking into account factors such as compliance findings, event analysis experiences, and data analysis. In addition, Regional Entities consider factors such as noncompliance information when conducting an IRA of a registered entity. The ERO Enterprise also uses noncompliance information as part of a feedback loop to the standards development process. This allows enhanced Reliability Standards through appropriate information flows from compliance monitoring and enforcement to the standards drafting process and other NERC programs. NERC regularly provides analysis and lessons learned from noncompliance information to the public.¹⁸

2015 Enforcement Results

In 2015, enforcement activities throughout the ERO Enterprise reflected the full implementation of the risk-based approach introduced in 2013 through the Reliability Assurance Initiative. The risk-based approach used by the ERO Enterprise aligns the outcome of any noncompliance to the risk that particular noncompliance posed to the reliability of the BPS. In that sense, the outcome could range from a significant monetary penalty to a streamlined disposition outside of the enforcement process. This approach, and the high usage of streamlined methods shown below, are predicated on a significant level of cooperation by registered entities. In this context, cooperation is evidenced in part by high levels of self-identification of noncompliance and prompt mitigation of issues. These historic trends continued in 2015, as noted in the Appendix. Maintaining these trends of high self-identification and prompt mitigation is essential to the effectiveness of the risk-based program.

This report discusses the results achieved in 2015 with respect to two streamlined programs in particular: Self-Logging and Compliance Exceptions. Included in the Appendix are processing efficiency results, which indicate how these programs have allowed the ERO Enterprise to operate more efficiently.

These two processes allowed the ERO Enterprise to consolidate the efficiency gains obtained with the introduction of the Find, Fix, Track, and Report process in 2011.¹⁹

¹⁵ The NERC Rules of Procedure are available at <http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx>.

¹⁶ Posted compliance exceptions, Spreadsheet Notices of Penalty, and Full Notices of Penalty are available at <http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx>.

¹⁷ Quarterly enforcement program information is available at [http://www.nerc.com/gov/bot/BOTCC/Pages/ComplianceCommittee\(BOTCC\).aspx](http://www.nerc.com/gov/bot/BOTCC/Pages/ComplianceCommittee(BOTCC).aspx).

¹⁸ For example, NERC posts quarterly compliance reports at [http://www.nerc.com/gov/bot/BOTCC/Pages/ComplianceCommittee\(BOTCC\).aspx](http://www.nerc.com/gov/bot/BOTCC/Pages/ComplianceCommittee(BOTCC).aspx).

¹⁹ See the Appendix for information regarding processing efficiency.

As noted below, the ERO Enterprise continues to process violations that require the imposition of monetary penalties when those are warranted. Consistent with the risk-based approach that happens when violations pose a serious or significant risk to the reliability of the BPS (either individually considered or in the aggregate). Serious risk violations generally involve uncontrolled loss of load, outages from vegetation contacts, or programmatic failures, particularly on the CIP side.

The ERO Enterprise also continues to analyze the minimal risk noncompliance that is resolved as compliance exceptions to look for trends and emerging risks.

For 2016, the ERO Enterprise expects to continue to grow both programs as well as look for opportunities for enhancement. NERC regularly reviews Regional Entity enforcement processes and samples outcomes to ensure that the implementation is consistent with the requirements of the programs. NERC will continue to do so in 2016. NERC will also continue to monitor mitigation completion, self-reports, and the level of risk posed by noncompliance with Reliability Standards.

Historically, these metrics have shown that very few instances of noncompliance pose a serious or significant risk to the reliability of the BPS, which most noncompliance is self-identified by registered entities, and that mitigation is promptly done. The continuation of these trends help demonstrate the effectiveness of the ERO Enterprise enforcement program.

Disposition of Noncompliance in 2015

Below are summaries of the four methods used to process noncompliance in 2015. Additional information regarding ERO Enterprise 2015 processing-related goals and metrics and other relevant trends are also found in the Appendix.

Compliance Exceptions

Compliance exceptions are a disposition track used for noncompliance posing a minimal risk to the reliability of the BPS that does not warrant a penalty and is not pursued through an enforcement action.²⁰ Compliance exceptions must be mitigated within 12 months of the time of the notification to the registered entity of compliance exception treatment. In 2015, this disposition track became available to all registered entities throughout the ERO Enterprise. Use of compliance exceptions as a disposition track in 2015 is shown in Figure 2.

In 2015, the ERO Enterprise fully implemented the compliance exception disposition track. Throughout 2015, the ERO Enterprise has been aligned with CCC Criteria regarding compliance exceptions²¹ by regularly using compliance exceptions and consistently exercising appropriate judgment in treating noncompliance matters as compliance exceptions when they posed a minimal risk to the reliability of the BPS. Because compliance exceptions may come from any of the Reliability Standards, the exercise of appropriate judgment is informed by the facts and circumstances of the noncompliance, the risk posed by the noncompliance to BPS reliability, and the potentially deterrent effect of an enforcement action or penalty, among other things.

In 2015, out of 741 instances of noncompliance posing a minimal risk, the ERO Enterprise disposed of 514 (69.4%) as compliance exceptions. This allowed the Regional Entities to dispose of minimal risk noncompliance efficiently

²⁰ Enforcement actions are contemplated in Section 5 of the CMEP; alternative disposition methods are contemplated in Section 3A.0 of the CMEP.

²¹ CCC Criteria D.3: Minimal risk violations are consistently and appropriately treated as compliance exceptions. For minimal risk issues not processed as compliance exceptions, the evaluation and determination for enforcement treatment is properly documented.

and focus resources on moderate to serious risk noncompliance.²² Information on processing efficiencies in 2015 is found in the Appendix.

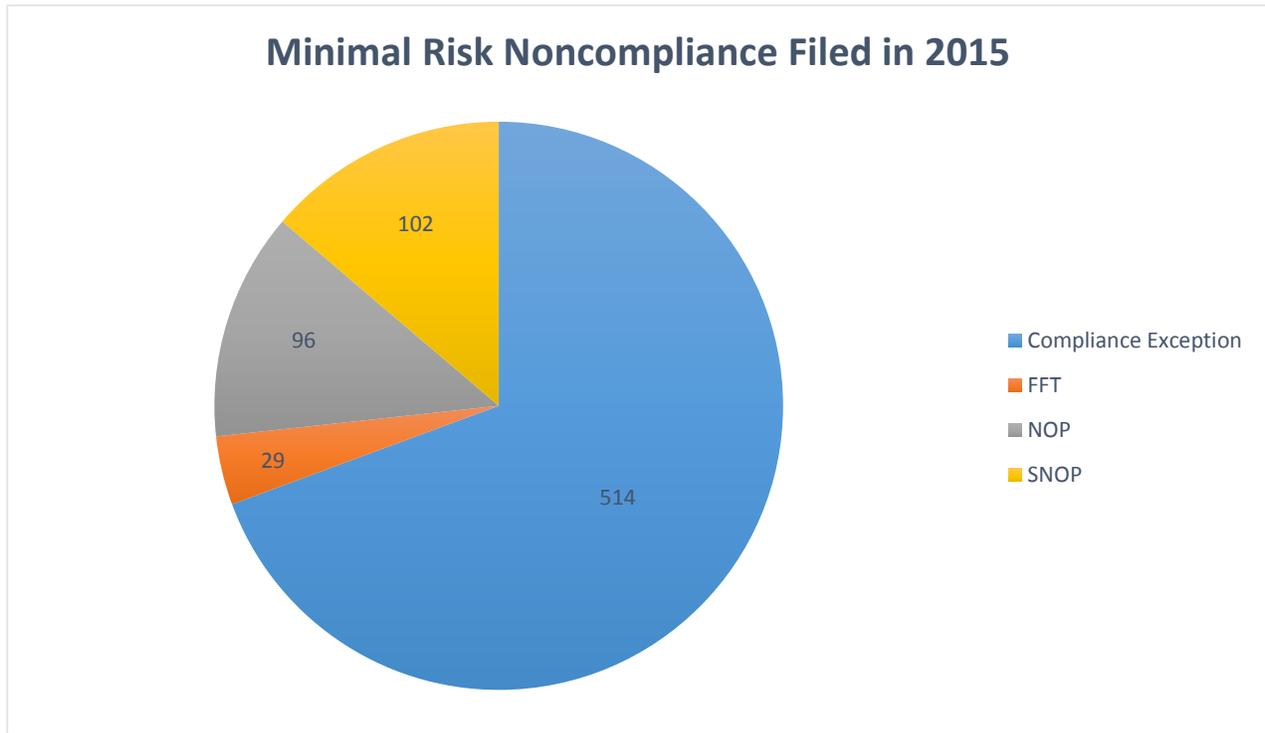


Figure 2: Minimal Risk Noncompliance Filed in 2015

Find, Fix, Track, and Report (FFT)

The FFT program—the first, significant step in implementing a risk-based approach to enforcement implemented by the ERO Enterprise in 2011—is a process that the ERO Enterprise uses primarily to resolve moderate risk issues that are suitable for streamlined treatment (as opposed to through a Notice of Penalty). Under the FFT program, moderate risk issues are fixed, tracked, and reported to Regional Entities and NERC. This noncompliance is not subject to penalties. FFTs also may be used to dispose of minimal risk noncompliance that is related to a moderate issue being resolved as an FFT. In 2015, compliance exceptions have superseded the FFT program for resolving minimal risk noncompliance.²³ In 2015, out of 980 instances of minimal or moderate risk noncompliance, the ERO Enterprise disposed of 8% as FFTs.

Spreadsheet Notice of Penalty (SNOP)

SNOPs include noncompliance posing a minimal or moderate risk to the reliability of the BPS. Once Regional Entities have entered into Settlement Agreements with, or have issued Notices of Confirmed Violations (NOCVs) to the registered entities, that information is reported to NERC for oversight review and approval. NERC then files that information with FERC in a spreadsheet format for review and approval. The SNOP identifies the following: the Regional Entity, the registered entity, disposition as a NOCV or Settlement Agreement, the violation, Reliability Standard, Violation Risk Factor and Severity Level, total penalty or non-monetary sanction, method of discovery, mitigation activity, mitigation completion date, date Regional Entity verified mitigation completion, an admission, denial, or no contest to violation, and other factors affecting the penalty determination, such as

²² In addition to increasing Regional Entity efficiencies, this also creates efficiencies for registered entities and allows them to focus resources on reliability and compliance.

²³ FFT treatment will only apply to minimal risk noncompliance if that noncompliance is associated with a moderate risk noncompliance receiving FFT treatment.

compliance history, internal compliance program, and compliance culture. In 2015, out of 980 instances of minimal or moderate risk noncompliance, the ERO Enterprise disposed of 18% as SNOPs.

Full Notices of Penalty (NOP)

Full NOPs generally include noncompliance that poses a serious or substantial risk to the reliability of the BPS. Full NOPs may also be appropriate for a registered entity that has a large number of minimal or moderate risk violations that could be indicative of a systemic issue, dispositions involving higher than typical penalty amounts, or those with extensive mitigation or above and beyond actions taken by the registered entity. Similar to SNOPs, once the Regional Entity has resolved the violation, NERC receives the information for oversight review and approval. NERC then files the Full NOP with FERC for review and approval. Full NOPs generally are violations resulting in the following: extended outages, uncontrolled loss of load, cascading blackouts, vegetation contacts, systemic or significant performance failures, intentional or willful acts or omissions, and gross negligence. In 2015, out of 1025 instances of noncompliance posing various levels of risk, the ERO Enterprise disposed of 256 (25%) as Full NOPs.

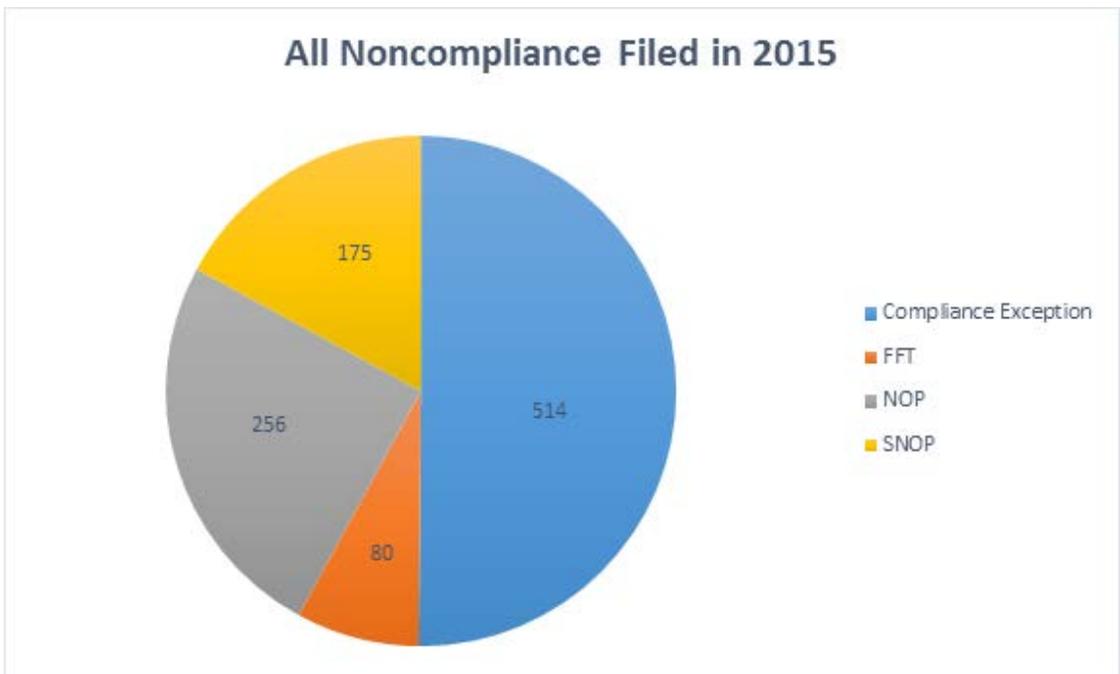


Figure 3: All Noncompliance Filed in 2015

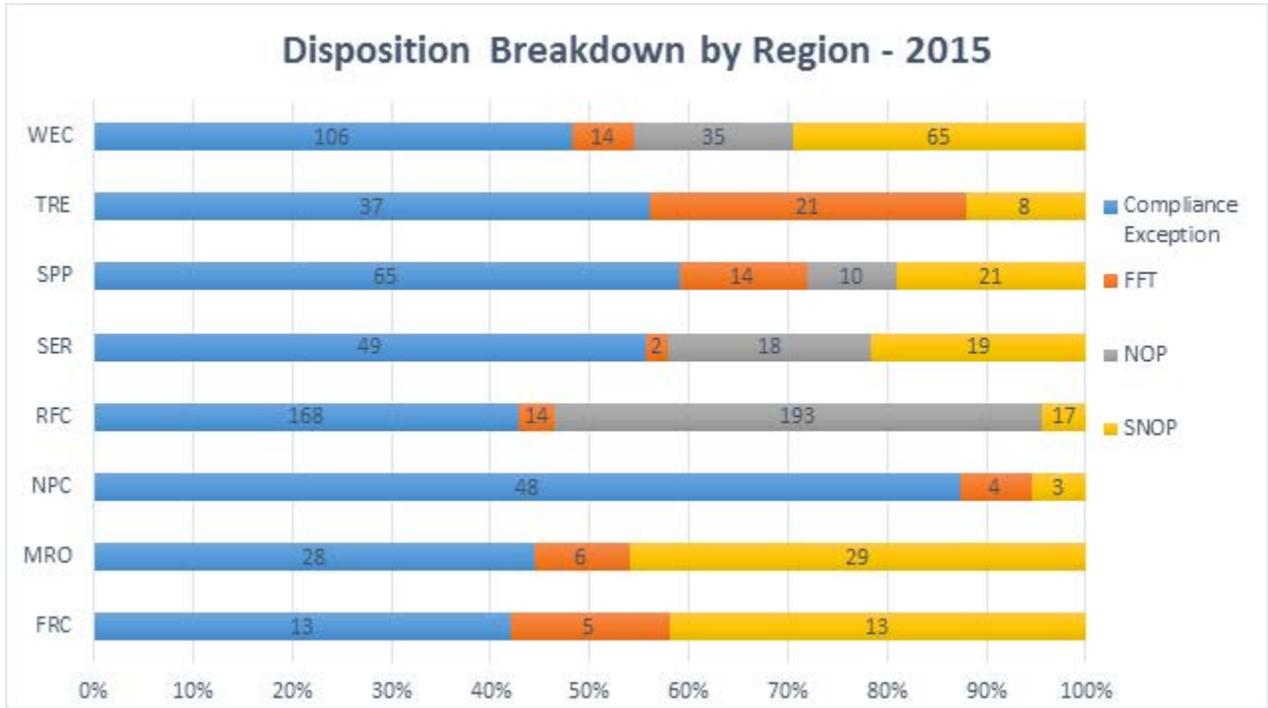


Figure 4: Disposition Breakdown by Region - 2015

Self-Logging Use

In 2013, the ERO Enterprise selected certain registered entities to self-log minimal risk noncompliance. At the start of 2015, self-logging became open to all registered entities that met the program qualifications based on Regional Entity evaluation and approval. Through the self-logging program, the ERO Enterprise seeks to encourage registered entities to detect, accurately assess the risk of, and adequately mitigate minimal risk noncompliance with the Reliability Standards. Specifically, in evaluating whether a registered entity is eligible for the program, the Regional Entities will conduct a formal evaluation of the registered entity’s controls associated with the registered entity’s ability to identify, assess, and correct noncompliance.²⁴

Once a registered entity is approved to self-log, that log is periodically reviewed by the Regional Entity. Properly logged items are entitled to the presumption of being resolved as compliance exceptions unless there are additional risks involved. This is consistent with the notion that noncompliance that is self-identified through internal controls, corrected through a strong compliance culture, and documented by the entity, should not be resolved through the enforcement process or incur a penalty, absent a higher risk to the reliability of the BPS.

Since self-logging became available to all registered entities that met the program qualifications at the start of 2015, 42 registered entities have been approved by Regional Entities to self-log as of December 31, 2015. These registered entities represent nearly all of the reliability functions. To help benchmark the effectiveness of the self-logging program, the CCC proposed that the ERO Enterprise monitor the percentage of registered entities within a Functional Model category authorized to self-log minimal risk violations. Figures 5 and 6, respectively, represent the registered entities by reliability function that are self-logging and the Regional Entities use of the self-logging program.²⁵

²⁴ In November 2015, FERC approved the ERO Enterprise Self-Logging Program document, which includes the method to evaluate eligibility. The program document is available at <http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Enterprise%20Self-Logging%20Program.pdf>.

²⁵ Currently, no registered entities are self-logging at FRCC, and FRCC has no formal requests from entities to date.

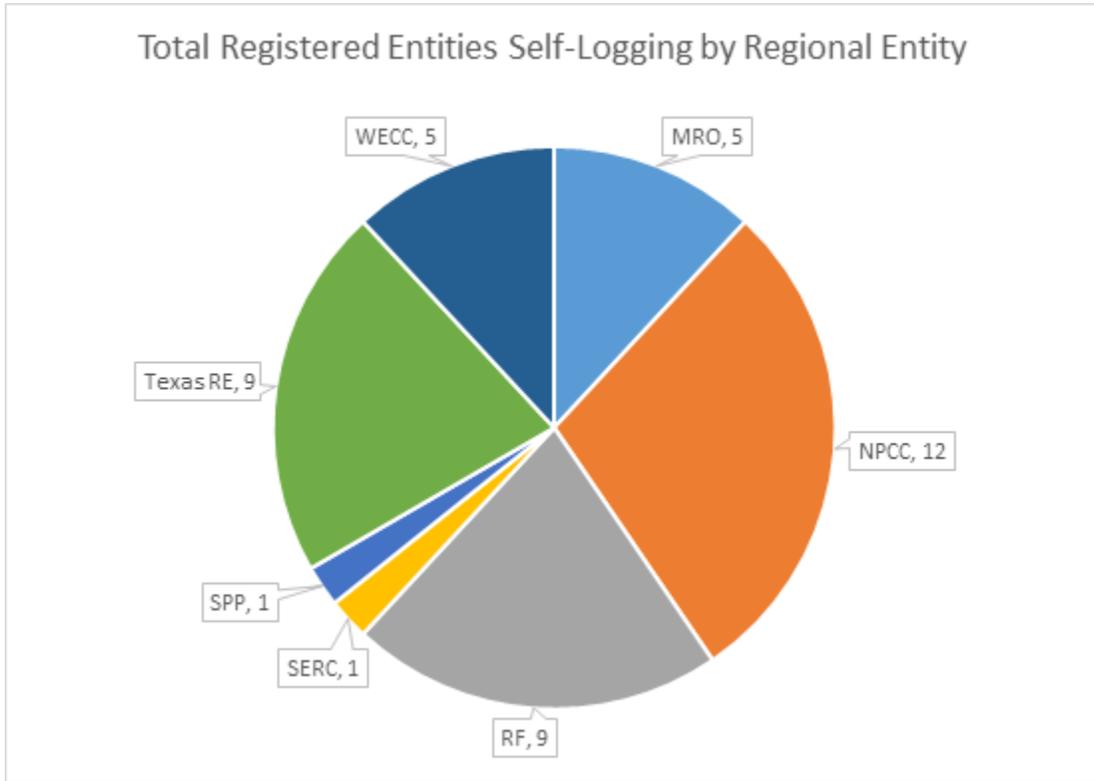


Figure 5: Total Registered Entities Self-Logging by Regional Entity

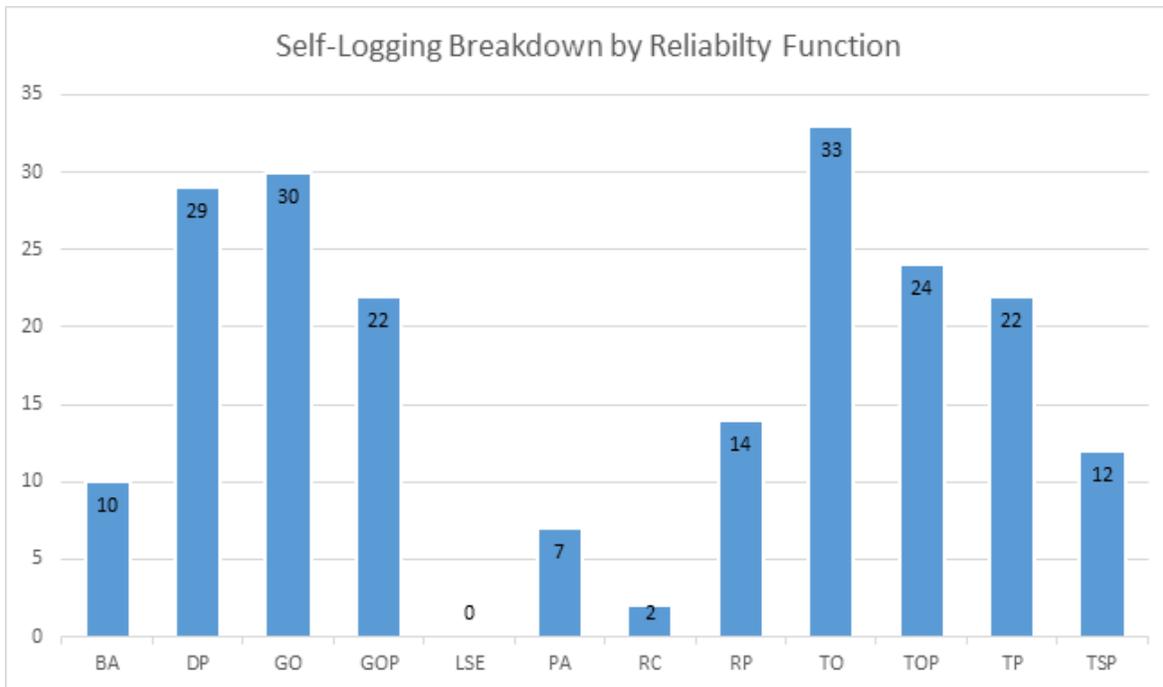


Figure 6: Self-Logging Breakdown by Reliability Function

ERO Enterprise CMEP Training, Education, and Outreach

ERO Enterprise Staff Training and Education

To address success factor 1 on ERO Enterprise staff competency during 2015, NERC Compliance Assurance and Compliance Enforcement departments, supported by the Regional Entities, developed and provided ongoing education and training on the transformation of compliance monitoring and enforcement for the ERO Enterprise staff. In particular, the training focused heavily on continuing education for implementing the IRA and ICE components of the risk-based CMEP to support successful implementation and consistency. In addition, NERC hosted one workshop for all CMEP staff in March 2015, which included education on Regional Entity IRA and ICE processes and another workshop in October 2015 specifically for enforcement staff.

During the initial risk-based CMEP implementation stage, the ERO Enterprise conducted training on the foundational IRA and ICE concepts using real-life scenarios and examples. Current training provides further depth and incorporates lessons learned from examples obtained throughout actual application of risk-based CMEP. For example, in July 2015, NERC sponsored an instructor-led training for scoping and performing audits and assessing internal controls. Over 30 ERO Enterprise staff responsible for conducting audits and performing ICE activities attended one or both of the 16-hour courses offered. Additionally, NERC recommended online training available through the ERO Enterprise learning management system, including Auditing for Internal Control and Risk Assessment for staff responsible for IRA and ICE activities. NERC continues to identify relevant and available online courses to include as part of the overall ERO Enterprise risk-based training curriculum within the learning management system. Figure 7 below identifies the number of hours of training by competency area.

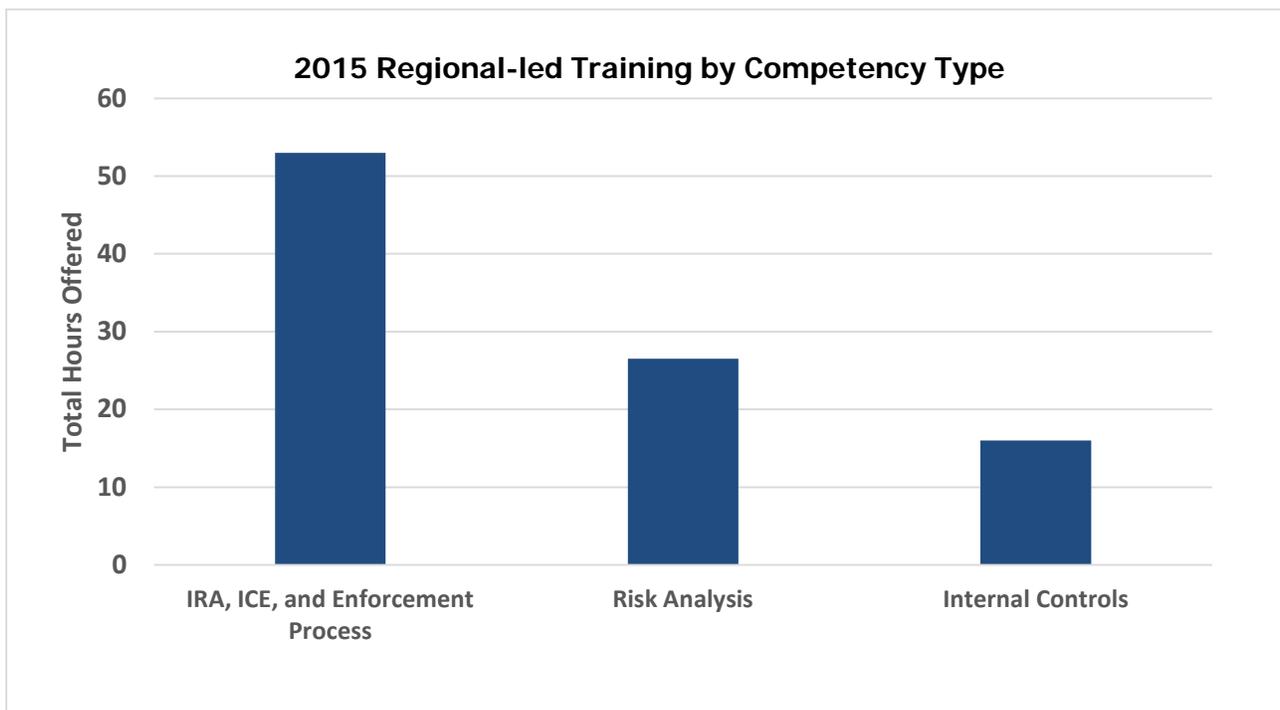


Figure 7: 2015 Regional Entity-led Training Hours of by Competency Type

Following each of the training and education events, a survey was distributed to obtain information on the general satisfaction, delivery method, content, and overall value participants felt they gained from the sessions. ERO Enterprise staff used this input for future training activities.

Further, NERC engaged a vendor to perform a compliance monitoring personnel competency analysis to assist with long-term curriculum development for the risk-based compliance monitoring portion of the CMEP. The product deliverables for this effort will include a well-defined task listing by role and a recommended training and education plan to inform the qualification program for the risk-based CMEP. The ERO Enterprise will use these deliverables to refine and update the exiting ERO Enterprise competency guide, which outlines role and competency expectations for compliance monitoring staff. Similarly, the ERO Enforcement Group is developing a competency guide that will identify the combination of skills, attributes, and behaviors that are directly related to successful performance of enforcement positions. This guide will also inform the training needs of ERO Enterprise enforcement staff.

Industry Stakeholder Information and Outreach

During the broad implementation of risk-based design, NERC and the Regional Entities have taken advantage of several outreach opportunities to identify lessons learned and gather input into how to best implement the risk-based design. The ERO Enterprise continues to collaborate to identify common processes and opportunities to improve consistency in implementation through industry advisory groups, discussion with various trade organizations, and ongoing webinars and workshops. In addition, NERC and the Regional Entities performed outreach on the CIP Version 5 transition to support industry stakeholder readiness.

NERC focused on success factor 2 (relating to industry stakeholder information and outreach for risk-based CMEP) through various events, such as workshops and webinars. During Q4 of 2014 and Q1 of 2015, the ERO Enterprise hosted a series of three outreach events. The three outreach events included ERO Enterprise staff and industry panelists presenting on risk-based topics. The outreach events provided continued communication and education to industry stakeholders on the ERO Enterprise's transformation to risk-based compliance monitoring and enforcement activities. During these events, presentations were given by panels of industry stakeholders and ERO Enterprise staff. In support of success factor 6 (regarding recognized value), the ERO Enterprise solicited feedback from participants in these events. Based on this feedback, participants noted that the events provided an opportunity for industry stakeholders to share examples, tips, and techniques for how registered entities can prepare for future interactions with risk-based CMEP activities. Stakeholders also found that the industry panels addressed some areas of concern regarding expectations for participating in IRA and ICE processes and allowed industry to hear different viewpoints from various involvement in on-going risk-based CMEP activities. NERC staff also presented at the spring and fall Standards and Compliance Workshops in Atlanta, GA, and San Diego, CA, respectively. The Spring Standards and Compliance Workshop featured a joint industry and Regional Entity session on risk-based CMEP to facilitate further mutual understanding of risk-based concepts.

Additionally, the ERO Enterprise hosted a series of webinars on each risk element outlined in the 2015 CMEP Implementation Plan. Each monthly webinar focused on one risk element and included guidance and discussion on the areas of focus identified in the 2015 CMEP Implementation Plan. Figure 8 demonstrates the number of participants on the webinars and the level of satisfaction.

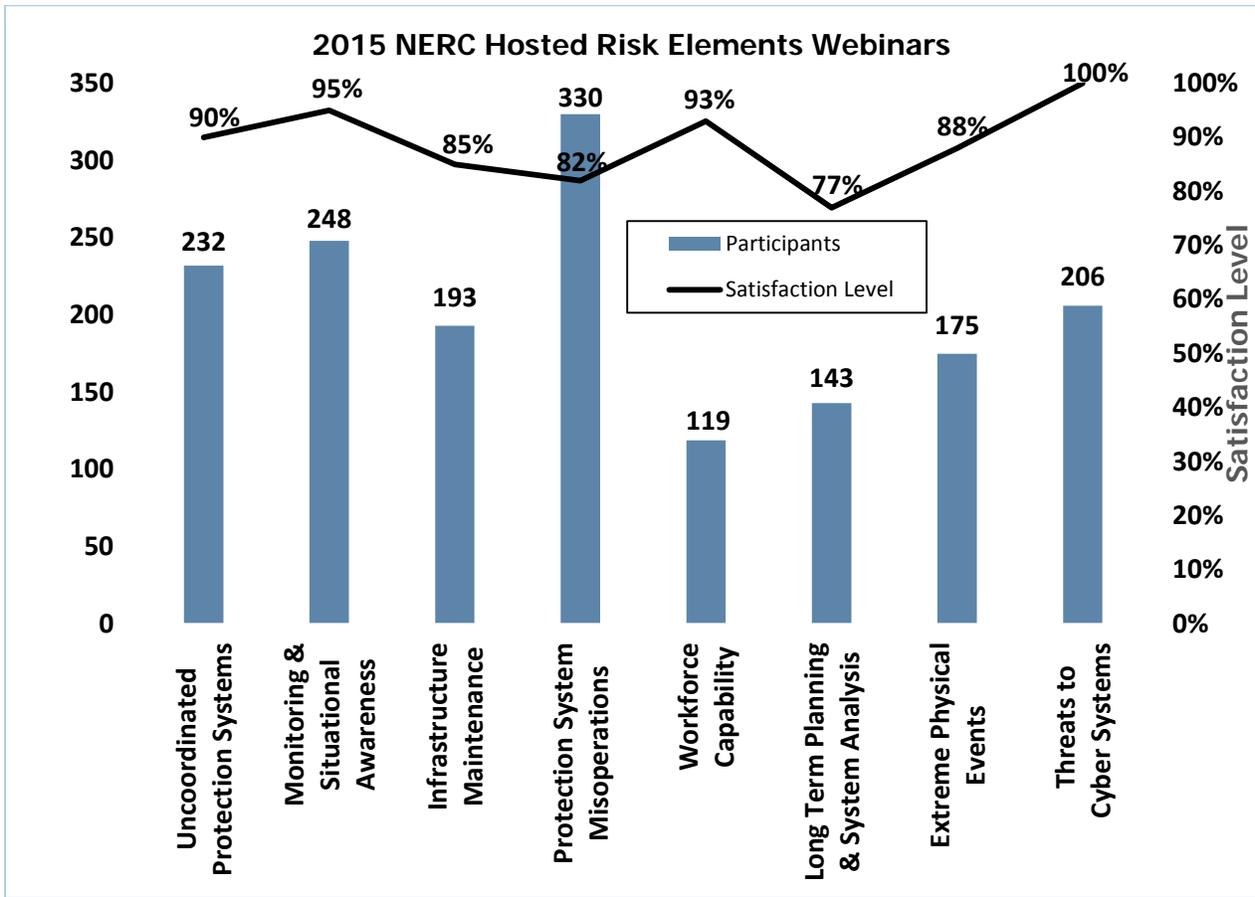


Figure 8: Risk Elements Webinars Participants and Satisfaction

Each Regional Entity also conducted meetings, conference calls, webinars, and workshops to address the industry’s questions and concerns over risk-based CMEP. All key elements and region-specific subjects of compliance monitoring and enforcement were discussed during a risk-based CMEP workshop in early 2015 and at the semi-annual Standards & Compliance workshops, with attendance ranging from 80 to 200 participants. The workshops provided a platform to discuss specific risk-based subjects such as self-logging, the IRA and ICE processes, and other components of the risk-based CMEP.

Although there was a continued focus of outreach activities on the risk-based CMEP approach, Regional Entities also conducted outreach for other areas such as new Reliability Standards and the CIP Version 5 transition through face-to-face meetings and conferences with industry. In addition, NERC and the Regional Entities coordinated with a group of industry stakeholders for an educational exercise in February 2015. The purpose of that exercise was to discuss how the ERO Enterprise scales ICE processes for smaller, low-risk registered entities, and to help NERC and the Regional Entities obtain a better understanding of how small entities identify, evaluate, and document internal controls. During the exercise, NERC and the Regional Entities explained that they appropriately scale the internal control evaluation to take into account entity size and risk characteristics. This exercise supported success factor 6 in demonstrating recognized value of the risk-based CMEP for entities of all sized. Figure 9 illustrates the total number of industry outreach events and Figure 10 illustrates stakeholder participation in Regional Entity 2015 industry outreach events, which included topics on risk-based CMEP and CIP.

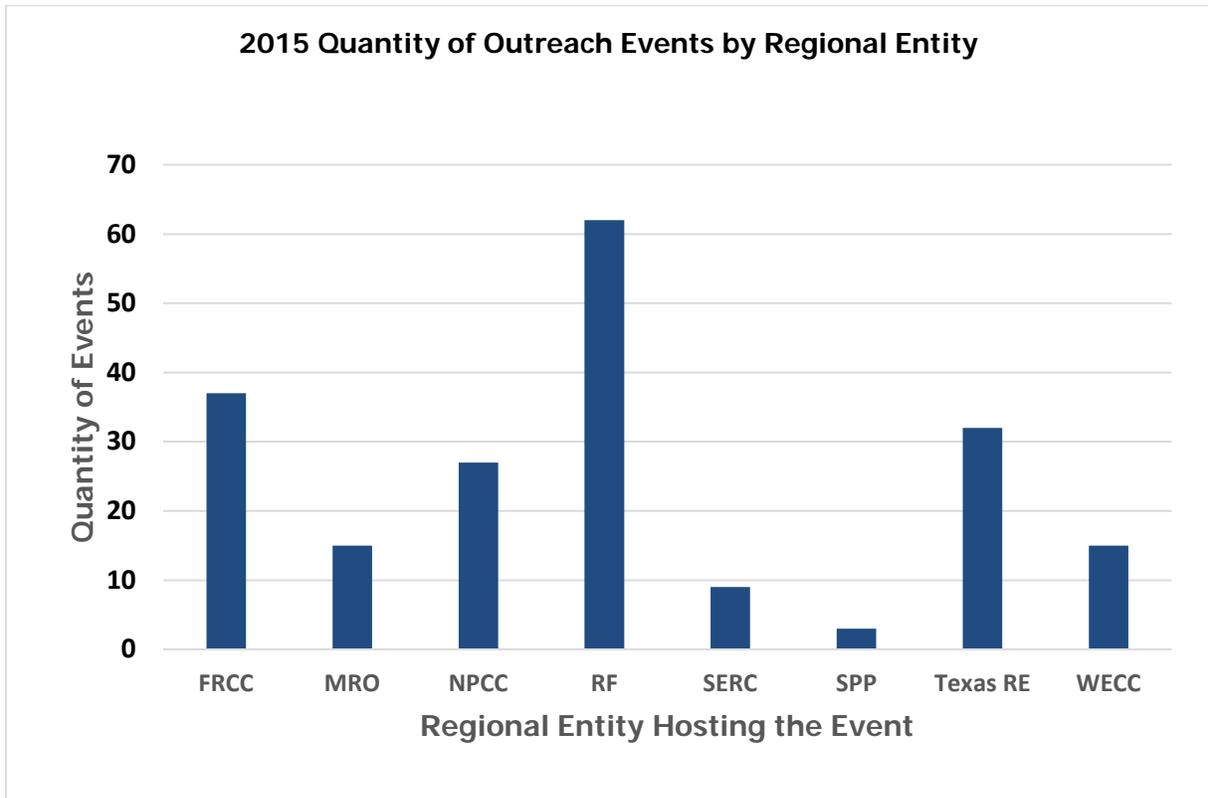


Figure 9: Regional Entity 2015 Industry Outreach Events

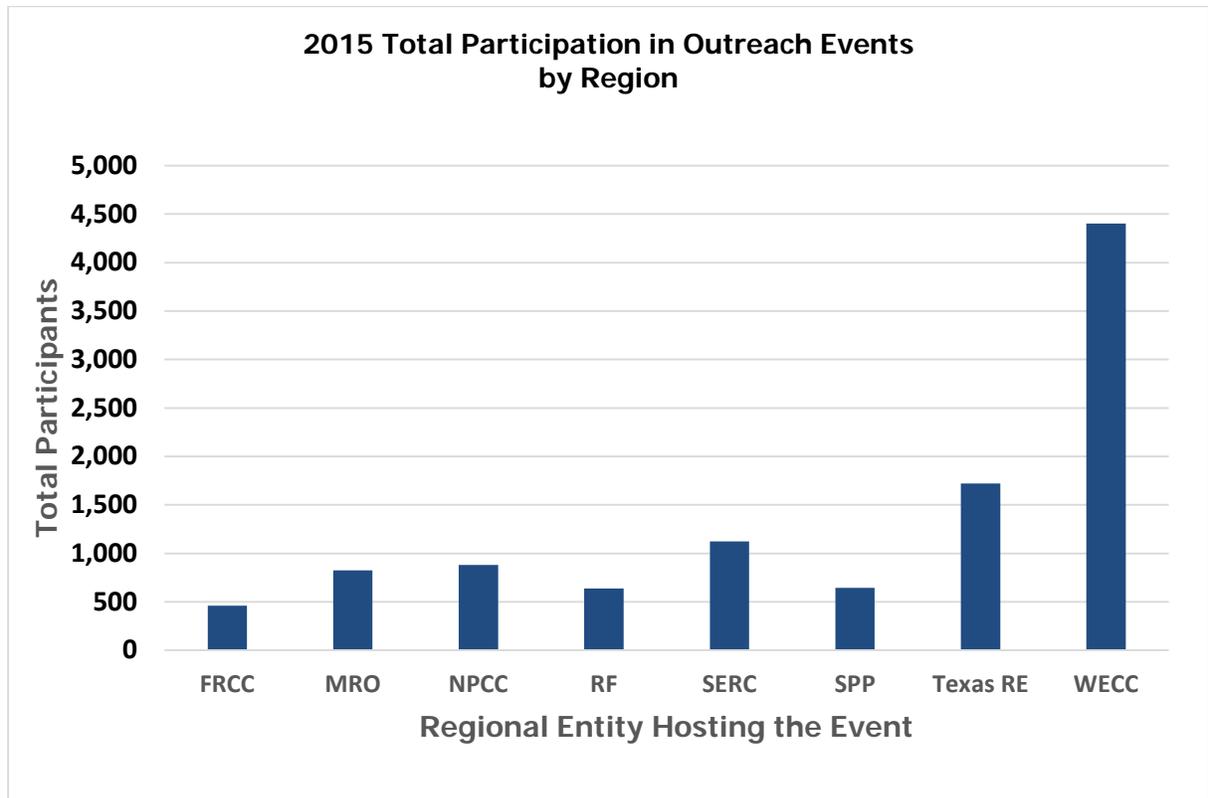


Figure 10: Regional Entity 2015 Industry Participation in Outreach Events

In 2016, NERC and the Regional Entities will continue to conduct outreach activities that focus on self-logging, compliance exceptions, risk elements, frequently asked questions, and examples of completed IRAs and ICES. NERC plans to use existing industry events, like the Standards and Compliance workshops, to provide information on risk-based activities.

NERC Oversight of the Regional Entities

Risk-based Compliance Monitoring Oversight

At the end of 2014, the ERO Enterprise finalized IRA and ICE Guides in support of success factors 3 and 4 on consistency and balanced transparency. During the first half of 2015, NERC Compliance Assurance staff assessed each Region's processes and degree of alignment with the criteria from these guides. This review established conceptual consistency in the application of risk-based compliance monitoring among all eight Regional Entities. At the end of these reviews, NERC provided reports that included feedback and recommendations to the Regional Entities on their processes. Overall, NERC concluded that Regional Entities were conceptually aligned on the major components of the risk-based compliance monitoring framework.

During the remainder of 2015, NERC oversight focused on further refinement of the risk-based CMEP in support of implementation. Such oversight included frequent engagements with Regional Entities and development of an IRA analysis team to ensure consistency across Regional Entities in areas where consistency is most important. In addition, NERC engaged in observations of audits of registered entities conducted by Regional Entities, collected IRA results, and reviewed Regional Entities' post-audit feedback surveys. The following sections describe these oversight activities in more detail. Going forward in 2016, NERC will review lessons learned from implementation in 2015 to inform its risk-based approach to oversight of the Regional Entities.

Oversight of Initial Implementation of Risk-based Compliance Monitoring

Although all Regional Entities were conceptually aligned on the major components, there were cases, due to timing and the initial implementation status of IRA and ICE, the Regional Entity's IRA or ICE processes as documented and described may not have yet been fully implemented. Accordingly, some Regional Entities were assessed on conceptual alignment as documented or described and not on whether such practices were actually fully implemented or documented. In addition to assessing alignment with the IRA and ICE Guides, oversight activities revealed other opportunities for IRA and ICE process improvements, enhanced IRA and ICE tools, guidance, and training across the ERO Enterprise.

Recognizing that 2015 was an implementation year, initial oversight activities revealed that Regional Entities made meaningful strides in transitioning to risk-based compliance activities. Overall, all eight Regional Entities were generally aligned with the IRA and ICE alignment criteria reviewed. As part of these oversight activities, NERC and Regional Entity staff also identified some general improvement opportunities to assist in successful implementation throughout 2015.

After closing out initial implementation oversight activities in June 2015, NERC and the Regional Entities continued to collaborate to identify program opportunities and refinement needs. Further, NERC continued conducting risk-based compliance monitoring oversight through a variety of methods described in the sections below.

Registered Entity Audit Observations and Reviews

NERC samples a selection of Regional Entity audits of registered entities to observe and review. Through audit observations, NERC monitors both the audit process, including audit-scoping determinations, and assesses the Regional Entities' evaluations of registered entity compliance with NERC Reliability Standards. Further, audit observations help NERC to assess the overall implementation of ERO Enterprise activities, such as risk-based compliance monitoring, CIP Version 5 transition, Physical Security Reliability Standard implementation, and the Coordinated Oversight Program of MRREs, and to identify program development needs, training, and outreach. In 2015, NERC observed a total of seven audits with audit scopes including both CIP and Operations and Planning and with registered entities within the Coordinated Oversight Program for MRREs. NERC did not identify any concerns relating to any Regional Entity evaluation of a registered entity's compliance with the NERC Reliability Standards.

NERC's involvement in the audit observations provided a better understanding of the ERO Enterprise audit process applied in a risk-based environment. NERC will also use lessons learned to help shape the compliance monitoring observation program for 2016. For example, starting in 2016, NERC staff will participate in other aspects of compliance monitoring activities in addition to audit observations. As recommended and noted by Regional Entity staff, NERC observations of Regional Entity IRA and ICE processes, as well as off-site, pre-audit evidence reviews, will provide NERC staff more line of sight to how Regional Entities are implementing risk-based compliance monitoring. Further, the 2016 audit observation approach will include a NERC staff development opportunity that invites NERC staff outside of Compliance Assurance to participate as observers in the Regional Entity audits of registered entities.

From the observations of these seven audits, NERC identified some positive observations, as well as lessons learned and opportunities for consistency and overall improvements to compliance monitoring. For example, NERC noted that Regional Entity staff continue to provide registered entities updates on the audit status to keep the entities informed and hold open and timely discussions around possible areas of noncompliance. Further, registered entities stated that they felt the audit(s) were focused on high-risk areas and were tailored specifically to their entity characteristics. Improvement opportunities exist in the areas of the Coordinated Oversight Program for MRREs to help ensure that consistent and efficient processes are occurring, as well as the identification, documentation, and feedback of new or refined risk areas identified during compliance monitoring activities. This feedback can help refine or impact initial IRAs. This feedback loop is an important component of understanding a registered entity and properly assessing its risks to tailor monitoring activities.

IRA Results Summary Collection

During Q4 of 2015, NERC began collecting IRA summary reports to do the following: (1) monitor Regional Entity progress toward completing initial IRAs for registered entities; (2) gather data on risks being identified and associated NERC Reliability Standards and requirements monitored; and (3) understand how significant BPS reliability risks are being monitored. Going forward, and on a periodic basis, NERC will sample IRA summary reports and request supporting documentation of IRA activities. The purpose of sampling and reviewing supporting IRA documentation is to help further understand, on a total ERO Enterprise basis, Regional Entity processes and procedures being used to complete implementation of risk-based compliance monitoring and drive toward oversight that is monitoring the necessary risks for each entity. Through this monitoring activity, NERC can assist in identifying good practices, lessons learned, and other opportunities for program consistency and improvement.

Being an implementation year, NERC's primary focus of review in Q4 of 2015 has been on establishing a repeatable process for collection of IRA results summaries, creating mechanisms to maintain and track information contained within the IRA results summaries, and identifying registered entities involved in initial IRAs. As the monitoring program evolves in 2016, NERC will gather and analyze data to further understand how significant BPS reliability risks are being monitored across the ERO Enterprise.

Review of Registered Entity Post-Audit Feedback Surveys

Following every audit, registered entities have an opportunity to complete post-audit feedback surveys. Since transitioning to risk-based compliance monitoring, the feedback survey now includes questions relating to all steps within the risk-based compliance monitoring framework. During 2015, NERC and the Regional Entities updated the post-audit feedback survey to reflect risk-based activities, which is now electronically available to the registered entities.

Both NERC and the Regional Entities review the surveys to help gauge industry stakeholder perception, as well as to enhance understanding of risk-based compliance monitoring activities. Post-audit feedback surveys aim to provide a feedback loop to NERC and the Regional Entities by identifying successes and opportunities of program development, as well as possible education and training opportunities for ERO Enterprise staff. In 2015, NERC and the Regional Entities collected 70 post-audit feedback surveys, which is a response rate of about 35% of the total

number of audits conducted in 2015. Overall, survey responses indicated continued support by registered entities of the risk-based compliance monitoring approach, noting that most audits had a clear focus of monitoring efforts on reliability risk. Further, registered entities noted their appreciation for the CIP Version 5 outreach provided by the audit teams, as well as the audit team's flexibility to audit scheduling, clear and transparent communication during the audit, and the professional demeanor of the audit team. Registered entities also commended the audit teams' review of large volumes of work during the off-site pre-audit portion. In addition, feedback surveys indicated an opportunity for the ERO Enterprise to improve communication regarding the IRA and ICE results and impact on compliance oversight plans.

Risk-based Enforcement Oversight

NERC oversight of the Regional Entity enforcement processes is performed, among other activities, through the review of the supporting evidence, and other information provided by the Regional Entities over the course of focused engagements 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 consistent implementation of the risk-based CMEP. Such recommendations and findings also helped to identify priority areas for training of ERO Enterprise staff throughout 2015.

These reviews complement the analysis by NERC of enforcement data and calculation of metrics²⁶ and provides input to the development of feedback, guidance, and training.²⁷

Annual Reviews Conducted in 2015

NERC reviews specific enforcement-related processes throughout the year. Subjects that have been reviewed include mitigation plans, dismissals, settlement practices, and FFTs. As a result of the reviews, NERC provides feedback to the Regional Entities on areas and activities to enhance consistency and effectiveness of processes.

In September 2015, NERC filed its annual report of the FFT program. During Q1 of 2015, NERC and FERC jointly performed the annual sampling and process review of the Regional Entities' FFT programs. The purpose of the review was to gather information on the implementation and effectiveness of the FFT program across all eight Regional Entities. NERC and FERC's 2015 review involved a coordinated sample of 100 processed FFTs for the period of October 2013 through September 2014. NERC's and FERC's review of the record included evaluation of the methods used by the Regional Entities to process Possible Violations as FFTs. NERC and FERC reviewed Regional Entity internal documents, including enforcement process diagrams, procedure manuals, step-by-step internal processes, checklists, and FFT Notice Letters.

Of the 100 FFTs reviewed, NERC and FERC did not identify any noncompliance that was inappropriate for FFT treatment. The results of the review indicate that the program remains successful and continues to be properly implemented.

A combined review of Compliance Exceptions and FFTs began, in coordination with FERC, in Q4 of 2015. NERC will also conduct a review of the self-logging program in 2016 to encompass 2015 activities.

²⁶ NERC analyzes enforcement data to calculate the rates of use of enforcement 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, as well as to provide insight in determining the effectiveness of Regional Entity programs and adequacy of Regional Entity and NERC resources.

²⁷ NERC provides feedback, guidance, and training to the Regional Entities. In 2015, the ERO Enterprise provided training to Regional Entity staff and the industry on areas such as compliance exceptions and the self-logging program. NERC developed this training based on early experience with implementing the programs, in addition to observations from the various reviews.

Other Significant 2015 Activities

Managing the Transition to Version 5 of the CIP Standards

The ERO Enterprise recognized 2015 as a critical year in ensuring registered entity preparation for the April 1, 2016, effective date of certain CIP Version 5 Reliability Standards requirements. To support implementation readiness during 2015, NERC focused its efforts in three key areas: written guidance and Reliability Standard Audit Worksheets (RSAWs) completion, stakeholder outreach, and ERO Enterprise staff workshops.

NERC worked with the Regional Entities and industry stakeholders through the transition advisory group²⁸ to finalize and issue documents that provide guidance to the industry on the implementation of various CIP Version 5 requirements. The ERO Enterprise and the transition advisory group have finalized eight lessons learned documents and 40 Frequently Asked Questions (FAQs). Table 3 below lists the completed lessons learned and FAQs.

Standard/Requirement	Topic
CIP-002-5.1 Requirement R1	FAQ #36: Considering misuse
CIP-002-5.1 Requirement R1 Attachment 1	FAQ #45: Generation and calculating 1500MW
	FAQ #49: Shared Systems
	FAQ #52: 15-minute impact
	FAQ #58: Addressing redundancy of systems
	FAQ #77: Tie line metering and dialup access
	FAQ #89: PACS and facility locations
	FAQ #53: Transmission scheduling systems
	FAQ #61: Controlling groups of generation
	FAQ #3-2014: Scoping UPS, HVAC and building control systems*
	Lesson Learned: Generation segmentation
	Lesson Learned: Far-end relay
	Lesson Learned: Generation interconnection
CIP-002-5.1	Lesson Learned: Mixed-trust EACMS
	Lesson Learned: Grouping of BES Cyber Systems
	Lesson Learned: Communications networking
CIP-003-6 Requirement R2	FAQ #23: IEC 61850 a routable protocol
CIP-004-6 Requirement R4 Part 4.1	FAQ #62: Applying "CIP Exceptional Circumstances" clause
CIP-004-6	FAQ #63: Granularity of training
	FAQ #64: Revoking access
	Lesson Learned: Managing vendor access
CIP-005-5 Requirement R1	FAQ #80: Applying dial-up connectivity controls
	FAQ #21: PCAs and non-routable communications
	FAQ #81: ESPs and stand-alone networks
	FAQ #76: Firewalls and Electronic Security Perimeters
	Lesson Learned: External Routable Connectivity

²⁸ Roster for the transition advisory group is available at http://www.nerc.com/pa/CI/Documents/V5TAG_Roster_070815.pdf.

Table 3: Completed CIP Version 5 Transition Lessons Learned and FAQs	
Standard/Requirement	Topic
CIP-005-5 Requirement R2	FAQ #73: Intermediate Systems
CIP-006-6 Requirement R1	FAQ #83: Protecting cables between ESPs
	FAQ #86: Using different physical security controls
	FAQ #91: Monitoring access to physical access controls
CIP-006-6 Requirement R3	FAQ #90: Testing physical access controls
CIP-007-6 Requirement R1	FAQ #94: Signage for physical port protection
CIP-007-6 Requirement R3	FAQ #1-2014: Malicious code and detective controls*
	FAQ #98: Malicious code controls
CIP-007-6 Requirement R5	FAQ #92: Identifying default or generic accounts
	FAQ #93: Password safe
	FAQ #101: Password only access
CIP-010-2 Requirement R1	FAQ #107: Baseline testing
	FAQ #114: New requirements for testing of BCAs
CIP-010-2 Requirement R3	FAQ #108: Vulnerability Scanning
	FAQ #68: ICS vulnerabilities
	FAQ #111: Penetration testing
	FAQ #112: Sampling methods for vulnerability assessments
CIP-010-2	FAQ #113: Test environments
	FAQ #2-2014: Verifying vendor testing adequacy*
CIP-011-2	FAQ #128: Protecting BCS information
	FAQ #129: Redeployment or reuse of devices
	FAQ #130: Destruction of data practices

*The FAQ numbering convention changed after these FAQs were identified by date.

On March 13, 2015, NERC issued revised RSAWs for CIP Version 5 and incorporated any new revisions to the standards as a result of standards development completed in 2015. ERO Enterprise CIP compliance monitoring staff and the standards drafting team for the CIP V5 revisions project regularly met during Q1 of 2015 to comprehensively review and update the CIP RSAWs to increase clarity and improve the industry's understanding of compliance expectations for both newly modified requirements and previously approved language.

In addition to developing written guidance for registered entities during the transition period, NERC and the Regional Entities focused heavily on information outreach and training during 2015. Specifically, 2015 events included Regional Entity workshops for registered entities, more individualized outreach through Small Group Advisory Sessions, and visits through the Security Reliability Program, in addition to several CIP-focused CMEP training activities for Regional Entity staff. Figure 9, in the previous section "Industry Stakeholder Information and Outreach" includes Regional Entity outreach events on the CIP Version 5 transition.

While NERC has continued its efforts to accomplish the goals of the CIP Version 5 Transition Program and entered its final stage of completing remaining guidance for outstanding topics in 2015, a focused effort has been underway to design an ERO Enterprise-wide oversight plan for 2016. NERC understands that the implementation of CIP Version 5 represents a significant shift in addressing cybersecurity. As the industry gains implementation experience with this new set of Reliability Standards, NERC's oversight of CIP Version 5 will rely on risk-based compliance monitoring and enforcement concepts. In particular, focus in 2016 will be on key areas to determine how well security risk is being managed, with emphasis on effective collaboration across the ERO Enterprise and

industry to address security and compliance. NERC and the Regional Entities will incorporate that focus in phased approaches based on function and risk throughout 2016 and beyond. NERC's oversight plan for CIP Version 5 in 2016 includes three primary components.

The first component includes on-site audit engagements in each Region at certain registered entities that could have a significant impact on the reliable operation of the Bulk Electric System (BES), identified through risk assessment and as otherwise required to occur on a three-year cycle under the NERC Rules of Procedure. Second, through the risk-informed application of risk-based compliance monitoring tools (e.g., spot checks and guided self-certifications), NERC and the Regional Entities will seek to understand from applicable registered entities the quantities of facilities that possess high- and medium-impact BES Cyber Systems in CIP-002. The third component of the CIP Oversight Program may involve oversight of certain responsible entities' CIP programs by NERC in conjunction with staff from Applicable Governmental Authorities.

Physical Security Reliability Standard Implementation

The ERO Enterprise and industry have always made the reliability and security of the BPS a key priority. Industry stakeholders have decades of experience working to protect our shared infrastructure and are constantly reevaluating threats and taking steps to protect the system. Standards are one piece of this complex, dynamic endeavor of providing a comprehensive approach to reliability.

With CIP-014-2 becoming effective on October 1, 2015, NERC and the Regional Entities focused on implementation readiness for applicable registered entities during 2015. NERC released a guidance communication to the Regional Entities and industry in February 2015 on implementation of Requirements R1 and R2.²⁹ That communication included a link to a guidance document developed by the North American Transmission Forum (NATF) for Requirement R1.³⁰ Importantly, NERC recognizes that there may be more than one approach to achieving compliance with CIP-014-2's requirements, so NERC is neither "adopting" nor "endorsing" a specific approach as the only way to comply with the standard. Initially, NERC provided guidance for each requirement. In response to suggestions received in response to the NERC Board of Trustees request for policy input on CIP-014-1 for the May 7, 2015, NERC recognized the importance of limiting and coordinating any additional guidance. NERC thus limited its initiation of formal guidance communication though it will continue to coordinate with other industry groups, such as the NATF, on their efforts.

ERO Enterprise staff began in 2015 to engage with registered entities through a variety of outreach activities and coordinated site visits to discuss and understand their implementation of CIP-014-2. Based on initial observations from both NERC and Regional Entity staff, the industry made significant progress towards effective CIP-014-2 implementation and compliance. Physical security plans appeared to be focused on mitigating risk from specific threats to the critical stations or substations, and NERC was encouraged by the industry's initial progress and continued focus on a successful CIP-014-2 implementation.

The ERO Enterprise will monitor compliance to the standard in a manner that emphasizes assessing and supporting effective implementation.³¹ The focus areas through the end of 2015 and during early 2016 relate to CIP-014-2's requirements to identify critical stations and substations and ensuring that such identifications are appropriate and risk-informed. NERC, in collaboration with the Regional Entities, plans to confirm who the Reliability Standard applies to, whether each of those applicable registered entities performed a required risk assessment to

²⁹ <http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Memo%20to%20the%20ERO%20021015.pdf>

³⁰ <http://www.natf.net/wp-content/uploads/NATF-CIP-014-1-R1-Guideline-V1-Open.pdf>.

³¹ Prior guidance from February 9, 2015, related to the risk assessment and third party verifications required by the Reliability Standard also emphasized that compliance assurance activities will expect registered entities to be able to demonstrate that they implemented the requirement effectively. That guidance is available at <http://www.nerc.com/pa/CI/PhysicalSecurityStandardImplementationDL/CIP-014%20Memo%20to%20the%20ERO%20021015.pdf>.

determine whether they have critical facilities, and whether that required risk assessment resulted in the identification of critical facilities.³²

In Q2 of 2016, NERC and the Regional Entities will prioritize understanding of effective application of the first three requirements related to critical facility identification.³³ This approach is described in the 2016 ERO Enterprise CMEP Implementation Plan with formal notices to applicable registered entities expected to be provided by Regional Entities in Q1 of 2016.

Regional Entity Coordinated Oversight of Multi-region Registered Entities

In 2014, the ERO Enterprise developed a comprehensive coordinated oversight program. The program is designed to streamline risk assessment, compliance monitoring, and enforcement for the registered entities that use, own, or operate assets in areas covering more than one Regional Entity's territory.

Under the program, Regional Entities coordinate their oversight responsibilities over MRREs by designating one or more LREs to each MRRE or a group of MRREs. The LRE is selected based on reliability considerations and the registered entity's operational characteristics. The selected LRE works collaboratively with the remaining Regional Entities, known as AREs, and informs NERC of activities as appropriate.

The program was implemented in phases to facilitate learning and process development by the ERO Enterprise. During Q2 of 2014, notice was provided to select MRREs of the opportunity to request coordinated oversight. This initial phase resulted in approximately 74 registered entities (24 MRRE groups) participating in coordinated oversight. In Q2 of 2015 a full implementation phase of the program began with a broad notice to registered entities that any MRRE could request to participate in coordinated oversight. In response, registered entities demonstrated significant interest in the efficiency and consistency benefits of the program. In Q3 of 2015, the participation level increased to 152 registered entities (39 MRRE groups), over twofold from the initial phase of the program. The ERO Enterprise has selected the LREs for each participating MRRE group, and the LREs and AREs have already signed memoranda of understanding outlining their respective responsibilities. Figure 11 represents the distribution, including number and percentage of the total, of 152 MRREs by LRE, and Figure 12 represents the distribution of MRREs by registered function. The registered entities that opted to join the program are registered for various reliability functions in multiple regions.

NERC and the Regional Entities held several outreach events on coordinated oversight before and during the full implementation period including an industry webinar in Q2 of 2015. Additional outreach to non-participating MRREs was also provided. Finally, Program overview, contact information, and other documents are posted on NERC's website and updated regularly.³⁴ This program requires ongoing and timely communication, full sharing of information, and opportunity for ARE input and involvement concerning implementation of the CMEP for those MRREs involved in the program. Detailed procedures between LREs and AREs for implementing the program are key to the success of the program.

³² These confirmations are also intended to address quarterly reporting expectations to the Board of Trustees in support of its monitoring of the standard's implementation. NERC management, per the Board of Trustees' instruction when adopting the Physical Security Reliability Standard, will monitor and assess implementation of CIP-014-2. This monitoring includes the general number and characteristics of assets identified as critical and the scope of security plans developed to meet the requirements in CIP-014-2, including the timelines provided for implementation of the various security and resiliency measures included in the plan.

³³ The obligations of those requirements become effective through staggered enforcement dates beginning on October 1, 2015, through Q1 of 2016.

³⁴ Information on the Coordinated Oversight of MRREs Program is available at <http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/MRRE%20FAQ%20with%20Notice%201-12-15.pdf>.

In support of CCC Criteria, during 2016, the ERO Enterprise will continue to consider opportunities to refine the coordinated oversight program and to improve associated efficiency and consistency while also fulfilling obligations for implementation of the CMEP. Also, there will be organized efforts to continue to provide outreach on the coordinated oversight program and in particular to seek feedback from registered entities involved in the coordinated oversight program concerning any process improvements.

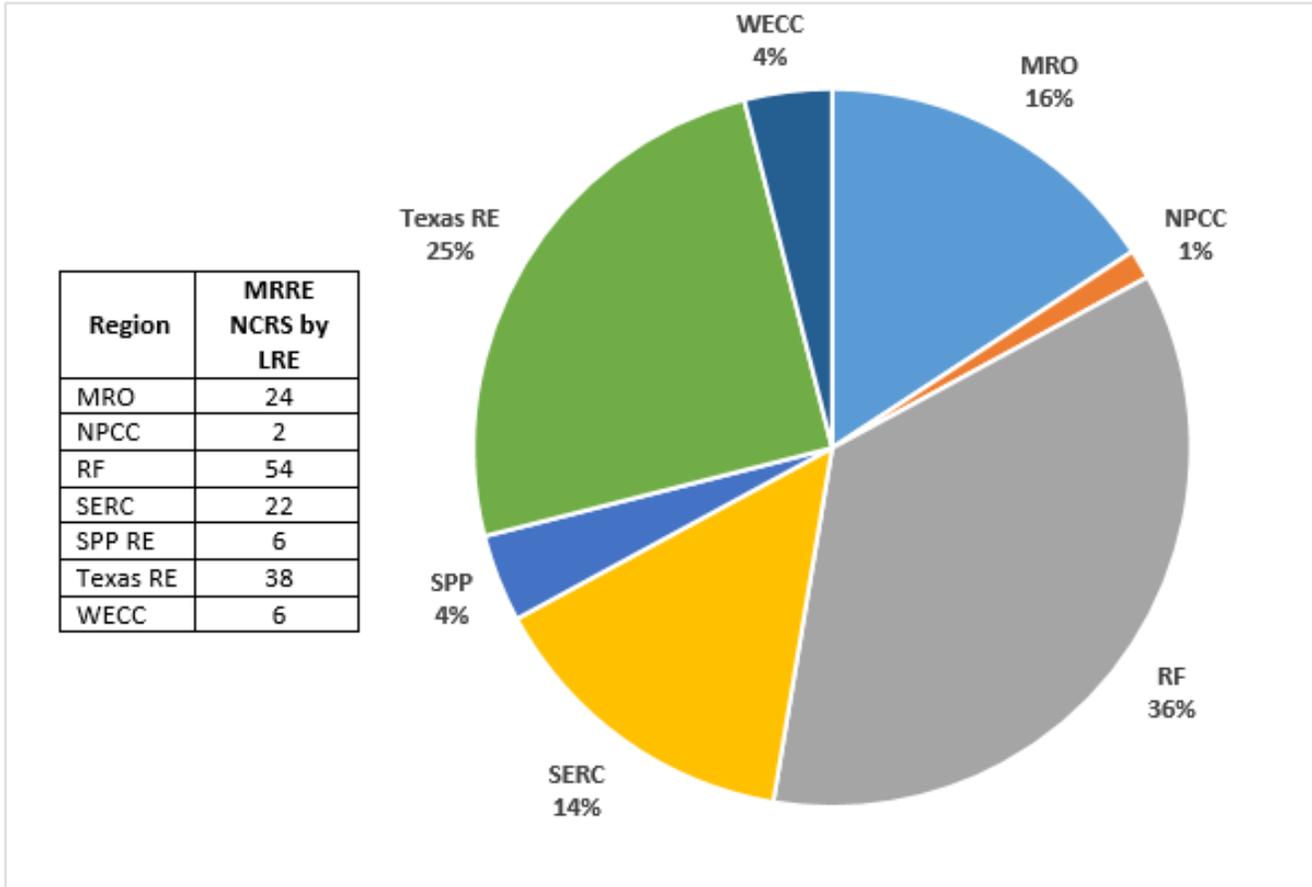


Figure 11: Number of MRRE NCRs by LRE and Regional Percentage of Total MRRE NCRs

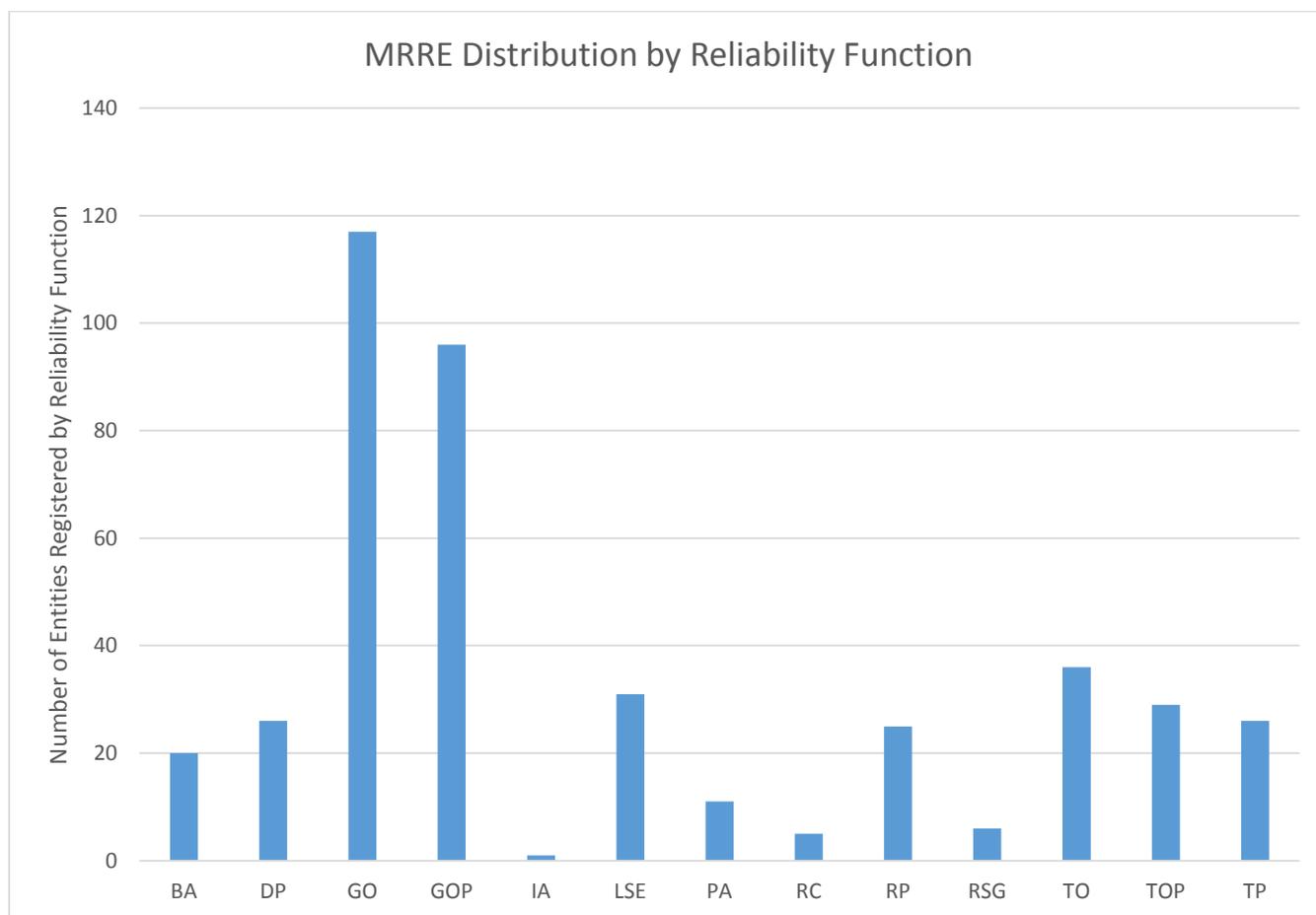


Figure 12: MRRE Distribution by Reliability Function

Regional Consistency Tool

The ERO Enterprise is committed to ensuring and promoting consistency among the Regional Entities and with applicable published processes, procedures, and rules. To assist the ERO Enterprise in its efforts to improve consistency among the Regional Entities and drive continuous improvement in day-to-day operations, the Regional Entities created the Regional Consistency Reporting Tool. This reporting tool allows registered entities or other relevant industry stakeholders to report any perceived inconsistency in the methods, practices, or tools of two or more Regional Entities.

The Regional Consistency Reporting Tool does not function as an appeal of a Regional Entity action or decision, and it does not replace the NERC or Regional Entity Compliance Hotlines for complaint reporting.

The Regional Consistency Reporting Tool is hosted on a secure, [third-party server](#). Reports are submitted only to those personnel at each Regional Entity who have specific permissions and training based on the issue.

Once a report is received, the Regional Entity will assess and evaluate the report. The evaluation reports will then be incorporated into a public findings spreadsheet. The identity of the reporter, if provided, will always remain protected. The reporter has the option to remain anonymous when making the report.

To improve consistency among the Regional Entities and drive continuous improvement in day-to-day operations, the Regional Entities also developed the Regional Consistency Reporting Tool as an additional channel of communication for registered entities and relevant industry stakeholders. The tool allows the public to report any

perceived inconsistencies among Regional Entities, including perceived inconsistencies with compliance monitoring and enforcement processes, procedures or rules. In 2015, 20 reports of perceived inconsistencies were submitted through the Regional Consistency Reporting Tool.³⁵ These 20 reports represent a diverse category of issues involving, among others, compliance monitoring, CMEP tools, event analysis, organization registration and BES asset identification. The majority of these reports involve substantive issues—with a handful involving administrative issues, such as inconsistent data transmittal methods from registered entities to Regional Entities. Out of these 20 reports, 13 have been successfully investigated and resolved; 3 have been assigned to ERO staff working groups for longer-term tracking and resolution; and 4 cases are in-process.

³⁵ Detailed information on the reported issues and findings is located on the NERC website, available at <https://secure.ethicspoint.com/domain/media/en/gui/38901/index.html>. In addition, this information is also posted on the Regional Entities websites.

Looking Ahead to 2016

To refine and align risk-based CMEP with the lessons learned from the implementation year, the ERO Enterprise identified three areas of focus going forward. The ERO Enterprise will focus on the following: (1) collaborating through NERC and Regional Entity working groups to share best practices to achieve successful implementation; (2) sharing best practices for risk assessments of registered entities to enhance consistency and common approaches; and (3) continuing emphasis on stakeholder understanding and perceptions.

To guide compliance monitoring and enforcement 2016 activities, NERC has identified the following priorities for the ERO Enterprise:

- Regional entity completion of initial IRAs for all BAs, TOPs, and RCs during 2016;
- ERO Enterprise completion of a plan for conducting initial IRA activities of all remaining registered entities by Q2 of 2016;
- Continued NERC and Regional Entity coordination on risk-based compliance monitoring, specifically:
 - Refining of risk elements and risk factor considerations to better prioritize risks and identify registered entity specific risks;
 - Evaluating ERO Enterprise IRA and ICE business rules;
 - Promoting consistency in ERO Enterprise IRA and ICE tools and processes; and
 - Improving training on IRA and ICE performance for ERO Enterprise staff.
- ERO Enterprise support of CIP Version 5 transition and Physical Security implementation through an ERO Enterprise monitoring approach, as outlined in the 2016 ERO Enterprise CMEP Implementation Plan;
- NERC coordinated review of compliance exceptions and FFTs with FERC; and
- ERO Enterprise review of self-logging program.

Appendix

This appendix includes an update on the ERO Enterprise processing-related goals and metrics in 2015 and other relevant trends.

Mitigation Completion Status

The ERO Enterprise actively tracks mitigation of noncompliance through Mitigation Plans and mitigation activities. NERC also conducts oversight of the Mitigation Plan processes and procedures to identify deficiencies and establish best practices.

During Q4 of 2014, NERC conducted a review of 120 Mitigation Plans submitted to FERC in 2013. The purpose of the Mitigation Plan review was to evaluate the Regional Entities' internal procedures and practices related to Mitigation Plan review and acceptance, certification, and verification. The review was a supplement to NERC's ongoing review of all Mitigation Plans, which are accepted by the Regional Entities and submitted to NERC for approval before they are submitted to FERC.

Based on its analysis of the review results, NERC concluded that the Regional Entities follow the procedural and content requirements of the CMEP as they relate to mitigation activities associated with noncompliance with the NERC Reliability Standards. During 2015, NERC observed improvement across the ERO Enterprise related to the description of interim risk mitigation and cause analysis in Mitigation Plans.

NERC is closely monitoring noncompliance for which mitigation has not been completed. The ERO Enterprise encourages all registered entities to submit timely and detailed certifications of completion of Mitigation Plans or mitigation activities.

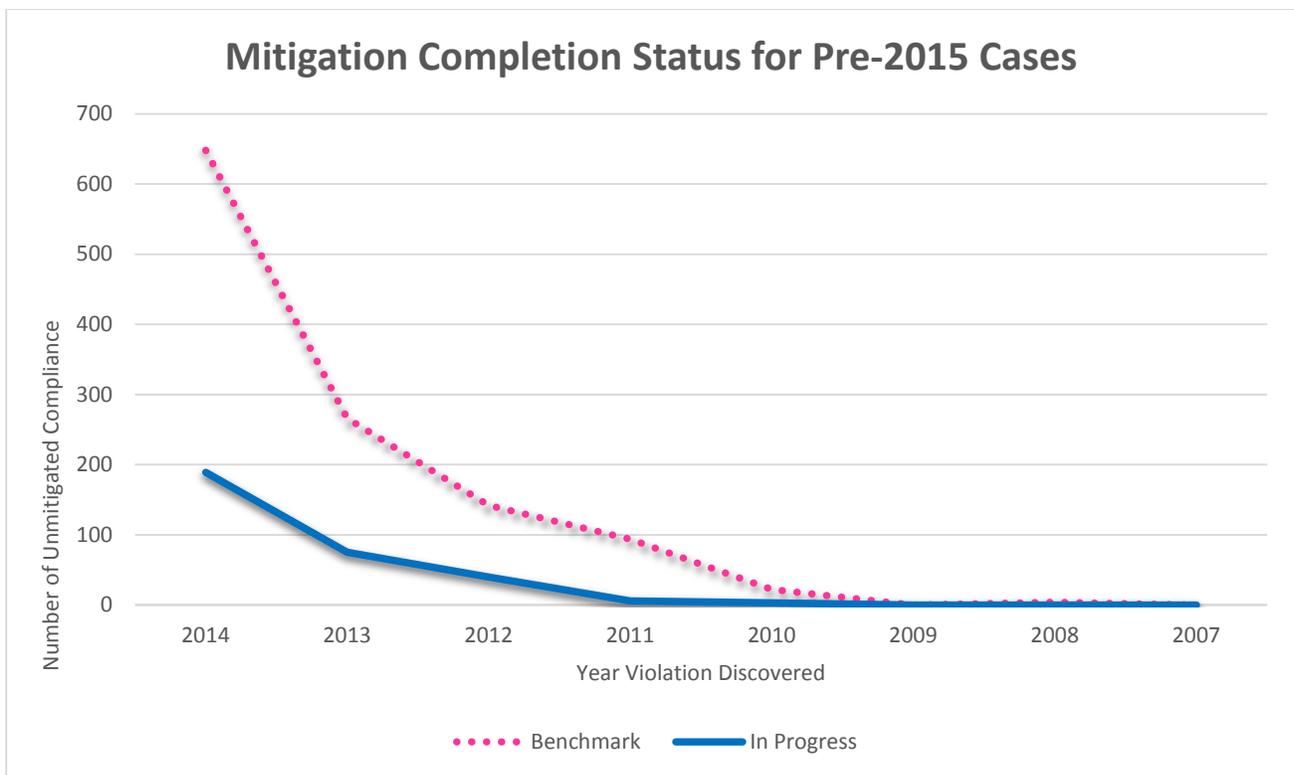


Figure 13: Mitigation Completion Status by Discovery Year

The outstanding mitigation activities from 2010 and before largely involve federal entities that have had limited interaction with their Regional Entities during the pendency of federal litigation related to NERC’s ability to assess financial penalties against federal entities. Since the litigation has been resolved in 2014, the Regional Entities have made significant progress in working with the federal registered entities to resolve their noncompliance and associated mitigation.

As of Q4 of 2015, mitigation has been completed for 80.39% of the instances of noncompliance discovered in 2014, which is an increase from 67.90% in Q3 of 2015. NERC met its target of 80% completion of noncompliance discovered in 2014.

The table below shows the ERO Enterprise’s targets and thresholds for mitigation activity completion by discovery year of the noncompliance.

Time frame	Required Mitigation	On going	Progress toward the goal	Threshold	Target
2010 and older	4182	3	99.93%	98%	100%
2011	1742	6	99.66%	95%	98%
2012	1461	40	97.26%	90%	95%
2013	1157	75	93.52%	75%	80%
2014	964	189	80.39%	75%	80%

Self-Assessment and Identification of Noncompliance

The ERO Enterprise monitors noncompliance discovery trends and promotes self-identification of noncompliance. The ERO Enterprise has set a target that the registered entities should discover 75% of noncompliance in 2015 through internal discovery methods. In 2015, registered entities self-identified 84% of the instances of noncompliance, resulting in an 8% increase over 2014. Typically, registered entities identify a higher percentage of noncompliance in the first quarter of each year when they conduct internal compliance evaluations and submit self-certification forms to the Regional Entities. In all quarters of 2015, the percentage of internally discovered instances of noncompliance was higher compared to the same periods in 2014. In Q4 of 2015, the registered entities self-identified 86.8% of noncompliance internally, compared to less than 72% in Q4 of 2014. All four quarters of 2015 identified more internally discovered noncompliance than any other compared year.³⁶

Registered entities’ ability to self-identify noncompliance allows for timely mitigation of such noncompliance, which results in a more timely reduction of risk to the BPS. The ERO Enterprise continues to encourage all registered entities to develop internal processes that would allow them to promptly self-identify and mitigate instances of noncompliance.

³⁶ Consistent with a decline in the overall number of instances of noncompliance, self-identified or not, the number of reported instances of noncompliance has been on the decline since 2011. In 2011, there were 2,618 total violations discovered; in 2014, there were 1,190; and in 2015, there were 840 violations discovered.

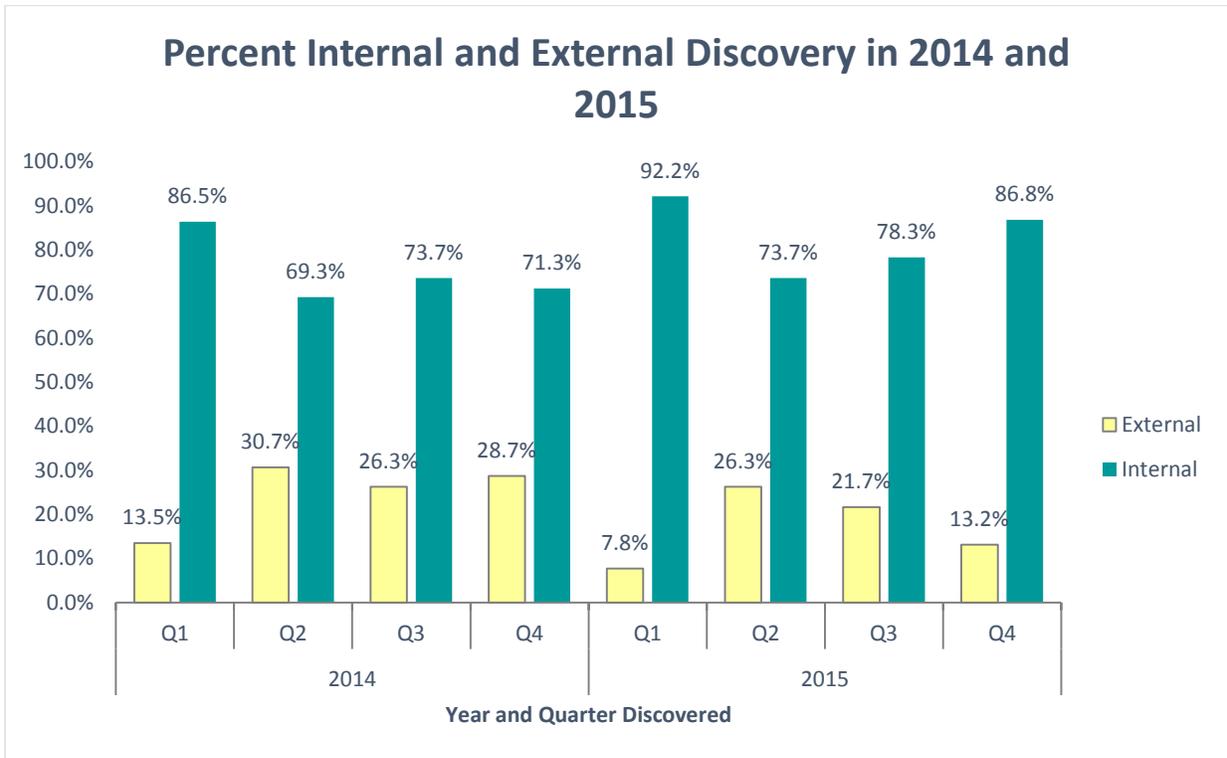


Figure 14: Internal Discovery Increased in 2015 Compared With the Prior Year

Noncompliance Processing Metrics

ERO Enterprise’s Pre-2014 Caseload

The ERO Enterprise monitors several measures that relate to the processing of open violations from prior years. Older pre-2014 violations have been a priority for both the Regions and NERC. In 2015, this increased focus continued to be successful as the non-federal entity pre-2014 noncompliance inventory continued to decline, dropping to 44, which is less than the threshold of 65 that was set for 2015.

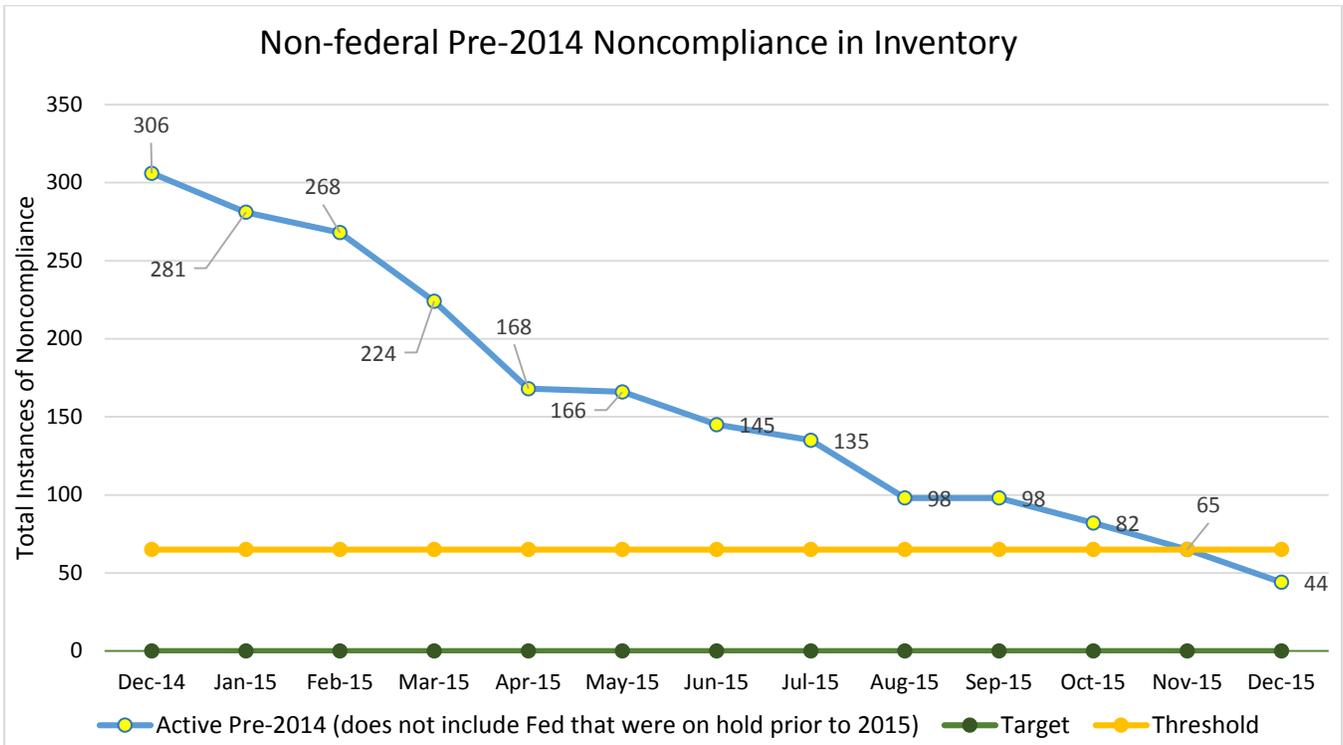


Figure 15: Non-federal Pre-2014 Noncompliance in Inventory Continues to Decline

The inventory for instances of noncompliance related to federal entities is also declining mainly because Regional Entities are currently processing these cases, which were on hold for several years. In Q4 2015, there were no federal entity noncompliance processed but this number is expected decline dramatically in 2016, starting with a high number of violations scheduled for Q1 2016. The majority of federal entity noncompliance relates to large agreement that should be resolved in Q1 2016. Once completed, NERC anticipates a more substantial decrease in the federal entity inventory.

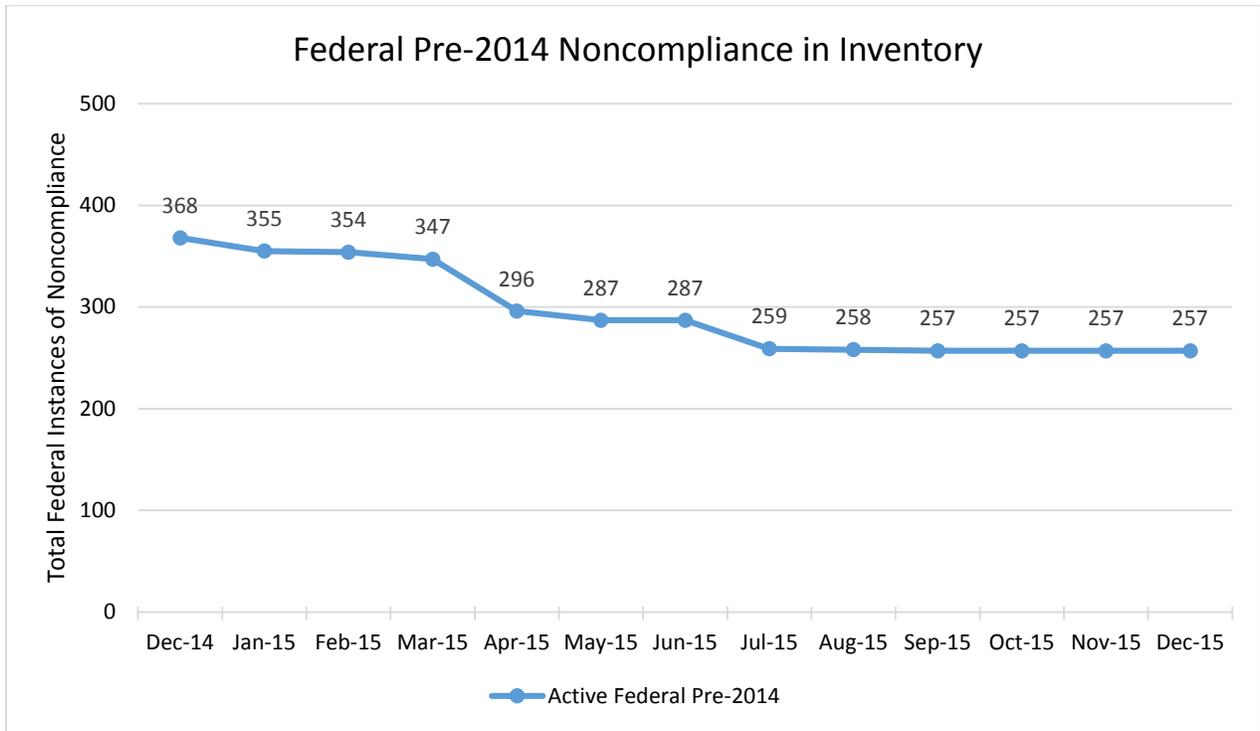


Figure 16: Federal Pre-2014 Noncompliance in Inventory Started Declining in 2015

Average Age of Noncompliance in the ERO Enterprise by Month

The average age of noncompliance continues to fluctuate but remains well below the threshold.

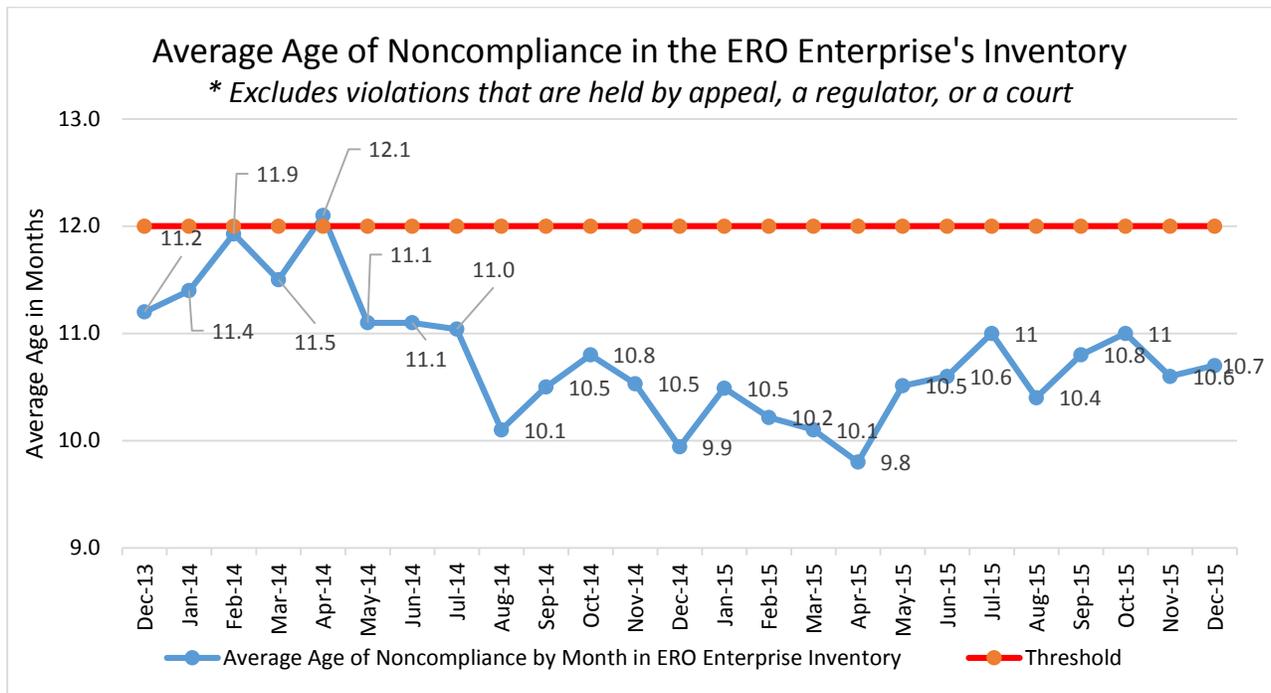


Figure 17: Average Age of Noncompliance in ERO Enterprise's Inventory

Since all Regional Entities began applying the Compliance Exception and FFT disposition tracks to qualifying minimal and moderate risk violations, the average processing time has declined. As shown in Figure 19 below, more than 60% of the inventory of noncompliance for the ERO Enterprise is less than one year old, and only 6% is over two years old.

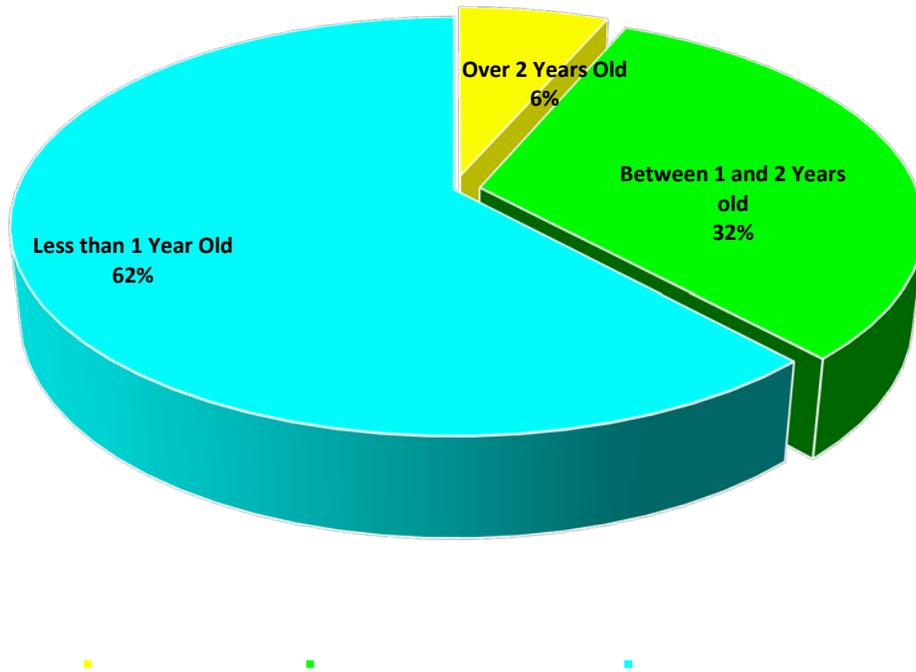


Figure 18: Age of Noncompliance in ERO Enterprise's Inventory

APPENDIX B

Phase One NERC Oversight Closeout Report

Phase One NERC Oversight Closeout Report

Regional Entity Risk-based Compliance Monitoring Implementation and IRA and ICE Alignment Reviews

June 23, 2015

Purpose

NERC's Compliance Assurance department (Compliance Assurance) previously documented a two-phased oversight plan for evaluating Regional Entity alignment with, and application of, the recently developed ERO Enterprise risk-based compliance monitoring guidance documents for the Inherent Risk Assessment (IRA) and Internal Control Evaluation (ICE) (IRA and ICE Guides).¹

Phase one oversight activities focused on ensuring conceptual alignment of each Regional Entity's processes to the guidance documents during the 2015 implementation year. Phase one oversight activities concluded in June 2015. This closeout report provides:

1. Summary of phase one oversight activities
2. Initial implementation accomplishments
3. Current alignment efforts
4. ERO Enterprise improvement recommendations
5. Next steps and phase two NERC oversight

Summary of Phase One Oversight

Phase one oversight activities revealed that Regional Entities have made great strides in demonstrating initiative in developing processes and tools to implement risk-based compliance activities. Additionally, Regional Entities are working to remediate alignment issues and incorporate NERC oversight recommendations. For example, some Regional Entities are developing plans to prioritize and complete initial IRAs for all registered entities in their footprint, outside the traditional three and six year audit cycles, as well as formalizing processes and procedures for conducting IRAs and ICEs. However, opportunities remain in other areas, such as processes used to revise or re-perform IRAs and ICEs outside the initial IRA and ICE conducted.

Further, and as seen in the quarterly collection and reporting of metric data, limited ICE activities are occurring across the ERO Enterprise and opportunities exist to mature ICE processes as well as the way Regional Entities use ICE as part of an overall compliance monitoring plan. NERC and the Regional Entities need to continue to assess where ICE improvements can be made, in both communication and training, to help build the ICE program. Continued dialogue with registered entities and data flows between NERC and Regional Entities will allow for the ERO Enterprise to effectively demonstrate the progress that is being made in overall implementation.

¹ Refer to NERC Compliance Assurance Oversight Plan 2015.

Phase one activities also identified, with input from Regional Entity staff, ERO Enterprise opportunities for guidance clarifications, development or enhancement of tools, and training that support joint efforts for successful implementation of IRA and ICE processes.

Phase One Oversight Background

Compliance Assurance compiled alignment criteria from the IRA and ICE Guides prior to conducting oversight activities at each Regional Entity’s site during the first and second quarters of 2015. Using the alignment criteria, Compliance Assurance walked through each Regional Entity’s IRA and ICE processes and assessed their degree of alignment with the criteria. NERC rated the Regional Entities’ processes as Fully Aligned, Partially Aligned, and Not Aligned. In many cases, due to the initial implementation status of IRA and ICE, the Regional Entity’s IRA or ICE processes as Compliance Assurance documented and described may not have yet been fully implemented. Accordingly, some Regional Entities were assessed on conceptual alignment as documented or described and not on whether such practices were actually fully implemented or documented. Compliance Assurance worked with Regional Entities to map process workflows and timelines to clearly illustrate and understand key components of Regional Entity IRA and ICE processes and tools. In addition to assessing alignment with the IRA and ICE Guides, oversight activities revealed other opportunities for IRA and ICE process improvements, enhanced IRA and ICE tools, guidance, and training across the ERO Enterprise.

NERC and the Regional Entities communicate regularly to ensure continued momentum on implementation efforts. NERC and Regional Entity staff have recurring monthly calls to discuss implementation of any recommendations, progress in remediation of any nonalignment issues, and general implementation efforts occurring throughout the year. ERO Enterprise staff also participate in bi-weekly calls to continue discussions on implementation concerns, lessons learned, and guidance needs.

Onsite Activities

Oversight teams consisted of a Compliance Assurance lead auditor and support staff. Compliance Assurance augmented its oversight teams by outsourcing support services in an effort to complete the phase one oversight activities more efficiently and effectively. In order to ensure a consistent approach, all the Compliance Assurance personnel that led engagements attended the first two onsite engagements. FERC also attended three onsite oversight engagements with the purpose of understanding Regional Entity processes and implementation of IRA and ICE. Table 1 below shows oversight engagements along with the oversight teams and observers.

Table 1: Oversight Engagement Summary		
Regional Entity	Site Visit Date	Oversight Team (OT) and Observers
RF	January 27-29, 2015	5 NERC staff (OT), 1 FERC staff (Observer)
Texas RE	March 9-11, 2015	4 NERC staff (OT)
FRCC	March 24-26, 2015	2 NERC and 3 Augmenters (OT)

SPP RE	April 14-16, 2015	2 NERC and 3 Augmenters (OT)
WECC	April 21-23, 2015	1 NERC, 2 Augmenters (OT), and 1 FERC staff (Observer)
SERC	May 12-14, 2015	1 NERC and 2 Augmenters (OT)
NPCC	May 26-28, 2015	2 NERC and 2 Augmenters (OT)
MRO	May 26-28, 2015	1 NERC and 2 Augmenters (OT)

Compliance Assurance drafted an initial Regional Entity oversight report following the conclusion of each onsite visit. Regional Entities received the draft report and had at least one week to review and provide feedback, which was ultimately incorporated into a final report issued to each Regional Entity.

Phase One Alignment Results Summary

For IRA alignment results, all eight Regional Entities were either fully or partially aligned with all alignment criteria reviewed. Similarly for ICE, six Regional Entities were either fully or partially aligned with all alignment criteria. For the remaining two Regional Entities, one Regional Entity was fully aligned with all but one ICE criterion and one Regional Entity did not have a documented ICE process ready for evaluation.

Compliance Assurance truly appreciates all the thought and hard work demonstrated by the Regional Entities in implementing IRA and ICE in such a short period of time. All of the Regional Entities have made great strides in implementing IRA and ICE processes that are in accordance with the ERO Enterprise guides, and the observations noted in this report serve only to enhance the effectiveness and efficiencies of those processes. Compliance Assurance would also like to thank the Regional Entities for their time spent walking through their processes and answering questions.

Initial Implementation Accomplishments

Phase one oversight activities identified Regional Entity processes and tools that appear to provide additional effectiveness and/or efficiencies in the implementation of risk-based compliance activities. Some Regional Entities, although at differing stages of implementation, demonstrated initiative in developing tools and processes to assist in performance of IRA and ICE. The tools and processes highlighted below include some of the Regional Entity initiatives that, with verification, could maximize efficiencies and encourage successful implementation of risk-based compliance activities. The following are some examples:

- FRCC, WECC, SERC, and MRO each created and used tools that link Reliability Standards to established risk factors. These Regional Entities are able to automatically generate a scope for any given registered entity based on the relevant risk factors and the registered entity's information. The tools provide efficiency in the Regional Entity's ability to conduct a risk factor analysis and confirm applicable Reliability Standards relating to risk factors and risk-based scoping determinations. The tools support a repeatable and consistent process while allowing for professional judgment in determining a registered entity's oversight scope.

- NPCC implemented a standardized, coded list of rationale for including a Reliability Standard or Requirement in the compliance monitoring scope. This process facilitates consistency in risk assessment and scoping across registered entities and also creates process efficiencies through the transfer of organizational knowledge between the personnel performing the IRAs. Further, this process supports NPCC's documentation protocols and conclusions for a registered entity's oversight scope.
- RF developed a reporting capability to identify macro-level Bulk Power System (BPS) risks within its footprint along with the registered entities affecting those risks. This macro-level analysis informs RF's IRA process currently and could potentially be used to prioritize the IRAs that are performed along with the related compliance oversight plans.
- WECC and FRCC each developed a tool to facilitate the evaluation of registered entity's internal controls. The tools describe the internal controls, the procedures performed to evaluate them, and the results of the evaluation. The use of this tool helps meet the professional auditing re-performance standard that documentation should exist in sufficient detail to allow an experienced auditor to reach similar conclusions, as well as the documentation expectations outlined in the ICE Guide.
- NPCC developed three ICE templates to facilitate the gathering of internal control information from registered entities based on their size, functional registrations, and the sophistication of their control processes. The templates range from simply providing specific internal controls for specific Reliability Standards to organizing controls based on general risks. These ICE templates could help identify internal controls related to the entity's specific BPS risks and support a tailored requests for information from the registered entity when considering internal controls and control environment.
- All Regional Entities created some form of targeted questionnaires to solicit risk and general information from registered entities.

Current Alignment Efforts

Compliance Assurance identified alignment opportunities and collaborated with the Regional Entities to remediate issues and improve overall IRA and ICE programs. The following is a summary of the most significant alignment issues currently being addressed by the Regional Entities. Each Regional Entity received individualized feedback on region-specific areas within their alignment reports.

Following phase one oversight, Regional Entities are doing the following activities:

- Developing a plan to prioritize and complete initial IRAs for all registered entities in their footprint. Regional Entities are executing IRAs based on the traditional three- and six-year audit cycles to support initial implementation but should begin planning and prioritizing IRAs based on analysis of the registered entity's risk to the BPS in its area and include milestones for the completion of IRAs for all registered entities within their footprint within a reasonable timeframe.
- Considering processes to revise, or criteria that would trigger a re-performance of, IRAs and ICEs outside the initial IRA and ICE conducted. As the IRA and ICE processes mature, Regional Entities will need to be able to revise IRAs and ICEs to determine scope and monitoring to effectively tailor compliance oversight plans to account for new, emerging, or unique information about the

registered entity or risks to the reliability of the BPS. Discussions will occur across the ERO Enterprise for best approach for determining possible IRA triggers.

- Enhancing IRA and ICE procedures to formally document and support processes for completing IRA and ICE.
- Reviewing and vetting existing IRA and ICE automated tools to ensure integrity and security of information and the accuracy of calculations and results.

ERO Enterprise Improvement Recommendations

The primary objective of 2015 is to ensure successful implementation of risk-based compliance activities. To meet this objective, NERC and the Regional Entities continue to collaborate and demonstrate implementation progress throughout the year. The phase one alignment review revealed significant progress and accomplishments across the ERO Enterprise in achieving this objective.

In addition to the alignment observations noted for the Regional Entities, Compliance Assurance, with input from Regional Entity staff, noted opportunities for the ERO Enterprise to clarify guidance, enhance tools, and provide training to continue the successful implementation of IRA and ICE processes.

The list identified below includes significant areas that Compliance Assurance recommends for consideration of possible actionable projects by NERC and the Regional Entities during 2015 and 2016. The recommendations below should be discussed and vetted among NERC and Regional Entity staff to determine whether actions, if any, are needed. Compliance Assurance recommends that NERC and the Regional Entities jointly review this list, prioritize each of the items, and determine appropriate actions to continue enhancements during 2015 and 2016.

General Opportunities and Recommendations

NERC and the Regional Entities should consider the following:

1. Developing a more formalized NERC and Regional Entity feedback process that could enhance knowledge sharing across the ERO Enterprise and ultimately improve IRA, ICE, and Reliability Standards over time. Some informal feedback processes regarding risk-based compliance monitoring currently exist, but a more formal approach would clarify expectations for feedback in the aforementioned areas.
2. Developing ERO Enterprise templates, or updating the current IRA Summary Results template, for ICE results and compliance oversight plans to help communicate consistent results to registered entities.
3. Developing a common database for registered entity information that will serve as a repository to be shared across the ERO Enterprise.
4. Editing the IRA and ICE Guides to ensure consistency of terms as well as other minor updates identified throughout the course of the year.

IRA Opportunities and Recommendations

NERC and the Regional Entities should consider the following:

5. Reviewing and updating IRA Appendix C, Risk Factors, to incorporate Regional Entity lessons learned from performing IRAs during 2015.
6. Developing a universal mapping of Risk Factors to Reliability Standards among the Regional Entities in order to standardize the relationship among risk to the BPS, Reliability Standards, and compliance monitoring scope across the ERO Enterprise. The mapping should allow for regional customization, but an initial mapping would facilitate a more consistent approach to risk assessment.
7. Consider developing a single, standardized IRA tool for inter-regional use. The single tool could combine certain effective elements of the automated tools used currently by several of the Regional Entities which would promote consistency in approach across the regions. Developing a common form/tool to facilitate the gathering of information and data from registered entities when conducting IRAs.

ICE Opportunities and Recommendations

NERC and the Regional Entities should consider the following:

8. Developing guidance regarding integration of ICE with the IRA and the timing of ICE relative to the IRA.
9. Developing an ERO Enterprise template to facilitate the gathering of internal control information from registered entities.
10. Providing evidence examples and common tools to facilitate the evaluation of internal controls such as an inventory of controls for specific Reliability Standards and work plans to assess control design and effectiveness. The tools can also address information requests and documentation requirements related to evaluating internal controls.

Training Opportunities

NERC and the Regional Entities should consider the following areas for training:

11. How to identify events and circumstances that could potentially trigger the re-performance of an IRA.
12. How to identify and evaluate key controls during an ICE, as well as explain the benefits and purpose of ICE beyond a possible audit scope reduction.
13. How to develop a monitoring plan for the Regional Entity beyond the traditional three and six year audit cycles and considers registered entity oversight plans. The training should inform how ERO Enterprise and Regional Entity risks help prioritize and determine when a registered entity's IRA occurs.

Next Steps and Phase Two NERC Oversight

Next steps for risk-based compliance monitoring implementation involve continued collaboration and joint efforts by NERC and Regional Entities to support risk-based compliance improvements, guidance development, and staff training to achieve a steady state for risk-based compliance monitoring.

Phase two oversight activities involve Compliance Assurance monitoring of Regional Entity implementation of phase one recommendations, as well continuing to monitor and evaluate Regional Entity risk-based compliance implementation and practical application of the IRA and ICE Guides, focusing on the areas identified above. Phase two oversight continues throughout the remainder of 2015. Following phase two oversight activities, which focuses on risk-based compliance implementation, NERC will transition to steady-state oversight model based on lessons learned from oversight of implementation activities. Compliance Assurance will follow the established ERO Enterprise Oversight Program for Compliance Monitoring, designed to encompass program design and development, operational oversight and leadership, coaching and support, and ongoing assessment with feedback to the corresponding regional programs.² The phase two oversight approach will outline objectives, detailed evaluation criteria, scope, methodology, and milestones. Compliance Assurance plans to circulate the documented phase two approach with the Regional Entities to ensure continued collaboration in support of the successful implementation of risk-based concepts. Table 2 below provides a preliminary timeline and milestones for NERC Compliance Assurance for the remainder of 2015. The timeline and milestones below may change based on future activities and finalization of NERC’s phase two oversight approach of risk-based compliance implementation.

Table 2: Preliminary Timeline and Milestones for NERC Compliance Assurance Activities (Subject to Change)

Milestone Description	Estimated Completion Date
Provide summary of Phase One Oversight Activities to ERO Compliance Monitoring Group (CMG) and obtain feedback on phase one report.	July 2, 2015
Begin discussions with ERO CMG and prioritization of ERO Enterprise improvement recommendations contained within phase one closeout report.	June 2015-July 2015
Complete phase two NERC oversight approach and circulate with Regional Entities through the ERO CMG. Obtain and incorporate feedback.	June 2015-July 2015
Provide phase two NERC oversight approach to ERO EMG for discussion at July 2015 ERO EMG meeting.	July 24, 2015
Explore all 13 recommendations with NERC and Regional Entities to vet, prioritize, and determine appropriate action, if any.	July-August 2015

² NERC and the Regional Entities are coordinating in the design and development of the ERO Enterprise Oversight Program for Compliance Monitoring, with anticipated completion date of year-end 2015.

Begin preliminary phase two oversight activities (TBD in phase two oversight approach)	August 2015
Prepare Phase Two Oversight Closeout Report or Provide Status Update Report on phase two activities	December 2015
Implement ERO Enterprise Oversight Program for Compliance Monitoring ³	Beyond December 2015

³ *Id.*