NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

The Application of Risk-based Compliance Monitoring and Enforcement Program Concepts to CIP Version 5

October 22, 2014

The purpose of this document is to demonstrate how NERC's Compliance Monitoring and Enforcement Program (CMEP) will apply risk-based concepts to the compliance monitoring and enforcement of Critical Infrastructure Protection Reliability Standards Version 5 (CIP Version 5). NERC will not set forth an independent, separate compliance monitoring and enforcement program for CIP Version 5. Rather, this document provides guidance as industry transitions to CIP Version 5. Additional information regarding Reliability Assurance Initiative (RAI) projects and programs for risk-based compliance monitoring and enforcement may be found in the standalone program documents, which are referenced herein and are available on NERC's RAI webpage.[1]

Introduction

CIP Version 5 represents a significant improvement – and change – over the currently-effective CIP Version 3, as it adopts new cyber security controls and extends the scope of systems that are protected by the CIP Reliability Standards. On November 22, 2013, FERC issued a final rule approving CIP Version 5. Under the FERC-approved implementation plan, registered entities will transition from compliance with currently-effective CIP Version 3 to CIP Version 5, thereby bypassing implementation of CIP Version 4.

In drafting CIP Version 5, the standards drafting team recognized the need to shift from the "zero tolerance" compliance and enforcement approach of the past with respect to several CIP requirements. This was for two reasons. First, while registered entities must identify, control, and minimize noncompliance, it is not reasonable to expect that registered entities will be able to prevent all noncompliance because of the breadth and high frequency of the cybersecurity obligations. Second, individual instances of noncompliance with these requirements in particular are less likely to pose a more-than-minimal risk to reliability. The standards drafting team recognized that, under these circumstances, the enforcement process would better promote the goals of reliability by focusing efforts and resources on avoiding noncompliance that poses a greater risk to reliability. Using an "identify, assess, and correct" approach, specific language in 17 CIP Version 5 requirements would have required registered entities to implement processes, plans, or procedures in a manner that would "identify, assess, and correct" instances of noncompliance. This approach would have required registered entities to develop internal controls and would have enabled noncompliance posing a minimal risk to reliability to be addressed outside of the enforcement process.

In Order No. 791, FERC directed NERC to develop modifications to the CIP Version 5 Standards. Among those modifications, FERC directed NERC to modify the "identify, assess, and correct" language in the 17

[1] http://www.nerc.com/pa/comp/Pages/Reliability-Assurance-Initiative.aspx.

CIP Version 5 requirements that contained it. While expressing its receptivity to other options, FERC indicated its preference that NERC remove the "identify, assess, and correct" language from the body of the standards, and further indicated its preference not to include compliance language in the standards requirements. In lieu of replacing the "identify, assess, and correct" language, FERC suggested that NERC develop a compliance and enforcement approach, through the CMEP, that would empower NERC and the Regional Entities to exercise risk-based enforcement discretion.

The Way Forward: the Reliability Assurance Initiative

In November 2012, the ERO Enterprise launched a multi-year effort, known as RAI, to identify and implement changes to enhance the effectiveness of the CMEP by using a risk-based approach. A risk-based approach is necessary for a proper allocation of ERO Enterprise resources, enables a process that focuses on improved reliability, and encourages registered entities to enhance internal controls, including those regarding the self-identification of noncompliance.

Further, the ERO Enterprise recognized that it is not practical, effective, or sustainable to monitor and treat all compliance issues to the same degree or in the same manner. Compliance monitoring and enforcement must be "right-sized" based on a number of considerations, including risk factors and registered entity management practices related to the detection, assessment, mitigation, and reporting of noncompliance.

In response to Order No. 791, the ERO determined that it would be useful to explain how the compliance monitoring and enforcement of CIP Version 5 will necessarily be shaped by risk-based CMEP concepts. The risk-based CMEP approach incorporates the fundamental rationale and principles of the self-correcting "identify, assess, and correct" language and applies it to all Reliability Standards. This approach:

- Recognizes that not all noncompliance requires formal enforcement action;
- Recognizes and rewards registered entities for efforts to improve internal controls and methods for the prompt self-identification and mitigation of noncompliance;
- Maintains ERO Enterprise visibility into all noncompliance to identify reliability risks and trends; and
- Maintains NERC oversight to identify implementation issues and opportunities for improvement.

The ERO Enterprise is well on its way to implementing the risk-based CMEP approach. Over the course of 2013-2014, the ERO Enterprise tested a number of concepts, processes, and programs for complete implementation in 2015. The ERO Enterprise is gaining experience – now – applying risk-based enforcement concepts to noncompliance with CIP Reliability Standards. For example, a substantial portion of the compliance exceptions that have been processed as part of the limited rollout of that program have resolved instances of noncompliance with CIP Reliability Standards. Beginning in 2015, the ERO Enterprise will consider all minimal risk noncompliance from all registered entities to be eligible for compliance exception treatment.

The risk-based CMEP concepts are discussed below.

Compliance Monitoring of CIP Version 5

The transformation for compliance monitoring involves the use of the oversight plan framework (Framework).[2] The Framework focuses on identifying, prioritizing, and addressing risks to the bulk power system (BPS), which enable each Regional Entity to allocate resources where they are most needed and likely to be the most effective. The result is a compliance oversight plan for each individual registered entity.

The ERO Enterprise's migration to a risk-based strategy for compliance monitoring includes a significant focus on cybersecurity and the CIP Version 5 Reliability Standards. The inherent risk assessment and internal control evaluation will be essential components for the monitoring of compliance with CIP Version 5.

Inherent Risk Assessment (IRA)

The Regional Entities conduct IRAs for the registered entities within their regions. 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, and functions performed, among others. The IRA enables the Regional Entities to tailor oversight appropriately. For example, a Regional Entity may choose not to include in the scope of its monitoring activities certain standards or requirements if the IRA shows less risk to reliability for those standards or requirements for that registered entity. Conversely, a Regional Entity may choose to focus its monitoring on areas for which the IRA shows greater risk.

CIP Version 5 was designed to apply security controls to those systems and processes that could cause the most significant impact to the grid. Therefore, in conducting the IRA for a Responsible Entity under CIP Version 5, the Regional Entity would consider, among other things, the Bulk Electric System (BES) Cyber System Categorization analysis developed pursuant to CIP-002-5.1 R1. This standard provides "bright-line" criteria for registered entities to categorize their BES Cyber Systems based on the impact of their associated Facilities, systems, and equipment, which, if destroyed, degraded, misused, or otherwise rendered unavailable, would affect reliable BES operation.

By understanding the entity's high, medium, and low impact BES Cyber Systems, the Regional Entities are able to tailor the compliance monitoring to the entity's risk and identify which systems in each category should be the focus of compliance monitoring activities.

Internal Control Evaluation (ICE)

Following the IRA, a registered entity may elect to provide information concerning the internal controls it uses to manage reliability risks to help focus the compliance oversight efforts of the Regional Entity. The process by which this evaluation takes place is called the ICE. The ICE is a voluntary process, and registered entities are not obligated to participate. However, the evaluation of internal controls may be

[2] *See, e.g.*, Overview of the ERO Enterprise's Risk-Based Compliance Monitoring and Enforcement Program (Sep. 5, 2014), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Overview%20of%20the%20ERO%20Enterprise's%20Risk-Based%20CMEP.pdf. *See also* 2015 ERO Compliance Monitoring and Enforcement Implementation Plan (Sep. 8, 2014), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Final_2015%20CMEP%20IP_V7_090814.pdf.

especially useful for tailoring compliance monitoring activities in the CIP context, as CIP Version 5 requires system or device level controls on hundreds of facilities that may operate thousands of devices.

As described in the ERO Enterprise Internal Control Evaluation Guide (ICE Guide),[3] the ICE may inform whether a registered entity has implemented effective internal controls that provide reasonable assurance of compliance with Reliability Standards associated with areas of risk identified through the IRA. The Regional Entity uses the IRA to identify the risks applicable to the registered entity and uses the ICE to understand how the registered entity manages or mitigates those risks to further tailor monitoring activities. The ICE is designed to be scalable, recognizing that the make-up of an internal control program will vary in accordance with the registered entity's size and complexity.

Monitoring 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) warranted for a particular registered entity based on reliability risks, as determined through the IRA and, if applicable, ICE processes. The Regional Entity may conduct more resource-intensive compliance monitoring activities with respect to functions or registered entities within its region that can have the most significant impact on reliability of the BPS, as determined through the IRA. For functional roles or registered entities that have a lesser impact on reliability to the BPS, the Regional Entity may tailor compliance monitoring approaches accordingly.

Example of Risk-Based Compliance Monitoring Approach to CIP Version 5

This example will refer to hypothetical entity called "ABC Co."

The Regional Entity performs an IRA for ABC Co., which is located within its region. As determined through the CIP-002-5.1 analysis, ABC Co. has numerous high and medium impact BES Cyber Systems. The Regional Entity considers ABC Co.'s geography, interconnectivity, and functions performed. From this assessment, the Regional Entity determines that workforce capability issues at ABC Co. could pose greater risk to reliability.

Therefore, as a result of its IRA, the Regional Entity proposes to include Reliability Standards that address the security of networks, Supervisory Control and Data Acquisition/Energy Management Systems (SCADA/EMS), and the personnel that support them. As part of its compliance oversight plan for ABC Co., the Regional Entity determines to place special emphasis on the following Reliability Standards for its next Compliance Audit of ABC Co.: CIP-002, CIP-004, CIP-005, and CIP-007.

ABC Co. is confident that its internal controls relating to its networks, SCADA/EMS, and personnel are well-designed and effective. ABC Co. agrees to participate in an ICE. As part of this ICE, ABC Co. provides documentation regarding the following to the Regional Entity:

- Management philosophy and communication in support of its internal compliance program;
- Evidence of yearly compliance assessments performed by independent firms; and

[3] The ERO Enterprise Internal Control Evaluation Guide (Oct. 2014) (ICE Guide), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO%20Enterprise%20Internal%20Control%20Evaluation%20Guide.pdf.

- Internal Audit Division with department goals and measures to ensure compliance with Reliability Standards.

The Regional Entity follows the process set forth in the ICE Guide to identify which of the internal controls provided by ABC Co. are considered "key" in support of the Reliability Standards in scope as part of the compliance oversight plan and should be tested. For example, the Regional Entity may review the following information and validating measures relating to internal controls for CIP-005 R1:[4]

- Electronic Security Perimeter diagrams indicating access points to applicable systems connected to a network via a routable protocol;
- Electronic Access Point network configurations, access lists, or firewall rules;
- The results of annual vulnerability assessments to identify points of access to BES Cyber Systems.

The Regional Entity then begins the process of evaluating the selected key controls in accordance with the methods set forth in the ICE Guide. With the key controls selected for testing, the Regional Entity has the information available to make decisions about the effectiveness of ABC Co.'s internal controls for the in-scope standards and more importantly, the effectiveness of the overall internal control program and whether it provides reasonable assurance of compliance.

In light of the information obtained through the IRA and ICE processes, the Regional Entity decides to define the following compliance monitoring plan for ABC Co.:

- Tri-annual Compliance Audit: ABC Co.'s tri-annual audit would be based primarily on the Reliability Standards identified by the IRA (CIP-002, CIP-004, CIP-005, and CIP-007), with limited reviews and testing of other Reliability Standards. Depending on the results of the ICE, the Regional Entity may adjust the amount of testing to be performed during the audit.
- Guided Self-Certifications: ABC Co. would demonstrate compliance with other applicable Reliability Standards by providing compliance information or evidence of controls through a Self-Certification program customized to ABC Co.'s IRA and ICE results.
- Regular Tests of Key Controls: The Regional Entity would assess any changes to ABC Co.'s internal control program to ensure overall program effectiveness.

Enforcement of Noncompliance for CIP Version 5

Over the past several years, the ERO Enterprise has been migrating to a risk-based strategy of assessing and processing noncompliance. Initially, each instance of noncompliance with the CIP Reliability Standards became a Possible Violation filed in a Notice of Penalty. By introducing the Find, Fix, Track and Report (FFT) process in 2011, the ERO Enterprise recognized that not all violations required the imposition of monetary penalties. The FFT process has successfully resolved over 2,000 instances of noncompliance with the Reliability Standards outside of a Notice of Penalty. Most of these FFTs posed a minimal risk to the reliability of the BPS, and 55% of them involved noncompliance with CIP Reliability Standards.

[4] The list of controls and measures provided here is for illustrative purposes only and should not be interpreted as an exhaustive or complete list of possible controls or an indication of which key controls a Regional Entity may choose to test or find acceptable in a specific case. Registered entities should consult the ICE Guide for further information regarding the ICE process.

Building on its experience with a streamlined process and a reduced record, the ERO Enterprise is implementing two major programs that were developed under RAI to continue the shift toward a risk-based model of enforcement. These programs mark the continued migration away from a "zero tolerance" approach, where all instances of noncompliance are evaluated as Possible Violations. These programs leverage existing internal practices at registered entities relating to self-monitoring, identification, assessment, and correction of noncompliance with Reliability Standards. By appropriately valuing and rewarding such efforts (i.e., by providing a disposition path outside of a formal enforcement action), the ERO Enterprise encourages the enhancement of internal controls and self-identification of noncompliance throughout the industry. These programs include the expansion of risk-based enforcement discretion (compliance exceptions) and the self-logging program.

These risk-based programs embody many of the same risk-based concepts of the "identify, assess, and correct" approach. However, these approaches apply to all Reliability Standards and requirements, not just the 17 CIP Version 5 requirements containing the "identify, assess, and correct" language.

Compliance Exceptions

Since 2013, the ERO Enterprise has exercised discretion when deciding whether to initiate an enforcement action for noncompliance posing a minimal risk to the reliability of the BPS. Issues resolved outside of an enforcement action are referred to as **compliance exceptions.**

Compliance exceptions reflect the "identify, assess, and correct" tenet that not all noncompliance requires processing in a formal enforcement action. Compliance exception treatment is especially appropriate if the registered entity adequately identifies its noncompliance, assesses the risk properly as minimal risk, and corrects (i.e. mitigates) the noncompliance in a timely and appropriate manner. A robust internal compliance program and management practices that led to timely discovery and timely mitigation of noncompliance would create a strong argument in favor of compliance exception treatment. However, all minimal risk noncompliance is eligible regardless of discovery method.

Compliance exceptions are similar to FFT remediated issues in that they will not incur any financial penalty. However, compliance exceptions differ from FFT remediated issues in several important ways. First, compliance exceptions are not subject to formal enforcement processes. Further, 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. Compliance exceptions are not part of a registered entity's violation history for purposes of aggravation of penalties. Finally, to maintain visibility and allow for appropriate oversight, all compliance exceptions will be documented, submitted to NERC for review, and reported to FERC.

Beginning in 2015, all minimal risk noncompliance from all registered entities will be eligible for compliance exception treatment. Additional information about compliance exceptions is available in the Compliance Exception Overview document.[5]

The ERO Enterprise is gaining experience identifying appropriate CIP noncompliance for compliance exception treatment. A substantial portion of the compliance exceptions processed during the limited

[5] Compliance Exception Overview (Oct. 1, 2014), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Compliance%20Exception%20Overview.pdf.

rollout of the program in 2013-2014 have resolved instances of noncompliance with CIP Reliability Standards.

Self-Logging Program

The self-logging program allows select registered entities with demonstrated effective management practices to self-monitor and identify, assess, and correct (i.e., mitigate) instances of noncompliance to log minimal risk noncompliance that would otherwise be individually self-reported. The Regional Entity confirms, following a periodic submission of the registered entity's log, that the registered entity has adequately identified and described the noncompliance, accurately assessed the risk, and appropriately mitigated the noncompliance. Once the review process is complete, the minimal risk issue is resolved as a compliance exception absent additional risk factors or other issues. 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 registered entity, should not be resolved through the enforcement process or incur a penalty, absent a higher risk to the BPS.

The experience of the ERO Enterprise to date has shown that logs increase visibility into noncompliance detected and corrected at the registered entity, as registered entities are more likely to record instances of noncompliance on their logs than self-report them. Further, the program fosters efficiency and reduces certain formal administrative processes associated with individual Self-Reports.

Participation in the self-logging program is voluntary. Also, the program is not limited to those CIP Version 5 Reliability Standards that originally contained the "identify, assess, and correct" language.

Additional information about the self-logging program, including eligibility, program operation, and the benefits of the program, is available in the Self-Logging of Minimal Risk Issues Program Overview.[6]

Example of Possible Risk-Based Enforcement Approach to CIP Version 5 Noncompliance

For this example, the ABC Co., which is described in the compliance monitoring portion of this document, is again referenced.

ABC Co. discovers that an employee completed CIP cybersecurity training 15 months and two weeks after the date the employee previously completed the training (CIP-004-5.1 R2). ABC Co. has identified this issue as posing a minimal risk to the reliability of the BPS.

If ABC Co. is allowed to self-log this noncompliance, it will log the noncompliance and actions taken to mitigate the noncompliance and prevent recurrence. Following review by the Regional Entity, there is a presumption that the noncompliance will be treated as a compliance exception unless the noncompliance is ineligible for such treatment (e.g., the noncompliance posed a greater than minimal risk, was the result of intentional or willful acts or omissions, or was the result of systemic or significant performance failures).

[6] Self-Logging of Minimal Risk Issues Program Overview (Oct. 1, 2014), *available at* http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Self-logging%20of%20Minimal%20Risk%20Issues%20Program%20Overview.pdf.

If ABC Co. is not allowed to self-log this noncompliance, it may be considered for compliance exception treatment (although there is no presumption). In that case, ABC Co. is encouraged to submit a Self-Report to its Regional Entity.

If the Regional Entity discovered the noncompliance during a Compliance Audit, instead of ABC Co. discovering it on its own, the noncompliance would still be eligible for compliance exception treatment. Whether the minimal risk noncompliance will actually be afforded compliance exception treatment will be determined through a review of the facts and circumstances.

A Regional Entity may determine that compliance exception treatment is not appropriate, for example, when the following facts and circumstances are present:

- Employees have found a way to circumvent the internal controls ABC Co. has in place to ensure the timely completion of training;
- As a result of major turnover in ABC Co.'s compliance department, there is no longer any effective control, practice, or system to ensure training is completed in a timely manner;
- Employees are generally not aware of CIP obligations;
- Multiple employees at ABC Co. are completing training late (or not at all);
- ABC Co. did not discover the issue promptly;
- ABC Co. did not mitigate the issue promptly;
- The underlying issue was foreseeable and could easily happen again (poor internal controls).

In considering whether to afford compliance exception treatment, the Regional Entity may consider, for example, the following facts and circumstances as those weighing in favor of compliance exception treatment:

- ABC Co. had internal controls in place to ensure timely completion of training, including issuing automated training reminder emails and disabling network access when training is not completed on time. However, the employee was on an extended leave, so he did not see the emails or notice when his network access was disabled;
- ABC Co. self-identified the issue through regular reviews of its records;
- ABC Co. has a limited number of employees completing training late;
- ABC Co. experienced an unforeseeable technical issue;
- ABC Co. addressed the issue with its employee promptly;
- The employee completed CIP training in previous years;
- ABC Co. employees are generally aware of CIP obligations.

To summarize, if ABC Co. is allowed to self-log this noncompliance, there is a presumption that the noncompliance will be afforded compliance exception treatment. If ABC Co. is not allowed to self-log this noncompliance, there is no presumption of compliance exception treatment. However, the

noncompliance is still eligible for compliance exception treatment regardless of how it was discovered (e.g., Self-Report, Compliance Audit).