NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 16, 2015

VIA OVERNIGHT MAIL

Doreen Friis
Regulatory Affairs Officer/Clerk
Nova Scotia Utility and Review Board
3rd Floor
1601 Lower Water Street
P.O. Box 1692, Unit "M"
Halifax, Nova Scotia B3J 3S3

RE: *North American Electric Reliability Corporation*

Dear Ms. Friis:

The North American Electric Reliability Corporation ("NERC") hereby submits Informational Filing of the North American Electric Reliability Corporation. NERC requests, to the extent necessary, a waiver of any applicable filing requirements with respect to this filing.

Please contact the undersigned if you have any questions.

Respectfully submitted,

/s/ Holly A. Hawkins

Holly A. Hawkins
Associate General Counsel for the North American Electric Reliability Corporation

Enclosure

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

BEFORE THE
NOVA SCOTIA UTILITIES AND REVIEW BOARD
THE PROVINCE OF NOVA SCOTIA

NORTH AMERICAN ELECTRIC	**)**
RELIABILITY CORPORATION	**)**

INFORMATIONAL FILING OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The North American Electric Reliability Corporation ("NERC") hereby submits, for informational purposes, a description of the various processes and programs developed and deployed through the ERO Enterprise's[1] Reliability Assurance Initiative ("RAI"). The initiative was developed to implement across the ERO Enterprise a risk-based compliance monitoring and enforcement program ("CMEP")[2] that provides reasonable assurance of reliability through compliance monitoring, appropriate deterrence through enforcement, and a feedback loop to improve Reliability Standards.

The processes and programs described herein are fully consistent with existing NERC Rules of Procedure and authority and the Federal Energy Regulatory Commission's ("FERC") rules, orders, and regulations.

[1] The term "ERO Enterprise" refers to NERC and the eight Regional Entities. The eight Regional Entities are Florida Reliability Coordinating Council ("FRCC"), Midwest Reliability Organization ("MRO"), Northeast Power Coordinating Council ("NPCC"), ReliabilityFirst ("RF"), SERC Reliability Corporation ("SERC"), Southwest Power Pool Regional Entity ("SPP RE"), Texas Reliability Entity ("Texas RE"), and Western Electricity Coordinating Council ("WECC").

[2] As the context requires, "CMEP" refers to the compliance monitoring and enforcement program or the document found at Appendix 4C of the NERC Rules of Procedure, which contains the rules associated with such program.

Section II of this filing describes the context for the development of the initiative. It discusses in summary form, the process of developing the risk-based approach to compliance monitoring and enforcement. Finally, the section describes the oversight and training programs established by the ERO Enterprise to ensure appropriate and consistent application of the processes discussed herein.

Section III of this filing describes the enhancement of a feedback loop between compliance monitoring and enforcement and other activities, including the development of Reliability Standards.

Section IV of the filing describes compliance monitoring processes, as well as the regulatory framework that allows implementation of these processes. This section discusses the identification and prioritization of risk elements, the inherent risk assessment ("IRA"), and internal controls evaluation ("ICE") processes, and the development of compliance oversight plans for registered entities including the planning and execution of Compliance Audits.

Section V of the filing discusses the processes associated with a greater exercise of enforcement discretion by the ERO Enterprise, specifically the use of compliance exceptions and self-logging of minimal risk issues.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

RAI was a collaborative effort among NERC, the Regional Entities, and industry to identify and implement changes to enhance the effectiveness of compliance monitoring and enforcement. Essentially, the initiative resulted in the adoption of a risk-based approach to compliance monitoring and enforcement. This approach benefits reliability by focusing resources applied to compliance monitoring and enforcement based on risk, thereby allowing the ERO Enterprise and registered entities to focus appropriate time and effort on higher-risk issues. As the reliable operation of the bulk power system ("BPS") is in the public interest, the focusing, by the ERO Enterprise on matters that pose greater risk to that reliable operation is also in the public interest. This approach does not equate to ignoring lesser-risk issues, which, as explained in this filing, continue to be identified, corrected, and tracked.

A risk-based approach is fully consistent with NERC's existing rules and authority, as demonstrated below. Further, this approach focuses on how the ERO Enterprise performs oversight and obtains assurance regarding compliance with Reliability Standards and does not create new or additional requirements (beyond those established in Reliability Standards) for registered entities operating the grid. However, this approach has the benefit of allowing the ERO Enterprise to leverage certain management practices in use at registered entities in focusing its own oversight activities. This ability to leverage management practices also has the effect of disseminating and enhancing such practices throughout industry.

The ERO Enterprise is implementing the new processes described in this filing fully in 2015. By the end of 2015, the ERO Enterprise expects to measure the success of this initiative in

a number of ways, including through measures related to staff competencies, robustness of outreach, program transparency, and sharing of best practices.

As the ERO, NERC has the oversight authority, responsibility, and obligation to monitor Regional Entities' adherence to the NERC Rules of Procedure, specifically the CMEP, and performance of their delegated responsibilities on behalf of NERC. NERC will continue its oversight activities to ensure consistency throughout the ERO Enterprise in identification of risks and evaluation of processes, procedures, and internal controls, as well as the assessment of risks associated with noncompliance and mitigation. NERC oversight of all components of the risk-based CMEP will be essential to the proper application of the program over the long-term.

Through implementation of the risk-based approach described in this filing, the ERO Enterprise also will strengthen the trust of the applicable governmental authorities in the ERO Enterprise's risk-based compliance and enforcement. An appropriate level of transparency will be in place for various facets of risk-based compliance monitoring and enforcement, balancing efficiency and the confidentiality needs of a registered entity with the needs of industry as a whole to learn from others.

II. DEVELOPMENT OF THE RELIABILITY ASSURANCE INITIATIVE

In 2012, the ERO Enterprise initiated a multi-year effort to identify and implement changes that enhance the effectiveness of the CMEP. The experience of the past several years demonstrates that a one-size-fits-all and zero tolerance approach to compliance monitoring and enforcement does not properly allocate time, attention and resources for serious and lesser risk noncompliance, does not demonstrably equate to more reliable operations of the BPS, and is not sustainable. In fact, the risk-based approach outlined herein is more likely to ensure the reliable

operation of the BPS. The case for a risk-based approach to compliance monitoring and enforcement has been previously outlined in a NERC white paper, *Incorporating Risk Concepts into the Implementation of Compliance and Enforcement*.[3]

Over this time, the ERO Enterprise tested, through various pilot programs, a number of concepts, processes, and programs to develop a risk-based compliance monitoring framework and a risk-based enforcement program. This experience is described below.

A. Compliance Pilot Program

The ERO Enterprise compliance pilot program focused on the development and implementation of approaches to risk assessments and testing of internal controls. The purpose of the compliance pilot program was to develop a single, common ERO Enterprise approach to compliance monitoring, focusing on risk-based assessments, scoping, internal controls review concepts, and tests of controls. Specific outcomes from the pilot program included proposed processes and methods for conducting inherent risk assessments of a registered entity and evaluating internal controls.

NERC and the Regional Entities initiated phase one of the pilot program during 2013. This phase explored different approaches to applying risk-based auditing concepts. In phase one, five Regional Entities designed pilots that included various approaches to audit scoping, inherent risk assessments, and testing of internal controls related to Reliability Standards. Regional Entities worked with registered entities to identify entity-specific risks and related internal

[3] *See* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/White%20Paper%20–%20The%20Need%20for%20Change%20(paper%201).pdf.

controls to scope an audit and assess compliance with the Reliability Standards in scope. Both Regional Entity and registered entity representatives involved in the pilots provided feedback on the pilot approaches.

The second phase of the pilot program evaluated the pilot results. Representatives from each of the eight Regional Entities reviewed pilot results and identified specific approaches or processes that the ERO Enterprise should use for its single, common method for compliance monitoring. Converging the various approaches into a single design began in January 2014 and included a detailed review of each pilot and presentation of each individual Regional Entity pilot design to an evaluation team during February 2014. The evaluation team consisted of an independent audit consultant and senior NERC, Regional, and industry representatives. To assist the evaluation team in determining the best approach, NERC and the Regional Entities invited a group of industry professionals to help develop criteria to evaluate the various approaches. The established criteria included transparency, design effectiveness, alignment to Reliability Standards, implementation requirements, and registered entity impact.

The third and final stage of the pilot program, beginning in June 2014, was finalizing the single, common approach to inherent risk assessments and internal controls evaluations. During the final stage, two smaller teams of NERC and Regional Entity staff designed guidance documents to provide an overall framework for how Regional Entities would conduct inherent risk assessments and internals control evaluations. The teams used the pilot results and evaluation criteria to finalize guidance documents. The two design teams coordinated with industry representatives to obtain input into the development and content of the guidance

documents. Additionally, the NERC Board of Trustees requested policy input from industry on the draft inherent risk assessment guidance, which the final guidance documents incorporated.

As explained below, the new processes developed through RAI associated with the compliance monitoring program have resulted in the development of a common framework for oversight of registered entities based on the identification of risk elements, assessment of an entity's inherent risk, and evaluation of its internal controls. Each of these components allows the Compliance Enforcement Authority ("CEA")[4] to select the appropriate monitoring tools on the basis of risk. The framework is based on the use of risk-based compliance monitoring practices similar to those utilized in other industries. The focus, method, and frequency of monitoring engagements are based on a common ERO Enterprise approach to assessing a registered entity's risk to the reliability of the BPS and may be further refined based on the strength of the registered entity's management controls related to compliance with Reliability Standards.

B. Enforcement Activities

Recognizing the opportunity for risk-based enforcement improvements, in parallel with the risk-based compliance activities referenced above, the ERO Enterprise began to transition away from a process-driven enforcement strategy to a proactive, risk-based strategy that defines, communicates, and promotes desired entity behavior in an effort to improve the reliability of the BPS. Specifically, this approach allows the ERO Enterprise to focus on the higher risks to the

[4] "Compliance Enforcement Authorities" or "CEAs" refer to NERC or the Regional Entity in their respective roles of monitoring and enforcing compliance with the NERC Reliability Standards.

reliability of the BPS, providing clear signals to registered entities about identified areas of concern and risk prioritization, while maintaining the ERO Enterprise's existing visibility into potential noncompliance issues regardless of the level of risk they posed. This approach also encourages the self-identification of noncompliance and enhancement of internal controls by registered entities. NERC and the Regional Entities worked together to develop a series of activities designed to further align enforcement processes with risk and to increase the transparency regarding the ERO Enterprise's assessment of the risk to the BPS posed by specific instances of noncompliance.

The ability of CEAs to arrive at a final determination with respect to all noncompliance in an efficient manner is in part dependent on the quality of the information they have about the noncompliance and related mitigation. With that in mind, NERC and Regional Entity staff prepared self-report[5] and mitigation plan[6] user guides. These user guides build on guidance previously available from NERC and the Regional Entities and explain, among other things, the type and quality of information that should be submitted with a self-report and mitigation plan in order to allow for a prompt evaluation and, as appropriate, prompt disposition of noncompliance (in particular, of noncompliance that posed a minimal risk to the reliability of the BPS).

[5] *ERO Self-Report User Guide* (April 2014), *available at*: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf.
[6] *ERO Mitigation Plan Guide* (April 2014), *available at*: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Mitigation%20Plan%20Guide%20(April%202014).pdf.

The ERO Enterprise also addressed concerns regarding timeliness of resolution of minimal risk issues and communication through the adoption of a triage process. As of January 1, 2014, all Regional Entities implemented a triage process. On average, within 60 days of discovery, regardless of discovery method, the CEA reviews noncompliance and determines whether: (i) there is enough information to support treating the noncompliance as a compliance exception; (ii) more information is required prior to determining the disposition; or (iii) the noncompliance needs to be enforced.

Finally, the ERO Enterprise developed additional processes to allow the continued streamlining of the resolution of minimal risk noncompliance, in particular that which is self-identified.

The Find, Fix, Track and Report ("FFT") program was the first step in implementing a risk-based strategy that recognizes that not all instances of noncompliance require the same type of enforcement process. The natural evolution of the FFT program includes the ability to exercise greater discretion, including by declining to initiate an enforcement action to resolve an instance of noncompliance that did not pose a serious or substantial risk to the reliability of the BPS. The ERO Enterprise developed two new processes to achieve this goal: the self-logging program and the use of compliance exceptions. Both are discussed in greater detail below.

The ERO Enterprise's risk-based approach generally reserves enforcement actions under section 5.0 of the CMEP for those issues that pose a higher risk to the reliability of the BPS. As to issues posing a lesser risk, NERC and the Regional Entities may exercise appropriate discretion whether to initiate a formal enforcement action or resolve the issue outside of the formal enforcement processes. 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. Finally, this approach improves reliability by acknowledging and encouraging the enhancement of internal controls and self-identification and mitigation of noncompliance by registered entities. Visibility and accountability is maintained because noncompliance that is not enforced is nevertheless mitigated, tracked for analytical purposes, and subject to oversight by NERC as discussed herein.

This approach is not new. Many enforcement agencies in the United States, including FERC, exercise discretion in addressing noncompliance with the regulations they administer and establish priorities for the allocation of their resources. Such enforcement agencies also acknowledge and reward management practices associated with the self-identification and mitigation of noncompliance by regulated entities.[7] The processes described herein build on the

[7] *See* John C. Moot, *Compliance Programs, Penalty Mitigation and the FERC*, 29 Energy Law Journal 547, 562-563 (2008) discussing a Securities and Exchange Commission ("SEC") action forgoing enforcement because "the company had quickly identified the violations, promptly reported them, remedied them internally through disciplinary actions, and taken prospective corrective action to avoid future violations." *See also id.* at 564-65 *citing, Environmental Protection Agency, Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations*, 65 Fed. Reg. 19,618 (2000), which discusses the EPA's policy on *Incentives for Self-Policing, Discovery, Disclosure, Correction and Prevention of Violations,* which provides "[t]he revised Policy … is designed to encourage greater compliance with Federal laws and regulations that protect human health and the

success of the FFT program, the ERO Enterprise's well-established process for differentiating the resolution of noncompliance based on the risk posed to the reliability of the BPS.

C. From Design to Implementation

The basic framework design for all of these processes was concluded with the posting of program documents and guides on the RAI page of the NERC website in September and October 2014.[8] As discussed below, the ERO Enterprise is continuing to develop tools and templates, and is continuing to perform oversight, in order to obtain assurance that CEAs are implementing the new processes appropriately and consistently. The ERO Enterprise also has strengthened the communication and outreach regarding the processes and program and developed a robust training program.

With the completion of the design, reflected in the various published guides discussed below, and the baseline training provided to ERO Enterprise staff, the program is ready to be implemented in 2015. Over time, and through NERC's oversight of the program, areas that require additional guidance and training will be identified and addressed (either in the form of

---

environment. It promotes a higher standard of self-policing by waiving gravity-based penalties for violations that are promptly disclosed and corrected, and which were discovered systematically-that is, through voluntary audits or compliance management systems." *See also* Orly Lobel, *Interlocking Regulatory and Industrial Relations: The Governance of Workplace Safety,* 57 ADMIN. L. REV. 1071, 1105-08 (2005) for a discussion of the Occupational Safety and Health Administration ("OSHA") "star" status program, under which OSHA can exempt employers from routine inspections and allow them to claim "star" status in exchange for maintaining exemplary safety records and satisfying other program certification requirements. The pursuit of "star" status improves employee safety and health, decreases regulatory costs, and enhances an entity's reputation.

[8] The RAI page is available at: http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

revised guides or through other means). In identifying such areas, NERC will consider the feedback from FERC staff, Regional Entities, registered entities, and other stakeholders. This iterative review cycle provides the most effective means of quickly adapting to specific implementation challenges.

1. Increased Outreach and Communication

Communication and education also are essential to the successful implementation of the risk-based compliance monitoring and enforcement approach. In recognition of this fact, the ERO Enterprise has significantly increased its stakeholder outreach efforts in the second half of 2014. Outreach efforts have taken a number of forms, including workshops, webinars, newsletters, and other communications.

A significant milestone associated with the outreach and communication efforts was the formation, in September 2014, of an advisory group composed of stakeholders representing diverse Standing Committee, Regional, and regulatory perspectives. The advisory group was based on the successful experience of other ERO Enterprise initiatives and provided input and advisory guidance to NERC and Regional Entity staff as it finalized the design of the various components of the risk-based approach to compliance monitoring and enforcement. Currently the advisory group provides assistance on RAI-related outreach and training to the industry, including the format and agenda for the workshops described below.

In November, 2014, the ERO Enterprise hosted two industry outreach workshops (on November 6, 2014 in Atlanta, GA and November 20, 2014 in Phoenix, AZ). The topics and agenda were the same for each event. At each workshop, a panel of participants from Regional Entities and stakeholder companies discussed their experiences and expectations about the

components of risk-based approach to compliance monitoring and enforcement. Discussion on the panels also included the application of the risk-based concepts to version 5 of the CIP Reliability Standards. The workshops were designed to foster practical conversations on how risk-based compliance monitoring and enforcement will look and feel to registered entities as the ERO Enterprise implements this approach in 2015.

NERC also conducted webinars to help disseminate information on the new processes.[9] In particular, an "RAI 101" webinar was held on October 3, with over 150 attendees, and presenters from NERC and several Regional Entities. The presentation and recording are also available on the NERC RAI page under "RAI Workshops and Webinars."

In the second half of 2014, NERC also increased its communication efforts associated with the initiative through individual announcements of relevant milestones, and spotlights of recent developments regarding RAI in its weekly and monthly publications. These materials have been distributed to broad distribution lists by email and are also posted on the NERC RAI page under "Program News."

2. Oversight by NERC

Oversight is essential to the long-term success of the compliance monitoring and enforcement program. Oversight ensures consistency in identification of risks and evaluation of processes, procedures, and internal controls, as well as the assessment of risks associated with

[9] A schedule of stakeholder outreach opportunities is available at: http://www.nerc.com/pa/comp/Documents/RAI%20Schedule.pdf.

noncompliance and mitigation. The, ERO Enterprise is currently developing measures of success to evaluate the risk-based approach to compliance monitoring and enforcement.

As part of its oversight role, NERC uses a combination of review processes to ensure that CEAs are implementing the CMEP effectively, to provide constructive feedback where appropriate, to identify trends, and to drive the implementation of best practices. In developing a comprehensive oversight plan, NERC has built, and will continue to build, on its experience overseeing CEAs on matters that involve the exercise of professional judgment. NERC's oversight of and involvement with the Regional Entities' compliance monitoring and enforcement activities are not limited to an after-the-fact determination of the quality of a Regional Entity's performance relative to a given process. NERC will regularly report on the results of its oversight, including performance as measured by certain key metrics, at its board meetings.

Regarding the compliance monitoring activities, NERC conducted Regional Entity reviews during the first quarter of 2015 with the intent of supporting conceptual consistency in the application of the ERO Enterprise's risk-based approach. Throughout 2015, NERC's oversight will begin to evolve into a more traditional evaluation to assess areas supporting consistency in implementation of the guidance documents and providing feedback on opportunities for greater consistency. During 2015, NERC will focus on samples of Regional Entity IRAs, ICEs, and other aspects of the Framework that utilized the new risk-based approaches.

Regarding the enforcement activities, NERC will continue to perform oversight on an ongoing basis through three main categories of activities: analysis of data and metrics, annual

spot checks of various programs, and dissemination of guidance and training. NERC oversight focuses on identifying areas for improvement in the future, rather than reopening closed matters. NERC prepares analyses and reports to assist with monitoring of CMEP processes for consistency and reasonable assurance of reliability, and to help identify trends that may affect BPS reliability. As an example, NERC analyzes repeat violations as well as new violations reported. Analysis of new violations helps identify significant violations that may adversely affect BPS reliability. Performance indices are also computed on a regular basis to quantify the performance of the Regional Entities and NERC in processing violations and mitigation and to provide insight in determining the effectiveness of regional programs and adequacy of regional and NERC resources. Additional detail regarding NERC oversight of the self-logging and compliance exceptions programs is included below.

NERC also collaborates closely with FERC staff on oversight. A current example of such collaboration is the joint review of the FFT program through a combined annual spot check.

NERC oversight of all components of the risk-based compliance monitoring and enforcement program will be essential to the proper application of the program over the long term.

3. Continuous Training

As the design of RAI is completed, dissemination of guidance and training continues to be an integral component of ongoing CMEP implementation and in support of progressive consistency across the ERO Enterprise. To consistently implement the risk-based compliance oversight framework ("Framework") and its components in 2015, NERC is collaborating with a

group of Regional Entity leaders to develop multiregional training covering all of the ERO Enterprise staff.

A NERC and Regional Entity core group of presenters has provided training to ERO Enterprise staff in a number of different venues. First, the group presented to auditors, enforcement and risk staff at the ERO Auditor Workshop in September, 2014. The presentations covered all aspects of the risk-based approach to compliance monitoring and enforcement, based on the near final versions of the various program documents available at the time.

This group is also implementing a phased program to provide more focused training to the staff performing IRAs and ICEs. Phase one of the training will address the implementation of the IRA and ICE guides, focusing first on regional staff that will actually perform IRAs and ICEs. Specifically, NERC and the Regional Entity leaders held three two-day sessions with Regional Entity staff in November and December, 2014. As noted above, to ensure consistency in training and approach, there is a core group of NERC-led presenters and trainers composed of both NERC and Regional Entity staff. The majority of the ERO Enterprise staff performing IRAs and ICEs committed to attending the in-person training sessions and all staff will be trained. The training included the discussion of hypotheticals and case studies developed based on the existing guides. This training was completed in December 2014.

Phase two will involve a reevaluation of guidance documents, development of lessons learned, and reevaluation of training needs. NERC and the Regional Entities will continue to assess training needs throughout 2015 and revise existing and ongoing training to incorporate Framework concepts.

Additional information on training is provided below, in connection with the discussions of Compliance Audits and enforcement processes. Training opportunities for industry, beyond those discussed in the context of outreach, above, are also in development.

4. Increased Coordination

Parallel to the adoption of a risk-based approach to compliance monitoring and enforcement, the ERO Enterprise is examining its practices associated with monitoring and enforcement for entities located in more than one Regional Entity footprint. There is an ongoing effort to enhance the coordination among Regional Entities for the execution of the compliance monitoring and enforcement processes defined in CMEP. These efforts include a more defined structure and transparency for such coordination. Initial results are expected to be available in 2015.

III. FEEDBACK LOOP FOR THE IMPROVEMENT OF RELIABILITY STANDARDS

The ERO Enterprise will factor the knowledge and information gained through the implementation of these new policies into future revisions of existing NERC Reliability Standards to improve their content and clarity. NERC will also use that knowledge and information in the evaluation of patterns that may indicate potential reliability gaps or risks. The ERO Enterprise will use these trends in determining appropriate approaches to address reliability risks, developing training and guidelines, completing reliability assessments, and performing other data-based analysis. This feedback will benefit both the ERO Enterprise and registered entities. In particular, the opportunities to analyze trends to identify and educate entities on reliability risks will facilitate the improved application of resources to minimize reliability risks to the BPS.

In addition to the Standards drafting process, NERC will also ensure appropriate information flows from compliance monitoring and enforcement to other NERC programs, including Reliability Assessment and Performance Analysis, Registration and Certification, and Event Analysis.

IV. RISK-BASED COMPLIANCE MONITORING

A. Regulatory Structure

Risk-based compliance monitoring is fully consistent with NERC's existing rules and authority and does not require a change in the fundamental tenets of the Rules of Procedure (including its Appendix 4C, the CMEP). The ERO Enterprise is implementing risk-based compliance monitoring in accordance with existing rules, regulations, and orders; the framework aligns the ERO Enterprise monitoring with specific requirements set out through the Generally Accepted Government Auditing Standards ("GAGAS") and Institute of Internal Auditors ("IIA")—standard monitoring practices used in various industries. In addition to the CMEP, referenced above, NERC's program for monitoring and enforcing compliance with Reliability Standards is implemented through the Sanction Guidelines (Appendix 4B to the Rules of Procedure) and delegation agreements with the eight Regional Entities.

As specified in section 4.1 of the NERC CMEP, NERC develops and posts an annual Compliance Monitoring and Enforcement Program Implementation Plan ("ERO CMEP IP") each year. The ERO CMEP IP is the annual operating plan for compliance monitoring and enforcement activities to ensure that NERC and the Regional Entities fulfill their responsibilities under applicable legislation.

Beginning with the 2015 CMEP IP and beyond, NERC replaced the approach used to develop the ERO CMEP IP and the Actively Monitored List ("AML") with processes that identify and prioritize continent-wide risks to the reliability of the BPS, as well as related

Reliability Standards and registration functional categories.[10] Specifically, the ERO determines risk elements, taking into account compliance findings and event analysis experiences, data analysis provided in several NERC publications and reports, and expert judgment of ERO Enterprise staff, committees and subcommittees. Examples of such data and reports include the State of Reliability Report, the Long-Term Reliability Assessment, publications from the Reliability Issues Steering Committee, special assessments or reports, the ERO Enterprise Strategic Plan, ERO Event Analysis Process insights, significant occurrences noted by NERC and Regional Entity Situation Awareness staffs, and other relevant documents pertaining to risks to the reliability of the BPS. This revised approach continues to identify a subset of NERC Reliability Standards and Requirements for monitoring purposes, but it provides input to the development of a more individualized compliance oversight plan for registered entities. Therefore, the transformation to focus on identifying and prioritizing risks replaces a static, one-size-fits-all list of Reliability Standards and prioritizes functions and Reliability Standards based on risk to determine the appropriate oversight method.

Regional Entities use the risk elements and other information identified in the annual ERO CMEP IP in developing their own individual annual Regional Entity implementation plans ("Regional Entity IPs"). Regional Entity IPs are based on a common template, developed by the ERO Enterprise, and include: (i) details on Regional Risk Assessment processes and results; (ii) Reliability Standards and Requirements associated with Regional Risk Assessment results; (iii)

[10] These processes are described in the Risk Elements Guide for the Development of the 2015 CMEP IP, *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_RiskElementsGuide_090814.pdf.

Regional compliance oversight plan, which includes its annual audit plan; and (iv) other key activities and processes used for CMEP implementation. NERC is evaluating the 2015 Regional Entity IPs that incorporate the risk elements outlined within the ERO CMEP IP for approval in accordance with section 4.2 of the CMEP.

The Rules of Procedure provide for seven compliance-monitoring processes, which are also referred to in this filing as CMEP tools (i.e., the main tools by which the monitoring program is executed). These methods include: (i) Compliance Audits; (ii) Self-Certifications; (iii) Spot Checks; (iv) Compliance Investigations; (v) Self-Reports; (vi) Periodic Data Submittals; and (vii) investigation of complaints. [11] The Rules of Procedure set forth steps for these methods, including requirements for the Regional Entity to report the results of the processes to NERC, which will then report to the applicable governmental authorities. The Rules of Procedure also specify the process steps after identifying registered entity noncompliance with a Reliability Standard.[12] These processes are unchanged. As discussed more fully below, all instances of noncompliance will continue to be reported and tracked at the Regional Entity, NERC, and FERC levels.

As explained below, the Regional Entity will determine the type and frequency of the compliance monitoring processes, or CMEP tools (e.g., off-site or on-site audits, spot checks or self-certifications), that are warranted for a particular registered entity based on reliability risks. The determination of the appropriate CMEP tools will be adjusted, as needed.

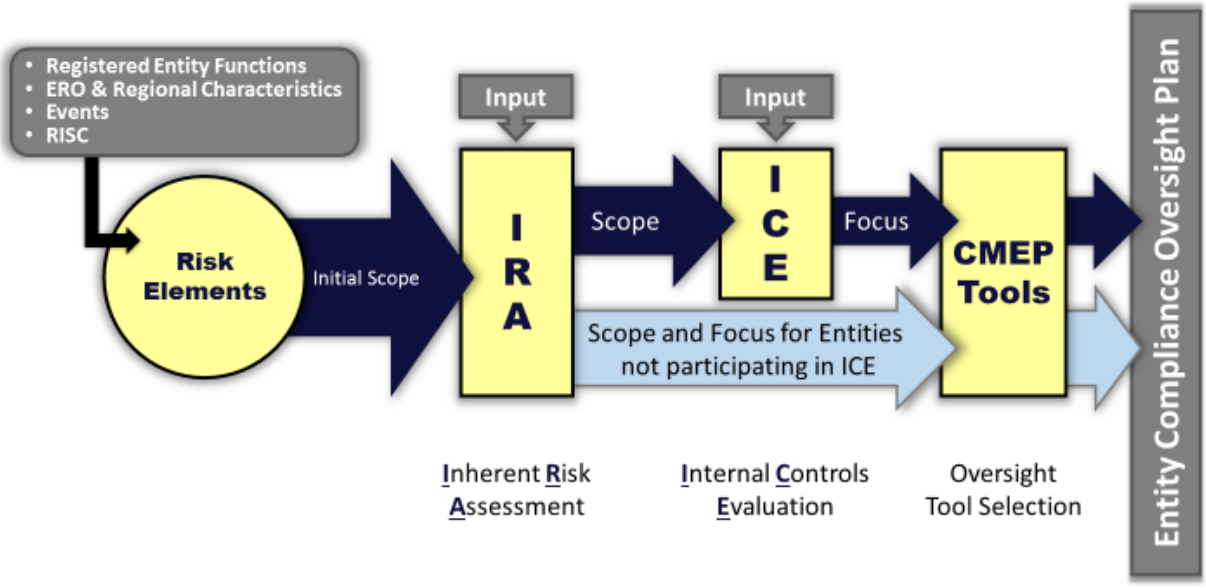
[11] CMEP §3.0 (Appendix 4C to the Rules of Procedure).
[12] *Id.* § 3.8.

In selecting CMEP tools, more resource-intensive compliance monitoring activities, particularly Compliance Audits, may be used for these and other functions or entities within a specific Regional Entity that can have the most significant impact on reliability of the BPS. Functional roles or entities that have a lesser impact on reliability to the BPS may have compliance monitoring approaches tailored accordingly, for example, the use of spot checks or self-certifications, instead of Compliance Audits, may be appropriate tools in such instances. Registered entities required to be audited at a minimum three-year interval per the NERC Rules of Procedure will continue to be audited at least once every three years,[13] although the actual frequency and scope will be determined based on the Framework.

B. Risk-Based Oversight Plan Framework

RAI resulted in the development of the Framework depicted below. The Framework illustrates a number of steps including the review of system-wide risk elements, the assessment of a registered entity's inherent risk, and, as applicable, the evaluation of a registered entity's internal controls. These steps allow each CEA to establish a monitoring plan that is tailored to the risk to the BPS posed by a particular entity or group of entities. As a result, the Framework allows the ERO Enterprise to focus its resources, as well as those of registered entities, on those areas that pose the highest risk and have the greatest potential to affect reliability. Each step of the Framework is more fully discussed below.

[13] NERC Rules of Procedure, § 403.11.1.



1. Risk Elements

The first step of the Framework consists of the identification and prioritization of ERO Enterprise-wide risks. Risks are identified and prioritized based on significance, likelihood, vulnerability, and potential impact to the reliability of the BPS through a process outlined in the Risk Elements Guide for the Development of the 2015 CMEP IP ("Risk Elements Guide").[14] Risks may be categorized as operational risks and planning risks, as well as threats to cyber systems or physical security. While risk identification occurs on an annual basis, risks are dynamic. Accordingly, periodic reviews and updates may be necessary and appropriate to address increased and emerging risks or in the alternative, to reflect mitigated risks.

[14] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_RiskElementsGuide_090814.pdf.

Through the review of the ERO Enterprise-wide risks, the ERO develops an annual compilation of risk elements reflected in the ERO CMEP IP.[15] The ERO CMEP IP serves as guidance to Regional Entities in the preparation of their Regional Entity IP. Any needed updates will be reflected in the ERO CMEP IP on a dynamic basis. The Regional Entity IPs are subject to review and approval by NERC as required in the Rules of Procedure.[16]

Reliability Standards are in place to help ensure the reliable operation of the BPS. Through the identification of risk elements, the ERO Enterprise maps a preliminary list of applicable Reliability Standards and responsible registration functional categories to the top reliability risks identified as areas of focus for monitoring purposes. This preliminary list is reflected in the ERO CMEP IP. As discussed above, this list and the processes used to identify and prioritize continent-wide risks to reliability of the BPS, as well as related Reliability Standards and registration functional categories, replaces the AML used in prior years.

The risks and associated Reliability Standards identified through the ERO CMEP IP and Regional Entity IP processes do not reflect the entirety of the risks that may affect the reliability of the BPS. As noted in the Risk Elements Guide, issues being addressed through other mechanisms are not included as areas of focus for compliance monitoring activities.

In order to focus on a complete picture of reliability risks when determining the appropriate compliance tool, Regional Entities then consider local risks and specific

[15] *Available at*: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_2015%20CMEP%20IP_V7_090814.pdf.
[16] NERC Rules of Procedure, § 402.1.1.

circumstances associated with individual registered entities within their footprints in developing their entity-specific compliance oversight plans. As a result, the scope of monitoring of a particular registered entity may include more, fewer, or different Reliability Standards than those outlined in the ERO and Regional Entity CMEP IPs.

2. Inherent Risk Assessment

After the ERO CMEP IP and Regional Entity IPs identify and prioritize risk elements, the IRA enables the CEAs to determine areas of focus and scoping of oversight for specific registered entities. As a result, the IRA identifies the Reliability Standards and Requirements that should be monitored.

The ERO Enterprise Inherent Risk Assessment Guide ("IRA Guide")[17] describes the process used to assess inherent risk of registered entities and serves as a guide for implementing and performing an IRA. As noted above, the ERO Enterprise is currently training to support the implementation and consistent application of the IRA process. In short, an IRA is a review of potential risks posed by an individual registered entity to the reliability of the BPS. An IRA considers factors such as assets, systems, geography, interconnectivity, prior compliance history, and overall unique entity composition. In considering such factors, a Regional Entity is not limited by the risk elements identified in the ERO CMEP IP. Rather, the IRA considers multiple factors to focus oversight to entity-specific risk. These factors may include the functional role

[17] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO_Enterprise_Inherent_Risk_Assessment_Guide_20141010.pdf.

and responsibilities of a registered entity. Risks may differ based on an entity's size, types of facilities, location, or the entity's assets, as applicable. An entity's system geography, population, and seasonal/ambient conditions may affect potential risk to reliability, as will BPS exposure (transmission, generation, and operating limitations), and interconnection points and critical paths. The existence or nonexistence of certain systems like Special Protection Systems, Undervoltage Load Shedding, Underfrequency Load Shedding, Supervisory Control and Data Acquisition ("SCADA"), and Energy Management Systems may reduce or increase exposure of the BPS to entity-specific risks. In addition to the physical systems and assets of an entity, an entity's past operational performance and compliance and enforcement history informs the IRA's selection of appropriate oversight tools.

While the IRA Guide provides guidance on risk factors and associate criteria/thresholds for Regional Entity consideration, it is important to note that certain risk factors and the associated criteria/thresholds may vary by region, by entity size, or by function. Depending on the unique characteristics of the entity, the conclusion may be that some of the listed risk factors may be more applicable or contributory than others, some may not be applicable at all, or there may be additional risk factors not listed that would be appropriate to consider. For example, while certain characteristics of a registered entity may result in a higher assignment of risk relative to that specific factor, the registered entity's size or function may mean that the risk factor itself does not merit significant consideration in determining an entity's unique inherent risks to the reliability of the BPS. This also reflects the notion that some risk factors that might contribute towards determining overall inherent risk for a larger entity may contribute differently to the evaluation of a smaller entity.

Communication between the Regional Entity and registered entity may provide critical information for a risk determination. As needed, CEAs work with the registered entity to ensure the CEA has appropriate and sufficient information to conduct the IRA and reach accurate conclusions. After the CEA finalizes IRA results, it communicates a summary of the results to the registered entity (including risk areas and impact on the scope of monitoring).

Below are some hypotheticals and one practical example of the application of the IRA process.

In a June 2014 presentation, MRO explained how the IRA process applies to registered entities.[18] First, a Regional Entity identifies risks at the regional level and categorizes risks into reliability themes. The Regional Entity identifies how susceptible a registered entity is to well-known risk themes such as events, and includes entity-specific data, regional factors affecting reliability, compliance history, and legal or regulatory factors affecting reliability. In addition, the Regional Entity assesses each registered entity by analyzing other specific factors important to its function, such as peak load capacity, BPS exposure, interconnection points, and other resources and trends. MRO illustrated potential results for three similarly situated registered entities.

Specifically, MRO illustrated what the results would be for risk assessments of three wind plants with similar registrations, Generator Owner and Generator Operator. Before

[18] *Reliability Assurance Initiative Update*, June 19, 2014, *available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative%20Workshops/Reliability%20Assurance%20Initiative_RAI_Webinar_6%2019%2014_Final.pdf.

conducting the IRAs, MRO would have identified 131 applicable Requirements for each wind plant. The individual risk assessments captured unique aspects of each registered entity and allowed for a tailored monitoring scope for each. Wind Farm #1's IRA resulted in an audit scope of 20 Requirements. Wind Farm #2 was responsible for interconnection of a nuclear facility and therefore had 25 Requirements in its audit scope. Finally, Wind Farm #3, which did not own a collector bus, had two Requirements in scope. Rather than conducting a Compliance Audit, MRO could determine to use another compliance monitoring tool, such as a guided Self-Certification.

In another example, SERC conducted an IRA of Georgia Transmission Corporation ("GTC") in preparation of a Compliance Audit.[19] SERC collected and reviewed data regarding GTC's potential risks to the BPS through a pre-audit survey, reviewed GTC's compliance history, and used SERC's understanding of GTC from previous audit engagements. Based on its review of communication and coordination of operators, and GTC's related arrangements with other entities for the performance of registered functions, SERC adjusted the audit scope. Specifically, SERC increased the scope of the audit by eight Requirements.

SERC and GTC both agreed that the processes resulted in an improved focus on inherent risk when compared with the 2008 audit of GTC. SERC and GTC also learned that additional communication should occur during the development of the IRA. SERC has adjusted its

[19] This experience was the subject of a presentation to the NERC Board of Trustees Compliance Committee on August 13, 2014. The presentation is available at http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/BOTCC%20-%20Presentation.pdf.

communication with registered entities while conducting an IRA based on its experience with GTC.

The Regional Entity will perform IRAs on a periodic basis. The frequency may vary based on occurrence of significant changes to existing reliability risks or emergence of new reliability risks. At a minimum, a Regional Entity will be expected to consider whether IRAs should be updated when NERC identifies risk elements through the annual ERO CMEP IP. After consideration of the facts and circumstances, the Regional Entity will determine whether changes are required from year-to-year or sooner. As NERC performs oversight and observes what factors tend to trigger revisions to IRAs, NERC will consider providing additional guidance on this issue. For monitoring activities performed in 2015, Regional Entities are in various stages of conducting IRAs for registered entities within their footprints. During 2015 and beyond, Regional Entities will continue to expand the IRA process to entities in their footprints based on risk and compliance monitoring schedules.

3. Internal Controls Evaluation

An Internal Controls Evaluation ("ICE") enables a further refinement of the compliance oversight plan for individual registered entities. The ERO Enterprise Internal Compliance Evaluation Guide ("ICE Guide")[20] was developed by NERC in partnership with Regional Entities, registered entities, and various other stakeholders to assist CEAs in identifying and

[20] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Enterprise%20Internal%20Control%20Evaluation%20Guide.pdf.

more effectively considering existing internal controls around CMEP objectives - compliance with Reliability Standards.[21]

Considering internal controls in the scope of audits is required under GAGAS.[22] The ICE is NERC and the Regional Entities' effort to formalize and standardize internal controls evaluation in a broader manner to complement risk-based monitoring of compliance through the IRA and using the breadth of CMEP monitoring tools more effectively. ICE refines the focus on those controls related to the entity-specific risks identified through the IRA and germane to the applicable Reliability Standards and allows CEA staff to leverage the entire breadth of CMEP tools more effectively, including to determine whether a Compliance Audit is necessary. During an ICE, Regional Entities may use existing information from past work with the Registered Entity, such as past audits, mitigation plans, previous Internal Compliance Program reviews conducted through enforcement. Registered entities have an opportunity to provide, on a voluntary basis, additional information related to the ICE including details that demonstrates the effectiveness of detective, corrective, and compensating controls. Because of the ICE, the

[21] The most generally accepted definition of the term "internal controls" comes from the Committee of Sponsoring Organizations of the Treadway Commission ("COSO"), "…a process, effected by an entity's board of directors, management and other personnel, designed to provide 'reasonable assurance' regarding the achievement of objectives…" in this case, compliance with NERC Reliability Standards. *Internal Control – Integrated Framework*, 1992, *available at:* http://www.coso.org/documents/internal%20control-integrated%20framework.pdf. In addition, GAGAS defines internal controls in a similar manner under Section 6.15 c.: "Internal control, sometimes referred to as management control, in the broadest sense includes the plan, policies, methods, and procedures adopted by management to meet its missions, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; noncompliance with provisions of laws, regulations, contracts or grant agreements; or abuse." Government Auditing Standards: 2011 Revision (Reissued on Jan. 20, 2012) p. 131, *available at:* http://gao.gov/assets/590/587281.pdf.

[22] See GAGAS Section 6.16.

Regional Entity may further focus the compliance assurance activities for a given entity. The depth and breadth of any particular area of review may decrease based on the Regional Entity's conclusions on its ability to rely on the internal controls of the registered entity. For example, if a registered entity demonstrates effective internal controls for a given Reliability Standard, the Regional Entity may determine that it does not need to audit the registered entity's compliance with that Reliability Standard as frequently or select a different monitoring tool. Conversely, if a registered entity does not demonstrate effective internal controls for a given Reliability Standard during the ICE, the scope will not change from the IRA.

Because the controls to be evaluated pursuant to the ICE process are those related to the inherent risk posed by a particular registered entity, the extent of an evaluation will naturally vary in accordance with that inherent risk.

Below are some examples of the application of the ICE process.

In the June 2014 presentation mentioned above, MRO provided examples regarding the evaluation of internal controls.[23] The first example involved a review of American Transmission Company's ("ATC") internal controls related to Reliability Standard COM-002. In this example, ATC's preventive control involved a random review of operator communications, followed by feedback and corrective actions. The review showed that ATC used three-part communication for routine exchanges. In addition, ATC's detective control involved a complete review of any

[23] *Reliability Assurance Initiative Update*, June 19, 2014, *available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative%20Workshops/Reliability%20Assurance%20Initiative_RAI_Webinar_6%2019%2014_Final.pdf.

situation in which a directive may be issued. MRO concluded that ATC would identify and address issues on a timely basis. Therefore, MRO determined that it did not need to directly test compliance with Reliability Standard COM-002.

The second example related to the Protection and Control ("PRC") family of NERC Reliability Standards. ATC had implemented preventative controls that tracked activities and alerted any upcoming or missing tests. ATC also had detective controls that involved random monthly management review of 10% of maintenance and testing records. MRO concluded that ATC had internal controls for all of the requirements related to maintenance and testing intervals. Thus, the result allowed for reduced sampling for the related PRC Reliability Standards.

In another example, in preparation for a Compliance Audit, SERC evaluated GTC's internal controls. As part of its evaluation, SERC reviewed GTC's independent audit reports, and accepted the independent audit report findings for 18 of the 38 Requirements in scope. Therefore, SERC did little to no additional testing in these areas. In reaching its conclusions, SERC determined that the independent audit reports: (i) adequately addressed the applicable Reliability Standards and Requirements; (ii) were relevant to the audit period; and (iii) reflected an appropriate level of rigor for SERC staff to draw the same conclusions.

The CEA is ultimately responsible for evaluating internal controls to determine proper oversight scope (i.e. the extent of reliance on internal controls for applicable Reliability Standards). The CEA makes this determination by understanding the BPS risks to which the registered entity is susceptible and gaining an understanding of how the registered entity controls or mitigates those risks in a meaningful manner. When the CEA has reasonable assurance that

internal controls are functioning to protect reliability in accord with Reliability Standards, the CEA may rely on those internal controls and therefore, extensive testing may not be necessary.

Depending on regional flexibility and available resources, a CEA may conduct an ICE outside of normal compliance monitoring processes. However, the ERO Enterprise anticipates that during 2015, Regional Entities will generally only conduct an ICE in preparation for a scheduled compliance monitoring activity, e.g., a Compliance Audit.

The complexity of internal controls and the CEA evaluation of such internal controls will be scaled in accordance with the size of the registered entity, as described in the ICE Guide. However, it is possible that after the IRA, few applicable standards may remain as part of the monitoring scope for an entity posing a small inherent risk. In that case, it is possible that an ICE may not result in a significant further tailoring of monitoring activities. Nevertheless, the ICE provides, even for those entities, an opportunity for continuous improvements in controls that could increase reliability and mitigate risks.

4. CMEP Tools

Ultimately, the Regional Entity will determine the type and frequency of the compliance monitoring tools (i.e., off-site or on-site audits, spot checks or self-certifications)[24] that are warranted for a particular registered entity based on reliability risks. The determination of the appropriate CMEP tools will be adjusted, as needed, within a given implementation year. Regional Entities' IPs may indicate CMEP tools being used during the implementation year (e.g.,

[24] CMEP §3.0 (Appendix 4C to the Rules of Procedure).

audit schedules, self-certifications, or periodic data submittals), but the Regional Entity will continue to identify appropriate CMEP tools to use based on results from regional risk assessments, IRAs, and ICEs.

NERC is currently reviewing the 2015 Regional Entity IPs for approval as provided in the Rules of Procedure. These region-specific plans provide the inputs and considerations that impact the development of compliance oversight plans for registered entities. Regional Entity IPs identify how the Regional Entities will use various compliance monitoring tools, such as on- and off-site audits. For example, prior to 2015, Regional Entities conducted audits for all entities on a three- and six-year audit cycle. Using a risk-informed approach, Regional Entities will continue to conduct three-year audits per the Rules of Procedure. However, a registered entity's IRA, and ICE if used, will determine the frequency and Compliance Audit scope rather than a standardized approach based solely on the registered function and the applicability of Requirements contained in an actively monitored list. In their 2015 Regional Entity IPs, the Regional Entities identified registered entities scheduled for Compliance Audits in 2015. However, all registered entities are subject to oversight, and additional registered entities, at the discretion of the Regional Entity, may also be subject to compliance monitoring in 2015.

C. Planning and Execution of Compliance Audits

Compliance Audits remain a relevant part of the ERO Enterprise's risk-based approach to compliance monitoring. Pursuant to the NERC Rules of Procedure, each Regional Entity must maintain and implement a program of proactive Compliance Audits of BPS owners, operators,

and users responsible for complying with Reliability Standards.[25] Further, a Compliance Audit of an entity registered as a Balancing Authority, Reliability Coordinator, or Transmission Operator must occur at least once every three years.[26] However, the time since the last audit is no longer the main driver for the audit planning process. Instead, as explained above, NERC and the Regional Entities will look to other key criteria to measure risk to the BPS, including entity processes, controls, and compliance history in determining the appropriate compliance monitoring tool for a particular registered entity. In 2015, some Regional Entity IPs may include Compliance Audits that were scheduled prior to full implementation of risk-based compliance monitoring. Beginning in 2016, however, the decision to conduct a Compliance Audit or select a different monitoring tool should be made in accordance with the risk-based processes outlined herein.

Risk-based audit principles and risk-based auditing are fully consistent with practices of other agencies, including for example, the Division of Audits and Accounting ("DAA") within FERC's Office of Enforcement. As DAA explained in the 2013 Staff Report on Enforcement, "Risk assessment continues to be an important aspect of DAA's audit program because a significant majority of audits are initiated without any allegation of wrongdoing. Audited entities are typically selected using risk-based criteria[.]"[27]

---

[25] NERC Rules of Procedure, § 403.11.
[26] *Id.* § 403.11.1.
[27] *2013 Report on Enforcement*, Docket No. AD07-13-006, p. 29 (Nov. 21, 2013), *available at:* http://www.ferc.gov/legal/staff-reports/2013/11-21-13-enforcement.pdf.

Moving from a strictly time-based audit cycle to a risk-based audit cycle will improve oversight of the reliability of the BPS. If a registered entity now on a minimum three-year audit schedule poses substantial risk to the reliability of the BPS, its CEA may schedule audits more frequently than every three years. Similarly, for registered entities not subject to the three-year cycle, CEAs will monitor these entities, and base compliance monitoring activities' frequency, depth, and breadth on that entity's specific risk to BPS reliability. The ERO Enterprise will also continue to use other compliance monitoring tools such as self-certifications and spot checks. Again, the use and application of compliance monitoring tools will vary based on the risk-based processes outlined above to create the best method for effective oversight of compliance with Reliability Standards.

As the ERO Enterprise implements a risk-based approach to monitoring compliance with Reliability Standards, NERC and the Regional Entities recognize the need for continued CEA staff training and additional tools, in addition to and in support of NERC oversight. For example, the ERO Enterprise Compliance Auditor Manual ("Manual"),[28] which includes the Compliance Auditor Handbook, is a recent tool developed to assist CEA staff.

NERC and the Regional Entities jointly developed the Manual to help improve consistency and quality of compliance monitoring across the ERO Enterprise. The Manual, which the Regional Entities adopted and began using in April 2014, contains common tools,

[28] *ERO Enterprise Compliance Auditor Manual*, *available at*: http://www.nerc.com/pa/comp/ERO%20Enterprise%20Compliance%20Auditor%20Manual%20DL/ERO_Enterprise_Compliance_Auditor_Manual_version_1.pdf.

techniques, and approaches for compliance auditors. The Manual Drafting Team completed the first draft of the Manual in December 2013 and provided it to the NERC and Regional Entity executive management for review and comment. The Manual is a living document, and revisions will occur as NERC and the Regional Entities improve, develop, and implement compliance monitoring processes. Currently, the Manual includes sections on: an Introduction to Compliance Auditing, the Compliance Auditor Handbook, and the Compliance Auditor Capabilities and Competency Guide. Additional sections continue to be developed for the Manual, including: Ethics and Standards, sampling methodology, supporting diagrams and flow charts, common forms and templates, and other content as needed.

Following the completion of the Manual, NERC and the Regional Entities supported the formal roll-out with training initiatives, information sessions, and workshops. NERC began roll-out and initial training to regional auditors on use of the Manual during the first quarter of 2014, with full implementation in the second half of 2014 and use for all audits scheduled in 2015. NERC and the eight Regional Entities also jointly developed communication and training activities. Training modules consisted of a series of presentations, exercises and, on-line and instructor-led training. As tools and processes evolve, they will be added to the Manual, with the development and administering of training to follow. NERC and the Regional Entities continue to incorporate the Manual as part of periodic training for compliance auditors, such as Auditor Team Lead training. In addition, NERC and the Regional Entities have established a process for Manual additions, enhancements, and updates. In addition to training, mid- and long-range revision management and maintenance are being developed to ensure the long-term sustainability of the document. Additionally, in 2015, NERC will perform oversight activities of

the Regional Entities to support implementation and process improvements related to the use of the Manual.

V. RISK-BASED ENFORCEMENT

A. FFT as the Platform for the Evolution of a Risk-based Enforcement Program

Over the past several years, the ERO Enterprise has been enhancing its risk-based approach for assessing and processing noncompliance. The ERO Enterprise continues to expect identification and mitigation of all instances of noncompliance, regardless of the level of risk they posed to the reliability of the BPS. However, not all instances of noncompliance require the same level of documentation and processing. The overwhelming majority of the caseload processed by the ERO Enterprise over the years has posed a minimal or moderate risk to the reliability of the BPS.[29] As a result, it is appropriate to use a variety of means to resolve noncompliance, including the exercise of discretion not to initiate a formal enforcement action.

Since 2011, the ERO Enterprise has used the FFT process to resolve over 2,000 instances of noncompliance with the Reliability Standards, most of which posed a minimal risk to the reliability of the BPS. Since June 2013, the FFT process has been used to resolve

[29] In 2012 and 2013, respectively, the ERO Enterprise handled 74% and 72% of the violations and issues posted or filed at FERC as FFTs or in Spreadsheet Notice of Penalty filings. Both of these disposition methods are used for only minimal or moderate risk noncompliance. *NERC Compliance Violation Statistics—Fourth Quarter 2013*, at 10, *available at:* http://www.nerc.com/pa/comp/CE/Pages/Compliance-Violation-Statistics.aspx. In addition, in 2013 and 2014, respectively, 72% and 70% of instances of noncompliance posed a minimal risk to the reliability of the BPS and 27% (in both years) posed a moderate risk. From 2012 through October 1, 2014, only 2% of violations posed a serious or substantial risk to the reliability of the BPS.

noncompliance posing a moderate risk to the BPS.[30] Building on the success of the FFT process, the ERO Enterprise identified and implemented additional processes that enhance its effectiveness while promoting and supporting reliability.

The processes discussed below further streamline the resolution of lesser-risk noncompliance with NERC Reliability Standards. This continued evolution is necessary to allow the ERO Enterprise, as well as industry, to allocate resources to address the issues posing a higher level of risk to reliability. In addition, this approach leverages registered entity existing internal practices relating to self-monitoring and assessment of compliance with Reliability Standards. By appropriately recognizing such efforts, the ERO Enterprise encourages the enhancement of internal controls and self-identification of noncompliance throughout the industry.

Based on the experience with a streamlined process and a reduced record for resolution of minimal risk noncompliance, since 2013, NERC and the Regional Entities have exercised discretion when deciding whether to initiate a formal enforcement action regarding certain instances of noncompliance posing a minimal risk to the reliability of the BPS. Noncompliance that is not pursued through a formal enforcement action by the ERO Enterprise is referred to as a

[30] *North American Electric Reliability Corp.*, 138 FERC ¶ 61,193 ("2012 FFT Order"), *order on reh'g*, 139 FERC ¶ 61,168 (2012) (approving FFT program); *North American Electric Reliability Corp*., 143 FERC ¶ 61,253 (2013) (approving expansion of program to include moderate risk issues and issues that will be mitigated within 90 days of posting, as well as proposal to publicly post FFT issues in lieu of submitting an informational filing); and *North American Electric Reliability Corp*., 148 FERC ¶ 61,214 (2014) (approving continued inclusion of moderate risk issues as well as expansion of program to include issues that will be mitigated within one year of posting, subject to conditions).

"compliance exception." As of September 30, 2014, a total 54 instances of noncompliance have received compliance exception treatment.

Beginning in October 2013, NERC and the Regional Entities began to allow select registered entities with demonstrated effective management practices to self-identify, assess, and mitigate instances of noncompliance to self-log minimal risk noncompliance that would otherwise be individually self-reported. Properly logged items are entitled to the presumption of being resolved as compliance exceptions unless there are additional risk factors involved. Logged items will be periodically filed with the Regional Entity. The Regional Entity will validate the logs. 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 BPS.

B. Regulatory Structure and Identification of the Risk Posed by Noncompliance

Section 3.8 of the CMEP, which describes what each CEA must do once it identifies a potential noncompliance with a Reliability Standard Requirement, provides, in part that:

> If the Preliminary Screen results in an affirmative determination with respect to the above criteria, a Possible Violation exists and the Compliance Enforcement Authority shall proceed in accordance with Section 5.0, unless an alternative enforcement process is used. (emphasis added)

Section 5.0 of the CMEP, which describes the processes associated with Enforcement Actions, further provides that:

> The following enforcement process is undertaken by the Compliance Enforcement Authority following identification of a Possible Violation of a Reliability Standard Requirement by a Registered Entity. However, under the circumstances presented by some Possible Violations, Alleged

> Violations or Confirmed Violations, absolute adherence to the following enforcement process, to the exclusion of other approaches, may not be the most appropriate, efficient or desirable means by which to achieve the overall objectives of the Compliance Program for NERC, the Compliance Enforcement Authority and the Registered Entity. In such circumstances, other approaches may be considered and employed. The Registered Entity shall be entitled to object to the use of any such other approach. (emphasis added)

These provisions allow the ERO Enterprise to use alternative processes that are appropriate, efficient, or desirable means to achieve the overall objectives of the CMEP. The resolution of noncompliance as compliance exceptions through the process described herein is such an alternative approach for the resolution of lesser-risk noncompliance that is fully consistent with the overall objectives of the CMEP.

FERC has expressed support for NERC and the Regional Entities to use risk-based compliance and enforcement processes, including using appropriate discretion when determining how to treat low-risk instances of noncompliance. For example, in its order approving Version 5 of the Critical Infrastructure Protection Reliability Standards, FERC stated:

> We understand that NERC has inserted the "identify, assess, and correct" language into the CIP Reliability Standard requirements to move its compliance processes towards a more risk-based model. With this objective in mind, we believe that a more appropriate balance might be struck to address the underlying concerns by developing compliance and enforcement processes that would grant NERC and the Regional Entities the ability to decline to pursue low risk violations of the Reliability Standards.[31]

[31] *Version 5 Critical Infrastructure Protection Reliability Standards,* Order No. 791, 145 FERC ¶ 61,160, P 75 (2013).

A common understanding of how the ERO Enterprise determines the various levels of risk of instances of noncompliance is fundamental to the continued evolution of the risk-based enforcement program. The ERO Enterprise uses three different levels to identify the risk posed by any instance of noncompliance: "serious and substantial," "moderate," and "minimal." The analysis that is performed is based on prior FERC orders and is discussed in the ERO Enterprise Self-Report User Guide.[32]

In FERC's 2012 FFT Order, FERC agreed that examples of serious and substantial issues are those involving or resulting in (i) extended forced outages; (ii) loss of load; (iii) cascading blackouts; (iv) certain vegetation contacts; (v) systemic or significant performance failures; (vi) intentional or willful acts or omissions; (vii) gross negligence; and (viii) other misconduct.[33] The ERO Enterprise concentrates its efforts on such serious and substantial issues when they infrequently arise. NERC files serious and substantial matters with FERC in Full Notices of Penalty.

Issues are determined to pose a minimal risk to BPS reliability based on the combination of the subject Reliability Standard requirement and the attendant facts and circumstances. If nothing serious could have occurred and there were complete or significant protections in place to reduce the risk, as a general matter, then the risk would likely be minimal.

---

[32] *See ERO Self-Report User Guide*, pp. 11-13 (April 2014), *available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf (describing the guidelines to help Registered Entities assess the risk to the reliability of the BPS posed by noncompliance with a Reliability Standard). *See also* the 2012 FFT Order, 138 FERC ¶ 61,193, at PP44-45 (FERC discussion of risk assessments including a review of actual versus potential risk).

[33] *Id.* P49.

The lack of harm is not sufficient justification, by itself, for a minimal or moderate risk assessment. The facts and circumstances leading to a moderate risk determination are necessarily different. If something serious could have occurred during a noncompliance and there were only some protections in place to reduce the risk, then the risk assessment would likely be moderate.[34] If the noncompliance is related to a serious event, then the risk would likely be serious and substantial. Examples of serious harm generally include loss of customer load, cascading outages, and malicious actions that affect Critical Assets.

The determination of the level of risk posed by instances of noncompliance resolved through an enforcement action is clearly identified in the Notice of Penalty or FFT spreadsheet. Numerous examples of these determinations are available on the Enforcement and Mitigation page of the NERC website.[35]

C. Compliance Exceptions

Consistent with the above, beginning in November 2013, the ERO Enterprise implemented, on a pilot basis, a method to expand the exercise of enforcement discretion by identifying minimal risk instances of noncompliance that do not warrant a penalty and which would be recorded and mitigated as a "compliance exception" without triggering a formal enforcement action under section 5.0 of the CMEP.

---

[34] *See ERO Self-Report User Guide*, 11-13 (April 2014), *available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Self-Report%20User%20Guide%20(April%202014).pdf (describing the guidelines to help Registered Entities assess the risk to the reliability of the BPS posed by noncompliance with a Reliability Standard). *See also* 2012 FFT Order at PP44-45 (2012) (FERC discussion of risk assessments including a review of actual versus potential risk).

[35] *Available at:* http://www.nerc.com/pa/comp/CE/Pages/Enforcement-and-Mitigation.aspx.

As noted above, the process of identifying and recording compliance exception builds on the FFT program. The exercise of discretion by the ERO Enterprise is informed by the facts and circumstances of the noncompliance, the risk posed by the noncompliance to the reliability of the BPS, and the deterrent effect of an enforcement action or penalty, among other things. These considerations are very similar to the considerations that have been used since 2011 to determine whether noncompliance should be processed as an FFT.[36]

Compliance exception is an alternative disposition method and is not a dismissal, FFT, or Notice of Penalty. It is essentially the exercise of enforcement discretion with respect to a noncompliance regardless of its method of discovery (self-report, self-certification, audit finding, etc.).

When an instance of noncompliance is disposed of as a compliance exception, NERC does not publicly post it as in the case of an FFT or file it with FERC as in the case of a Notice of Penalty. Rather, the Regional Entity retains the record for the compliance exception and provides NERC, through non-public means, a summary of the record. NERC then submits the compliance exceptions to FERC through non-public means.

A compliance exception is part of a registered entity's compliance history only to the extent it serves to inform the Regional Entity and NERC of the minimal risk issues that are detected and corrected by the registered entity, and may inform the Regional Entity's decision on how to treat future noncompliance with the same or similar facts. It should be noted that repeat

[36] *See, e.g.,* 2012 FFT Order at PP17-21.

compliance exceptions may not always be indicative of poor performance; they may in fact be evidence of robust controls in place to detect and correct instances of noncompliance as they occur. A registered entity may object to resolution of any issue as a compliance exception by providing written notification to the Regional Entity within seven days of the communication by the Regional Entity. In the event a registered entity objects to resolution as a compliance exception, the noncompliance will be resolved through one of the other enforcement processes established in the CMEP at the discretion of the Regional Entity.[37]

1. Instances of Noncompliance that Qualify for Recording as Compliance Exceptions

Minimal risk instances of noncompliance are eligible for processing as compliance exceptions regardless of the discovery method. Regardless of the discovery method, however, the noncompliance is recorded and tracked and reviewed by the Regional entity. As noted above, all compliance exceptions are also provided to NERC and FERC.

The Regional Entity determination of whether an instance of noncompliance is eligible for compliance exception treatment is essentially the same as the process it has been using, since 2011, to make a determination of eligibility for FFTs posing a minimal risk to the reliability of the BPS.[38] Regional Entities focus on the underlying facts and circumstances of the noncompliance, including what happened, why, where, and when. Another factor Regional Entities use to determine whether a noncompliance should be eligible for compliance exception

[37] CMEP (Appendix 4C to the Rules of Procedure) § 5.0 Enforcement Actions.
[38] *See, e.g.,* 2012 FFT Order at PP17-21.

treatment is the potential and actual level of risk to reliability, including mitigating factors during the pendency of the noncompliance. Regional Entities consider the registered entity's internal compliance program ("ICP"), including preventative and corrective processes and procedures, management practices, and culture of compliance as factors to help determine whether a noncompliance should receive compliance exception treatment. A robust ICP with strong management practices around Reliability Standards that led to timely discovery and swift mitigation of noncompliance creates a strong argument in favor of compliance exception treatment. Regional Entities also consider the presence and applicability of aggravating factors, such as repeat or repetitive noncompliance. An instance of noncompliance may be eligible for compliance exception treatment even if a registered entity has negative compliance history with a same or similar standard. This ensures that NERC and the Regional Entities do not discourage registered entities from robustly self-reporting noncompliance. However, repeat noncompliance should lead to a deeper look into root causes of mitigation failure and an examination of the connection between the registered entity's ICP, applicable organizational and management practices, and its day-to-day adherence to Reliability Standards in operations.

At this time, only noncompliance posing a minimal risk to the reliability of the BPS is eligible for compliance exception treatment. NERC's annual review of the program will consider the inclusion of moderate risk issues in the future.

2. Applicability throughout ERO Enterprise

Throughout the ERO Enterprise, a noncompliance can qualify for compliance exception treatment in two ways. The first way that noncompliance can qualify for compliance exception treatment is on a case-by-case basis; an individual issue is deemed to have posed a minimal risk

to the reliability of the BPS and does not warrant a penalty, as discussed above. Beginning in 2015, this discretionary treatment will be available for any qualified minimal risk noncompliance, regardless of the registered entity or discovery method, or version of the Reliability Standard and Requirement. The resolution of the noncompliance, including whether it may be resolved as a compliance exception, is based, as noted above, on a review of specific facts and circumstances.

The second way in which noncompliance posing a minimal risk to the reliability of the BPS can be resolved as a compliance exception is through the self-logging program. As explained below, noncompliance that is self-logged is presumed to be appropriate for disposition as a compliance exception. This approach, however, is limited to registered entities designated by the Regional Entity as eligible for self-logging.

As Regional Entities increase use of the compliance exception process for minimal risk issues in 2015 and beyond, the FFT process will remain available for processing of any minimal or moderate risk issue. However, it is likely that the FFT process would be used primarily to process those moderate risk issues that qualify, and minimal risk issues, when appropriate, would be disposed of as compliance exceptions. The FFT process will remain an available processing method for issues that do not qualify for compliance exception treatment when the facts and circumstances, mitigation, internal controls, and other factors, such as the registered entity's compliance history, make a monetary penalty and resolution through a Notice of Penalty filing inappropriate.

3. Processing and Recording of Compliance Exceptions

All noncompliance, including that which is eligible for compliance exception processing, is entered into the Regional Entity system, given a tracking ID, and undergoes the triage process. Upon determination that an item will be disposed of as a compliance exception, the Regional Entity provides information regarding said item to NERC through nonpublic means. The information provided to NERC includes the relevant Reliability Standard and Requirement, a brief description of the noncompliance, an assessment of the risk to the BPS posed by the issue, and a description of the actions taken (or to be taken) to mitigate the issue and prevent recurrence.

Compliance exceptions must be mitigated within twelve months of the time of the communication to the registered entity resolving the matter without an enforcement action.[39] The timing of completing mitigating activities is not always associated with the risk posed by the noncompliance.[40] Consistent with FERC's direction in its recent FFT order,[41] in the event Regional Entities dispose of a matter that has yet to be mitigate as a compliance exception, the record must clearly indicate (i) the expected completion date, (ii) the justification for the length of time required, and (iii) a description of all compensating measures in place during the period

[39] Some issues, despite their posing a lower risk, require mitigating steps that may require extra time to complete. Therefore, with the understanding that setting an abbreviated timeframe for mitigation completion as a condition of compliance exception processing does not always accurately reflect the risk posed by the noncompliance, the ERO Enterprise set a twelve-month mitigation completion timeframe for compliance exceptions. *See North American Electric Reliability Corp. Compliance Filing and Report on the Find, Fix, Track and Report Program*, Docket No. RC11-6-004 at pp. 47-49 (June 20, 2014).
[40] *Id.*
[41] *North American Electric Reliability Corp.*, 148 FERC ¶ 61,214 at P 37 (2014).

of noncompliance which reduce the risk to reliability while mitigation is ongoing. NERC will in turn provide this information to FERC staff. In addition, NERC will notify FERC staff when the mitigation is completed for each compliance exception with an extended mitigation period.

This mitigation completion period is not intended to allow every issue receiving compliance exception treatment to be unmitigated by the time of the determination. Rather, it is intended to allow flexibility for the Regional Entities to provide appropriate treatment, even for those instances of noncompliance that require additional time for mitigation.[42] The ERO Enterprise goal for the allowance of extended completion periods is to provide appropriate flexibility to ensure full mitigation, not to encourage the delay of mitigation activity. In fact, despite the fact that the ERO Enterprise may exercise discretion over noncompliance that is capable of being mitigated within twelve months, not all minimal risk matters with open mitigating activities may be appropriate for compliance exception treatment. Indeed, where NERC and the Regional Entities determine such mitigating activities are not prompt or are otherwise unnecessarily delayed, NERC and the Regional Entities will evaluate the totality of the facts and circumstances when assessing an appropriate disposition method.

Registered entities will notify the Regional Entity of completion of mitigation through an authorized representative of the registered entity (including through electronic means). The Regional Entity will track mitigation completion and will notify NERC of that completion.

---

[42] *North American Electric Reliability Corp. Compliance Filing and Report on the Compliance Enforcement Initiative and Proposed Enhancements to the Find, Fix, Track and Report (FFT) Program*, Docket No. RC11-6-004 at pp. 40-41 (March 15, 2013).

Failure to complete mitigation in the established timeframe, or any material misrepresentation of information provided in connection with this program, will result in rescission of the eligibility for compliance exception treatment.

A compliance exception notice indicates to a registered entity that the Regional Entity has completed its review of the matter.

4. Experience Gained during Pilot Phase

From November 2013 to the present, Regional Entities have been selecting compliance exception candidates from minimal risk noncompliance. This approach allowed the ERO Enterprise to implement the program gradually and refine the program requirements and processes. As of September 30, 2014, a total of fifty-four instances of noncompliance have been treated as compliance exceptions. Twenty-two compliance exceptions (41%) were low-risk CIP noncompliance; the remaining thirty-two compliance exceptions (59%) were non-CIP noncompliance. Fifty percent of the compliance exceptions were discovered in 2014. Twenty-five (46%) compliance exceptions were externally identified by Regional Entities (Compliance Audits, Spot Checks, or Investigations) and twenty-nine (54%) were internally identified by registered entities. NERC has included in its regular presentations to its Board of Trustees Compliance Committee information on compliance exceptions including levels of utilization, representative examples, and other data.

5. Visibility and Accountability

While the Regional Entity reports all instances of noncompliance to NERC, unlike an enforcement action, compliance exceptions are not filed or publicly posted.

There are, however, various ways for communicating to the public useful information regarding the overall rationale for decisions not to pursue certain matters as well as regarding the use of compliance exceptions throughout the ERO Enterprise. For example, NERC has published a Compliance Exceptions Overview document on its website.[43] This document describes the aspects of the compliance exceptions, including eligibility requirements, mitigation requirements, finality, and how visibility and accountability will be maintained as the program is implemented and expanded across the ERO Enterprise. In addition, to ensure that the public can derive the maximum value of information regarding compliance exceptions without altering the message that these issues are generally not ones worthy of significant attention, NERC will make an annual informational filing to FERC reviewing the progress of the program and considering any enhancements or expansions that may be necessary. The annual report will include observed trends by standard, region or other categories. The report will also include examples of matters treated as compliance exceptions. Similar information will also be reported on a regular basis to the NERC Board of Trustees Compliance Committee.[44]

Non-public enforcement discretion is consistent with other regulatory regimes, including FERC's. In FERC investigations closed without any action, the existence of the investigation remains non-public in all but rare circumstances.[45] In fact, in the Revised Policy Statement on

[43] Compliance Exceptions Overview, *available at*: http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Compliance%20Exception%20Overview.pdf.
[44] An example of the information submitted publicly to the Board of Trustees Compliance Committee is available at http://www.nerc.com/gov/bot/BOTCC/Compliance%20Committee%202013/November%2012%20Compliance%20Committee%20Agenda%20Package.pdf.
[45] *See* 18 C.F.R. Part 1b (2014).

Enforcement issued May 15, 2008, FERC noted that between 2005 and 2007, "Enforcement staff closed approximately 75 percent of its investigations without any sanctions being imposed, even though Enforcement staff found a violation in about half of those closed investigations. … Additionally, more than half of the self-reports submitted to FERC Enforcement staff were closed with no action."[46] From 2007 through 2013, FERC Office of Enforcement, Division of Investigations staff closed approximately 50 percent of its investigations without imposing sanctions—many with findings of violation.[47] The rare circumstances in which FERC does publish both the existence and the results of its investigations underscore their importance and allow FERC to communicate the importance of such matters to the regulated community.

Indeed, an enforcement agency should not, as a general matter, provide precise indications of where the bar is for its exercise of discretion. The Freedom of Information Act acknowledges this rationale in permitting a U.S. agency to withhold law enforcement records that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law[.]" 5 U.S.C. § 552(b)(7)(E).

There is also a privacy issue for those registered entities involved where no formal determination regarding a violation has been made. An entity's reputation could be adversely

[46] *Revised Policy Statement on Enforcement*, 123 FERC ¶ 61,156, P 9 (2008) (2008 Revised Policy Statement).
[47] *2013 Staff Report on Enforcement*, Docket No. AD07-13-006 pp. 22-25 (November 21, 2013) *available at:* http://www.ferc.gov/legal/staff-reports/2013/11-21-13-enforcement.pdf.

impacted if disclosed, even though there was no formal determination regarding a violation. In the context of investigations, FERC has acknowledged that "premature disclosure could adversely affect the reputation of the subject. Public disclosure at the outset of an investigation would risk exposing the subject to undue public suspicion without staff having conducted sufficient discovery to reach a preliminary finding that the subject may have violated a FERC requirement."[48] In the instance of a compliance exception, the CEA does not reach a determination regarding a violation. Therefore, public disclosure could "expose the subject to undue public suspicion."[49]

The nonpublic nature of compliance exceptions also reinforces the need for registered entities to shift focus and attention to higher-risk noncompliance, which is made public. The continuation of publicly posting the resolution of minimal risk noncompliance would dilute the message that is sent through the public disposition of higher-risk matters. As indicated above, trends and analysis associated with such minimal risk noncompliance may be educational or otherwise helpful, and will be provided to the public regularly. However, posting of individual accounts of trivial instances of noncompliance does not provide a benefit and diverts resources from the ERO Enterprise that should be allocated elsewhere. To illustrate this point, the following are examples of minimal risk instances of noncompliance that received compliance exceptions treatment.

---

[48] *Enforcement of Statutes, Regulations, and Orders,* 129 FERC ¶ 61,247 at P5 (2009); *order on reh'g.*, 134 FERC ¶ 61,054 (2011).
[49] *Id.*

- During an internal review, the entity identified that after an internal reorganization took place a year earlier, it had failed to document changes to the CIP senior manager within 30 calendar days of the effective date. The primary cause for the noncompliance was a lack of knowledge by the Primary Compliance Contact, who had been responsible for documenting the change, because the person had been in the position approximately six months at the time of the management change. The risk was minimal because the entity has no Critical Assets and is a small size utility.

- An entity self-identified that it had missed three work orders associated with three separate batteries each located at different generation facilities. The three instances of monthly frequency missed were from prior years and despite the missed work orders, the three batteries involved had been tested and maintained per prescribed frequency defined by the entity's program on a consistent basis.

- An entity self-identified that it failed to revoke access to Critical Cyber Assets (CCAs) within seven calendar days for personnel who no longer required such access to CCAs. The noncompliance was related to one employee who started working remotely and therefore did not need physical access to the CCAs. The helpdesk misinterpreted the email notification as no access removal is required since the employee is now working remotely.

The review, by the public, of these and other individual accounts of trivial, minimal risk noncompliance does not promote the reliability of the BPS.

6. Oversight by NERC

As discussed above, the resolution of noncompliance as compliance exceptions does not eliminate or reduce oversight or visibility regarding minimal risk noncompliance. NERC will continue to provide oversight of the program. All noncompliance, including that which is eligible for compliance exception processing, will continue to be entered into the Regional Entity compliance data systems and assigned a tracking identification number. Upon its determination that an item will be disposed of as a compliance exception, the Regional Entity will provide information to NERC on a monthly basis. The record will include the relevant Reliability Standard and requirement, a description of the issue, an assessment of the risk to the reliability of

the BPS posed by the issue, and the actions taken (or to be taken) to mitigate the issue and prevent recurrence. As with all identified instances of noncompliance, NERC provides the information submitted by the Regional Entity to FERC through non-public portals.

In 2014, NERC will continue to review all compliance exceptions. Beginning in 2015, however, NERC will, in a manner similar to its oversight of FFT, review a sample of compliance exceptions on a regular basis and provide guidance or adjustments on a prospective basis.

D. Self-logging Program

Beginning in October 2013, NERC and certain Regional Entities began to allow select registered entities with demonstrated effective management practices to self-identify, assess, and mitigate instances of noncompliance to log minimal risk noncompliance that would otherwise be individually self-reported. The logs contains a detailed description of the issue, the risk assessment with factual support, and the mitigating activities completed or to be completed by the Registered Entity. The log is periodically reviewed and approved by the Regional Entity (or in the case of multi-regional logs, Regional Entities). Logged items are presumed to be resolved as compliance exceptions once reviewed and approved by the Region(s). In that review and approval process, the Regional Entity determines that the issue is described accurately, that the minimal risk determination is justified and reasonable, and that the issue is adequately mitigated. This is consistent with the principle that minimal risk noncompliance that is self-identified, corrected, mitigated, and documented by the entity, should not be resolved through the formal enforcement process or incur a penalty absent a higher risk to the BPS.

The program relies on and promotes a closer understanding by Regional Entities of registered entities' management practices. In addition, it creates motivation and incentives for

registered entities to implement effective controls to detect and correct instance of noncompliance as they arise. Registered entities currently participating in the program report that they see a significant benefit, particularly associated with the presumption that logged items will be resolved as compliance exceptions and the efficiency gains associated with streamlining the processing of self-reports and mitigation plans.

1. Eligibility to Participate in the Program

In determining eligibility, the Regional Entities consider whether a registered entity is capable of self-identifying and mitigating minimal risk noncompliance on its own, as demonstrated by, among other things: (i) the registered entity's history of initiative and recognition of compliance obligations; (ii) the registered entity's reliable and accurate self-reporting of noncompliance to the Regional Entities; (iii) the registered entity's history of mitigating its noncompliance in a timely and thorough manner; (iv) the quality, comprehensiveness, and execution of the registered entity's internal compliance program; (v) the registered entity's cooperation with the Regional Entity during enforcement actions, compliance monitoring activities, and Regional Entity outreach; and (vi) the registered entity's performance during regional Compliance Audits.

An ICE, if performed, informs a Regional Entity's decision regarding participation in the self-logging program, but is not a prerequisite for participation. In fact, as noted above, an ICE may not always be necessary given the inherent risk posed by a particular entity for a particular function. However, the Regional Entity may inquire as to the internal controls in place to self-monitor and then identify, assess, and correct issues for which the registered entity is allowed to

log minimal risk noncompliance. This inquiry will be scaled in accordance with the risk posed by the registered entity.

Eligibility for the self-logging program is not an all-or-nothing proposition. Each registered entity may receive a set of individualized parameters for its participation in the program that reflects the risk posed by the registered entity and the strength and maturity of its practices in a given area. For example, a registered entity may be eligible to self-log noncompliance with certain Reliability Standards and not others.

Registered entities may lose eligibility to self-log for various reasons. A Regional Entity may remove a registered entity's ability to self-log minimal risk noncompliance for all or a subset of Reliability Standards if the registered entity has demonstrated deficiencies in identifying, assessing, or correcting noncompliance. Misrepresentation or repeated, avoidable inaccuracies in the log may also result in the loss of the registered entity's self-logging ability.

Participation in the self-logging program is voluntary. Registered entities may contact their Regional Entities regarding participation, but are not required to participate.

2. Processing and Recording of Self-Logged Noncompliance

Registered entities permitted to self-log must maintain a record of instances of noncompliance with NERC Reliability Standards that posed a minimal risk to the reliability of the BPS. Appropriate self-logging replaces the individual Self-Reports and accompanying formal Mitigation Plans for each such instance of noncompliance.

On the log, the registered entity records a detailed description of the minimal risk issue that it has identified, the basis of its minimal risk assessment, and the actions it has taken or will take to correct the issue, specifically the mitigating activities it has undertaken to address the

issue and prevent reoccurrence. Because only minimal risk issues are eligible for inclusion on the log, the registered entity's processes in place to determine risk are key to its eligibility for self-logging. The log is currently in the form of a spreadsheet similar to that used for FFT issues. It is expected that, in the future, subject to successful system upgrades, registered entities will be able to maintain their log electronically on the Regional Entity portal.

The registered entity submits its log for review by the Regional Entity every three months.[50] The Regional Entity must review the log to confirm that the registered entity has adequately identified and described the noncompliance, accurately assessed the risk, and appropriately corrected or identified the steps it will take to correct (i.e. mitigate) the noncompliance. The Regional Entity may submit any concerns, questions, or proposed revisions to the registered entity for consideration. Once the log is finalized, the log is submitted to NERC, and the minimal risk individual issues are processed as compliance exceptions. If compliance exception treatment is not appropriate for any individual instance of noncompliance recorded in the log, the matter may be resolved through any of the remaining disposition tracks. At this time, noncompliance posing a moderate or greater risk to the reliability of the BPS is ineligible for self-logging.

In the event the registered entity identifies a noncompliance and determines that it poses more than a minimal risk, or the registered entity is not certain of the level of risk posed by the noncompliance, the registered entity is encouraged to submit a Self-Report to its Regional Entity.

[50] The Regional Entity may adjust this period to six months based on its experience with the registered entity in the self-logging program.

3. Experience Gained during Pilot Phase

Self-logging began, as a pilot program, in October 2013. A few representative experiences are related below.

The New York Power Authority ("NYPA"), a state public power organization, participated in a pilot program and shared its experience during a public webinar.[51] NYPA explained how compliance exceptions and self-logging are implemented and why it will benefit registered entities. NPCC used information gathered from several sources including a 2012 voluntary Entity Impact Evaluation[52] of NYPA and the results of a voluntary 2013 ICE of NYPA to determine the scope of Reliability Standards subject to self-logging. As part of its internal controls structure, NYPA conducts internal investigations of potential compliance concerns, which involve: (i) identification of a concern, (ii) a fact-finding investigation (interviews and evidence collection), (iii) a review of applicable standard requirements and regulatory guidance, (iv) identification of mitigating factors, (v) determination of whether a possible violation occurred and its status (ended or continuing), (vi) an assessment of the potential and actual risks, (vii) analyzing whether it had any previous violations related to the issue, and (viii) mitigation activities in progress or completed. After conducting its internal investigation, NYPA notified NPCC of any noncompliance and its risk assessment. For possible violations identified by

[51] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative%20Workshops/Reliability%20Assurance%20Initiative_RAI_Webinar_6%2019%2014_Final.pdf.

[52] "Entity Impact Evaluation" was a working name for the IRA.

NYPA as minimal risk, NPCC conducted a review and, if NPCC affirmed the minimal risk, included it as a violation in the log.

NYPA maintained and submitted tracking spreadsheets to NPCC at least once every six months. NPCC determined if any of the issues needed further mitigation or enforcement action. The implementation required NYPA to internally assess actual and potential risk, process, track, and remediate issues, have a notification procedure for a possible minimal risk issue, and conduct monthly conference calls with NPCC. During monthly conference calls, NPCC and NYPA reviewed actions from the last meeting, tracked spreadsheets, reviewed and discussed each issue, discussed implementation matters, and reviewed the RAI Pilot Program status. Self-logging allowed NYPA to test and investigate its internal controls and address the steps needed to mitigate possible violations.

The American Transmission Company ("ATC"), a multi-state, transmission-only utility, also participated in the June 2014 webinar. ATC explained the scoping process for its audit and espoused the value of compliance exceptions. ATC also indicated that it views self-logging as essential to a truly risk-based approach to compliance oversight.

After participating in the self-logging pilot, ATC communicated that its compliance program will be further enhanced and structured towards an internal controls framework in the future. ATC predicted that by transitioning into the reliability assurance model, it will strengthen its processes and programs that support the COSO fundamental concepts, refine its internal controls, better define activities to monitor the execution of internal controls, bring more formality and structure to its corrective action process, and enhance its position as "audit ready."

One pilot involved a multiregional registered entity, American Electric Power ("AEP"), one of the largest electric utilities in the U.S. AEP participated in an enforcement pilot with RF, Texas RE, and SPP RE. Based on the results of RF's evaluation of AEP's internal controls, along with other considerations such as AEP's compliance history, its history of self-assessment and self-reporting possible violations, and the quality of its internal controls, AEP logged minimal risk noncompliance (that would otherwise qualify for FFT treatment) of certain CIP standards.

The log, as well as AEP's procedures for maintaining the log and ensuring that noncompliance was discovered, recorded, and mitigated, was periodically checked by the three Regional Entities. After review and approval by the Regional Entities, the minimal risk issues were treated as compliance exceptions.

4. Visibility and Accountability

The ERO Enterprise will continue to have visibility and accountability over all instances of self-logged noncompliance. In practice, as explained in more detail below, in many instances the logged instances of noncompliance may be more comprehensive than self-reports, because of the presumption of compliance exception treatment. The ERO Enterprise will use the information collected through the self-logging program primarily for trending purposes. However, to the extent that items are not properly logged or there is an issue with the risk assessment or mitigation activities, the Regional Entity may, as discussed above, remove the item for processing through any other means and may modify the scope of the entity's ability to log (or exclude the entity from the logging program altogether).

NERC and Regional Entities also will periodically evaluate the registered entities' participation in the self-logging program. If NERC or the Regional Entity determines that a registered entity is no longer eligible to participate in the self-logging program, or if they should adjust the parameters of its participation, NERC or the Regional Entity will provide notice to the registered entity and each other including an explanation of such determination.

5. Benefits of Self-logging

To date, the ERO Enterprise has identified several benefits of self-logging. First, because the minimal risk issues have the presumption of compliance exception treatment, experience has shown, as noted above, that logs often increase visibility into noncompliance detected and corrected at the registered entity. The experience with the program shows that the registered entity may be more likely to record additional information on its log than it would include in a self-report. There are a number of incentives associated with logging of noncompliance. For instance, logged items treated as compliance exceptions will not incur a financial penalty. Further, logged items treated as compliance exceptions are not part of a registered entity's violation history for purposes of aggravation of penalties.[53] Given these incentives, registered entities have shown a greater inclination to identify potential noncompliance, including at times when they may be uncertain about whether the identified issue is a noncompliance.

Second, the program fosters efficiency and reduces certain formal administrative processes associated with individual Self-Reports. As mentioned previously, efficiency does not

[53] As explained above, a compliance exception is part of a registered entity's compliance history only to the extent that it serves to inform the ERO Enterprise of potential risk.

necessarily mean less time or effort. Rather, it is using the requisite time, knowledge, and skills required for each circumstance. Once there is an understanding of the registered entity's internal processes associated with identification, assessment, and correction of noncompliance, and there is an alignment as to the expectations of the Regional Entity regarding the type of information to be included in the log, including for the risk assessment, the entities participating in the program have reported efficiency gains.

The third benefit of self-logging is that the log is an ideal forum for trend spotting because all minimal risk issues related to a particular area and the mitigation associated with them are contained on the log. Experience has shown that the log review and discussion may trigger productive dialogue between the Regional Entity and the registered entity regarding expanding mitigating activities to prevent broader issues in the future.

Fourth, because the registered entity must do its own risk assessment in order to determine whether the noncompliance qualifies for self-logging, and because the rationale contained within the log must support the risk assessment, Regional Entities see more analysis of risk on the registered entity's part when it comes to noncompliance with Reliability Standards than is common in self-reports.

Finally, self-logging is a valuable tool to recognize management practices around Reliability Standards and good performance on the part of registered entity, and at the same time allow the Regional Entities to focus time and resources on issues that pose a greater risk to reliability of the BPS.

6. Oversight by NERC

The Regional Entities inform NERC of registered entities allowed to self-log minimal risk noncompliance. NERC exercises oversight over the program to ensure it is administered consistently and appropriately.

Regional Entities document the factors they analyzed when determining the eligibility of each registered entity to self-log. In accordance with the program document,[54] this documentation includes (i) evaluation of the registered entity's compliance history, (ii) consideration of the timing and quality of the registered entity's Self-Reports, (iii) assurance of the registered entity's ability to assess the risk of noncompliance accurately, (iv) examination of the registered entity's mitigation performance, (v) review of the registered entity's internal compliance program documents, including the date of the latest review, (vi) determination of the registered entity's risk, including the results of an Inherent Risk Assessment, if applicable, (vii) justification for the scope of Reliability Standards for which the registered entity is permitted to self-log, and (viii) a description of the Regional Entity's structure and process for reviewing requests to join the self-logging program, including the department(s) responsible for making eligibility decisions.

NERC will periodically review the Regional Entities' eligibility determinations. NERC may also request information on eligibility determinations outside of a regular periodic review based on questions about a registered entity's participation.

[54] *Available at:* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Self-logging%20of%20Minimal%20Risk%20Issues%20Program%20Overview.pdf.

VI. CONCLUSION

The ERO Enterprise has developed the concepts, processes, pilots, and programs detailed above to implement a more robust, risk-based program for compliance monitoring and enforcement of Reliability Standards that benefits reliability. These processes are consistent with existing Rules of Procedure and allow registered entities and the ERO Enterprise to focus on areas posing greater risk to the reliability of the BPS while maintaining appropriate visibility over lesser-risk issues. NERC has posted guides and program documents and provided training and outreach efforts related to the new and expanded processes and programs to allow for full implementation in 2015. This implementation will accompany additional training and outreach efforts directed at ERO Enterprise staff and industry stakeholders. NERC oversight of all these risk-based processes and programs will ensure NERC will identify and address additional guidance and training to adapt quickly to specific implementation challenges. In identifying such areas, NERC will consider the feedback from registered entities, Regional Entities, and other stakeholders.

VII. NOTICES AND COMMUNICATION

Notices and communications with respect to this filing may be addressed to the following:

NERC
Gerald W. Cauley
President and Chief Executive Officer
Steven Noess
Director, Compliance Assurance
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595 – facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Sonia C. Mendonca
Associate General Counsel and Senior Director of Enforcement
Teresina A. Stasko
Senior Counsel and Manager of Enforcement Actions
Leigh Anne Faugust
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
sonia.mendonca@nerc.net
teresina.stasko@nerc.net
leigh.faugust@nerc.net

FRCC
Stacey Dochoda
President & Chief Executive Officer
Linda Campbell
Vice President & Executive Director – Standards & Compliance
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 600
Tampa, Florida 33607-8402
(813) 207-7968
(813) 289-5646 – facsimile
sdochoda@frcc.com
lcampbell@frcc.com

MRO
Daniel P. Skaar
President & Chief Executive Officer
Sara E. Patrick
Vice President of Enforcement and Regulatory Affairs
Midwest Reliability Organization
380 St. Peter Street, Suite 800
St. Paul, MN 55102
(651) 855-1760
(651) 855-1712 – facsimile
dp.skaar@midwestreliability.org
se.patrick@midwestreliability.org

NPCC
Edward A. Schwerdt
President & Chief Executive Officer
Stanley E. Kopman
Assistant Vice President of Compliance
Walter Cintron
Manager of Compliance Enforcement
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas-10th Fl.
New York, N.Y. 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
eschwerdt@npcc.org
skopman@npcc.org
wcintron@npcc.org

RF
Timothy R. Gallagher
President & Chief Executive Officer
Robert K. Wargo
Vice President, Reliability Assurance & Monitoring
L. Jason Blake
General Counsel
Megan E. Gambrel
Senior Counsel
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, OH 44131
(330) 456-2488
tim.gallagher@rfirst.org
bob.wargo@rfirst.org
jason.blake@rfirst.org
megan.gambrel@rfirst.org

SERC
R. Scott Henry
President and Chief Executive Officer
Andrea B. Koch
Director of Compliance and Analytics
James M. McGrane
Managing Counsel – Enforcement
SERC Reliability Corporation
3701 Arco Corporate Drive, Suite 300
Charlotte, NC 28273
(704) 357-7372
(704) 357-7914 – facsimile
shenry@serc1.org
akoch@serc1.org
jmcgrane@serc1.org

SPP RE
Ron Ciesiel
General Manager
Southwest Power Pool Regional Entity
201 Worthen Drive
Little Rock, AR 72223-4936
(501) 614-3265
(501) 482-2025 – facsimile
rciesiel.re@spp.org

Texas RE
Jim Albright
Vice President & Chief Program Officer
Curtis Crews, PE
Director, Compliance Assessments
Derrick Davis
Director, Enforcement, Reliability Standards & Registration
Texas Reliability Entity, Inc.
805 Las Cimas Parkway, Suite 200
Austin, TX 78746
(512) 583-4915
jim.albright@texasre.org
curtis.crews@texasre.org
derrick.davis@texasre.org

WECC
Chris J. Luras
Director of Compliance Risk Analysis & Enforcement
Ruben H. Arredondo
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103-1114
(801) 582-0353(801) 883-6894 – facsimile
cluras@wecc.biz
rarredondo@wecc.biz

Respectfully submitted

/s/ Teresina A. Stasko

Gerald W. Cauley
President and Chief Executive Officer
Steven Noess
Director, Compliance Assurance
North American Electric Reliability Corporation
3353 Peachtree Road, N.E.
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560
(404) 446-2595 – facsimile

Charles A. Berardesco
Senior Vice President and General Counsel
Sonia C. Mendonca
Associate General Counsel and Senior Director of Enforcement
Teresina A. Stasko*
Senior Counsel and Manager of Enforcement Actions
Leigh Anne Faugust*
Associate Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net
sonia.mendonca@nerc.net
teresina.stasko@nerc.net
leigh.faugust@nerc.net

Counsel for North American Electric Reliability Corporation

July 16, 2015