NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Agenda
Compliance Committee

November 1, 2019 | 11:00 a.m. – 12:00 p.m. Eastern

Participant Dial-in: 1-800-479-1004 | Conference ID: 1018665
WebEx: www.readytalk.com | Enter Code: 4469686 | Click "Join"

Introduction and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Announcement

Agenda Items

1. **Follow-up Regarding Action Items from Prior Meeting – Discussion**
2. **2020 Compliance Monitoring and Enforcement Program Implementation Plan* – Update**
3. **Compliance Monitoring and Enforcement Program Quarterly Report* – Update**
   a. Internal Controls
   b. Streamlining in Enforcement
4. **Adjournment**

*Background materials included.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Antitrust Compliance Guidelines

General

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

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

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

Prohibited Activities

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

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

Activities That Are Permitted

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

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

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

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

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

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

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

2020 Compliance Monitoring and Enforcement Program Implementation Plan

Action
Update

Background
The Electric Reliability Organization (ERO) Enterprise[1] Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP) is the annual operating plan used by the ERO Enterprise in performing CMEP responsibilities and duties. The ERO Enterprise executes CMEP activities in accordance with the NERC Rules of Procedure (ROP) (including Appendix 4C), their respective Regional Delegation Agreements, and other agreements with regulatory authorities in Canada and Mexico. The ROP requires development of an annual CMEP IP[2].

The ERO Enterprise is pleased to release an enhanced, user-friendly CMEP IP for 2020. Collectively, NERC and each RE have worked collaboratively throughout this IP's development to streamline the ROP's timing and risk assessment processes into one cohesive narrative, compared to a main IP with several regional appendices as in previous years. By streamlining the development in this manner, the ERO Enterprise believes that it is also more effectively and efficiently fulfilling the timing and risk assessment obligations of the CMEP IP, which will also enhance efforts to modify and adjust going forward. Through this enhancement, the ERO Enterprise will address areas where there may be specific regional considerations in the main risk element description. The ERO Enterprise believes that this will make the IP both more user-friendly and more relevant to registered entities. Specifically, the IP represents the ERO Enterprise's high-level priorities for its CMEP. While the ERO Enterprise will determine individual monitoring decisions for each registered entity based on its unique characteristics, registered entities should consider the risk elements and their associated areas of focus as they evaluate opportunities and their own prioritization to enhance internal controls and compliance operations focus.

Summary
NERC posted the 2020 CMEP IP on September 20, 2019. NERC anticipates posting a revised IP with links to each RE's compliance monitoring schedule in November 2019.

During the implementation year, NERC or an RE may update its portions of the IP. Updates may include, but are not limited to, changes to compliance monitoring processes; changes to RE processes; or updates resulting from a major event, Federal Energy Regulatory Commission (FERC) Order, or other matter. REs submit updates to the NERC Compliance Assurance group, which reviews the updates and makes any necessary changes. When changes occur, NERC posts a revised plan on its website and issues an announcement.

[1] The ERO Enterprise is comprised of NERC and the six Regional Entities (REs), which collectively bring together their leadership, experience, judgment, skills, and supporting technologies to fulfill the ERO's statutory obligations to assure the reliability of the North American bulk power system (BPS).
[2] https://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx, Appendix 4C Section 4.0 (Annual Implementation Plans)

2020 Risk Elements

The 2020 risk elements are included in Table 1 and reflect a maturation of the risk-based approach to compliance monitoring. As the ERO Enterprise and industry continue to become more knowledgeable about the risks that require control emphasis or mitigation, risk elements will focus more on discrete risks. These discrete risks provide focus for measuring current state and validating registered entity progress. By tracking improvements, industry and the ERO Enterprise can justify focusing on different risks in the future.

Compliance monitoring is not the only tool available to address the risks identified. CMEP staff may assist in various forms of outreach with industry to encourage best practices to achieve the common goal of mitigating risk to the BPS.[3] Enforcement may consider these risks when assessing risk for possible noncompliance, assisting with mitigation plans, or assessing penalties.

Table 1: Comparison of 2019 Risk Elements and 2020 Risk Elements

2019 Risk Elements	2020 Risk Elements
Improper Management of Employee and Insider Access	Management of Access and Access Controls
Improper Management of Employee and Insider Access	Insufficient Long-Term and Operations Planning Due to Inadequate Models
Insufficient Operational Planning Due to Inadequate Models	
Spare Equipment with Extended Lead Time	Loss of Major Transmission Equipment with Extended Lead Times
Inadequate Real-time Analysis during Tool and Data Outages	Inadequate Real-time Analysis During Tool and Data Outages
Improper Determination of Misoperations	Improper Determinations of Misoperations
Inhibited Ability to Ride Through Events	Gaps in Program Execution
Gaps in Program Execution	Texas RE: Resource Adequacy

A summary of the reasoning that led to each identified risk element is as follows:

- **Management of Access and Access Controls:** This risk element establishes a focus on the human element of security, one of the descriptors of cyber security vulnerabilities identified in the 2018 Reliability Issues Steering Committee report[4].
- **Insufficient Long-Term and Operations Planning Due to Inadequate Models:** Compliance monitoring should seek to understand how registered entities manage the risk of planning in a changing environment, including the integration of inverter-based resources, increasing dependence on natural gas, and increasingly dynamic loads.

[3] For example, in 2019, the ERO Enterprise noted in its 2019 CMEP IP that it may engage in targeted efforts to understand registered entities' implementation of specific, newer aspects of IRO-008 and TOP-001. NERC, RE, and FERC staff worked in 2019 to better understand the strategies and techniques used by registered entities to perform Real-time Assessments (RTAs) during events where the entity or their Reliability Coordinator or Transmission Operator has experienced a loss or degradation of data or of their primary tools used to maintain situational awareness. A team of staff from NERC, FERC, and the REs began collaborating with a small number of registered entities to focus on the practices and controls to evaluate the effectiveness of RTA implementation as related to the Reliability Standard requirements (e.g., IRO-008 and TOP-001). Aggregated information on potential industry best practices and concerns will be outlined in a public report after completion of the activity, which is expected in 2020.

[4] https://www.nerc.com/comm/RISC/Related%20Files%20DL/ERO-Reliability-_Risk_Priorities-Report_Board_Accepted_February_2018.pdf

- **Loss of Major Transmission Equipment with Extended Lead Times:** Several scenarios can damage expensive, long-lead time, transmission equipment, which can reduce contingency margins while industry implements emergency procedures and works towards replacing the equipment.
- **Inadequate Real-time Analysis during Tool and Data Outages:** Without the right tools and data, operators may not make decisions that are appropriate to ensure reliability for the given state of the system. This risk element establishes a focus on ensuring situational awareness is maintained regardless of Real-time Contingency Analysis status.
- **Improper Determinations of Misoperations:** Post-event reviews to capture lessons learned and how to reduce the impact of future events will be incomplete if not every event is noticed because the relay operations were not reviewed by qualified personnel.
- **Gaps in Program Execution:** Change management weaknesses have led to significant violations related to vegetation contacts, Facility Ratings, and maintenance of Protection System devices.
- **Resource Adequacy (Texas RE):** This risk element is primarily focused on the Texas Interconnection, although facts and circumstances of registered entities elsewhere may warrant similar focus. This risk element aims to ensure that available resources are appropriately managing frequency control and voltage control aspects in the Texas RE Interconnection.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 2

2020 ERO Enterprise Compliance Monitoring and Enforcement Program Implementation Plan

Version 1.0

September 2019

RELIABILITY | RESILIENCE | SECURITY




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

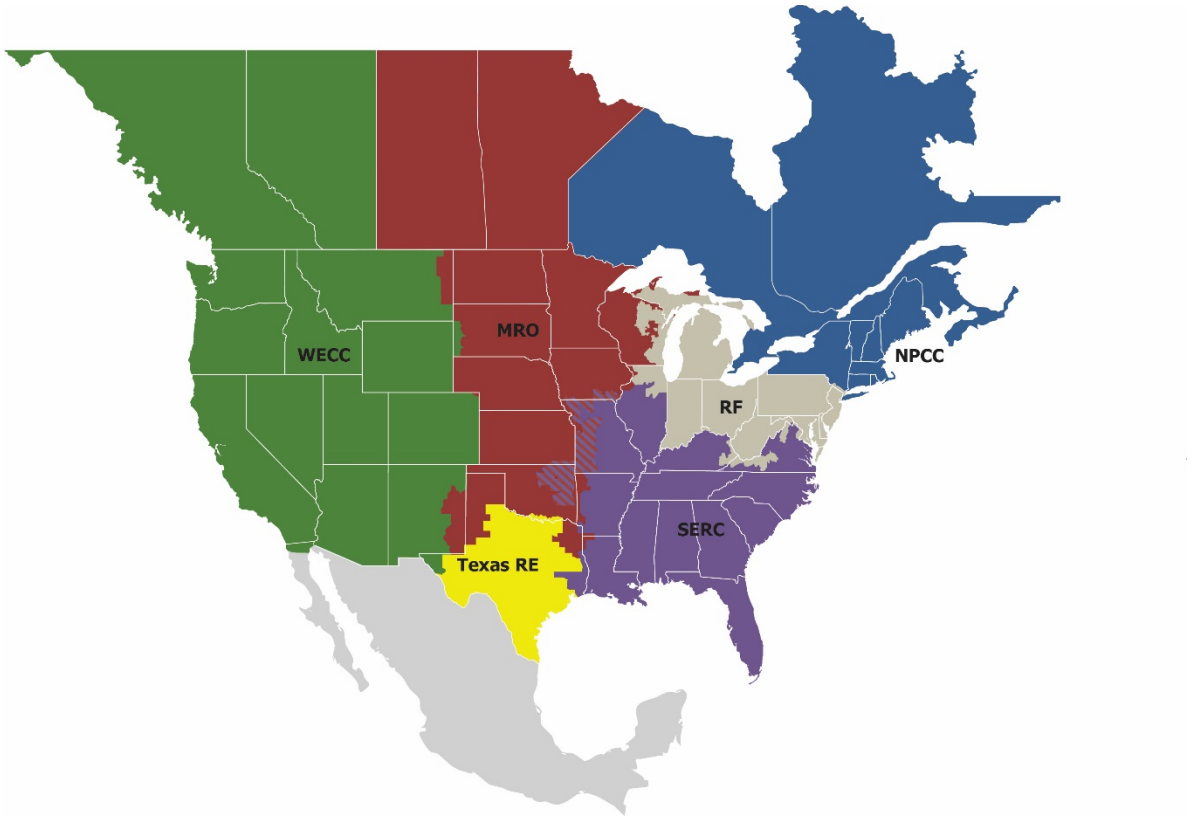
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Region while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Revision History

Version	Date	Revision Detail
Version 1.0	September 2019	• Release of the 2020 ERO CMEP Implementation Plan.

Introduction

Purpose

The Electric Reliability Organization (ERO) Enterprise[1] Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan (IP) is the annual operating plan used by the ERO Enterprise in performing CMEP responsibilities and duties. The ERO Enterprise executes CMEP activities in accordance with the NERC Rules of Procedure (ROP) (including Appendix 4C), their respective Regional Delegation Agreements, and other agreements with regulatory authorities in Canada and Mexico. The ROP requires development of an annual CMEP IP.[2]

The ERO Enterprise is pleased to release an enhanced, easier to use CMEP IP for this year. Collectively, NERC and each RE have worked collaboratively throughout this IP's development to streamline the ROP's timing and risk assessment processes into one cohesive narrative, compared to a main IP with several regional appendices as in years past. By streamlining the development in this manner, the ERO Enterprise believes that it is also more effectively and efficiently fulfilling the timing and risk assessment obligations of the CMEP IP, which will also enhance efforts to modify and adjust going forward. Through this enhancement, the ERO Enterprise will address areas where there may be specific regional considerations in the main risk element description itself. The ERO Enterprise believes that this will make the IP both more user-friendly and relevant to registered entities. Specifically, the IP represents the ERO Enterprise's high-level priorities for its CMEP. While the ERO Enterprise will determine individual monitoring decisions for each registered entity based on its unique characteristics, registered entities should consider the risk elements and their associated areas of focus as they evaluate opportunities and their own prioritization to enhance internal controls and compliance operations focus.

Monitoring Schedules

In November 2019, NERC will post links to each region's compliance monitoring schedule here.

[1] The ERO Enterprise comprised of NERC and the six Regional Entities, which collectively bring together their leadership, experience, judgment, skills, and supporting technologies to fulfill the ERO's statutory obligations to assure the reliability of the North American BPS.

[2] NERC ROP, Appendix 4C Section 4.0 (Annual Implementation Plans).

2020 ERO Enterprise Risk Elements

Process for Risk Elements and Associated Areas of Focus

The ERO Enterprise uses the ERO Enterprise Risk-based Compliance Monitoring Framework (Framework) to identify both ERO-Enterprise-wide risks to the reliability of the BPS and mitigating factors that may reduce or eliminate a given reliability risk. The ERO Enterprise accomplishes this by using the risk element development process.[3] As such, the ERO Enterprise identifies risk elements using data including, but not limited to: compliance findings; event analysis experience; data analysis; and the expert judgment of ERO Enterprise staff, committees, and subcommittees (e.g., NERC Reliability Issues Steering Committee). Reviewed publications include the Reliability Issues Steering Committee's (RISC) report.[4] The State of Reliability Report, [5] the Long-Term Reliability Assessment, publications from the RISC, special assessments, the ERO Enterprise Strategic Plan, and ERO Event Analysis Process insights. The ERO Enterprise uses these risk elements to identify and prioritize interconnection and continent-wide risks to the reliability of the BPS. These identified risks are used to focus compliance monitoring and enforcement activities.

The ERO Enterprise reviewed and reassessed the 2019 risk elements to determine applicability for 2020. Although the IP identifies NERC Reliability Standards and Requirements to be considered for focused CMEP activities, the ERO Enterprise recognizes by using the Framework and other risk-based processes that REs will develop an informed list of NERC Reliability Standards and Requirements specific to the risk a registered entity poses for any monitoring activities. Notably, the implementation plan is not intended to be a representation of just "important" Reliability Standards requirements; rather, it is intended to reflect the ERO Enterprise's prioritization within its CMEP based on its inputs and to communicate to registered entities to bring collective focus within their operations to address each prioritized risk.

Impact of Risk Elements

The REs evaluate the relevancy of the risk elements to the entity's facts and circumstances as they plan CMEP activities throughout the year. For a given registered entity, requirements other than those in the CMEP IP may be more relevant to assist mitigating the risk, or the risk may not apply to the entity at all. Thus, depending on regional distinctions or registered entity differences, focus will be tailored as needed.

The 2020 risk elements are included in Table 1 below and reflect a maturation of the risk-based approach to compliance monitoring. As the ERO Enterprise and industry continue to become more knowledgeable about the risks that require control emphasis or mitigation, risk elements will focus more on discrete risks. These discrete risks provide focus for measuring current state and validating registered entity progress. By tracking improvements, industry and the ERO Enterprise can justify focusing on different risks in the future.

[3] Appendix C, ERO Enterprise Guide for Compliance Monitoring; October 2016

[4] ERO Reliability Risk Priorities; February 2018

5 NERC State of Reliability 2018, available at https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_2018_SOR_06202018_Final.pdf

Compliance monitoring is not the only tool available to address the risks identified. CMEP staff may assist in various forms of outreach with industry to encourage best practices to achieve the common goal of mitigating risk to the BPS.[6] Enforcement may consider these risks when assessing risk for possible noncompliance, assisting with mitigation plans, or assessing penalties.

Table 1: Comparison of 2019 Risk Elements and 2020 Risk Elements

2019 Risk Elements	2020 Risk Elements
Improper Management of Employee and Insider Access	Management of Access and Access Controls
Insufficient Long-Term Planning Due to Inadequate Models	Insufficient Long-Term and Operations Planning Due to Inadequate Models
Insufficient Operational Planning Due to Inadequate Models	
Spare Equipment with Extended Lead Time	Loss of Major Transmission Equipment with Extended Lead Times
Inadequate Real-time Analysis During Tool and Data Outages	Inadequate Real-time Analysis During Tool and Data Outages
Improper Determination of Misoperations	Improper Determination of Misoperations
Inhibited Ability to Ride Through Events	Gaps in Program Execution
Gaps in Program Execution	Texas RE: Resource Adequacy

Management of Access and Access Controls

The protection of critical infrastructure remains an area of significant importance. This risk element establishes a focus on the human element of security, one of the descriptors of cybersecurity vulnerabilities identified in the 2018 RISC report.[7] Regardless of the sophistication of a security system, there is potential for human error. Compliance monitoring should seek to understand how entities manage the risk of access, including insider threat and remote access, and the complexity of the tasks the individuals perform. If security has increased the difficulty in performing personnel's normal tasks, personnel will look for ways to circumvent the security to make it easier to perform their job. On the other hand, when an entity replaces complex tasks with automation, focus should be on:

[6] For example, in 2019, the ERO Enterprise noted in its 2019 CMEP IP that it may engage in targeted efforts to understand entities implementation of specific, newer aspects of IRO-008 and TOP-001. NERC, RE, and FERC staff worked in 2019 to better understand the strategies and techniques used by entities to perform Real-time Assessments (RTAs) during events where the entity or their Reliability Coordinator or Transmission Operator has experienced a loss or degradation of data or of their primary tools used to maintain situational awareness. A team of staff from NERC, FERC, and the Regional Entities (REs) began collaborating with a small number of entities to focus on the practices and controls to evaluate the effectiveness of RTA implementation as related to the Reliability Standard requirements (e.g., IRO-008 and TOP-001). Aggregated information on potential industry best practices and concerns will be outlined in a public report after completion of the activity, which is expected in 2020.

[7] ERO Reliability Risk Priorities; February 2018

1) whether the automation was correctly configured; 2) controls to ensure the automation is operating as intended; and 3) how access, the ability to obtain and use, is implemented.

Harvesting credentials and exploiting physical and logical access of authorized users of BES facilities and Cyber Systems (BCSs) pose a major risk to systems that monitor and control the BES. With the target being users, privileged or non-privileged, who have authorized unescorted physical access and/or various levels of access to critical elements of the BES, the risk becomes elevated. By actively and covertly employing social engineering techniques and phishing emails, attackers may deceive authorized users to harvest credentials and gain unauthorized access.[8]

BES Cyber Systems possibly compromised by unauthorized access using another's credentials is a major business, compliance, and security risk to systems monitor and control the BES. Based on the results of NERC's Remote Access Study, many systems used to operate the BES rely on remote access technologies. Remote access refers to the ability to access a system, application, or data from a remote location. Remote access can take one of two forms: 1) human or user-initiated remote access, referred to as Interactive Remote Access in NERC's CIP Reliability Standards; or 2) automated system-to-system access. Registered entities frequently use Interactive Remote Access technologies to enable remote users to operate, support, and maintain control systems networks and other BES Cyber Systems. Among other things, providing for remote access enables users to efficiently access Cyber Assets to troubleshoot application software issues and repair data and modeling problems that cause application errors. These remote access technologies – while important for efficiently operating, supporting, and maintaining Cyber Assets, including those for control systems – could open up attack vectors. If not properly secured, remote access could result in unauthorized access to a registered entity's network and control systems with potentially serious consequences. For instance, an attacker could breach an environment via remote access by deliberately compromising security controls to obtain privileged access to critical systems. Although registered entities generally do not rely on Internet-facing systems to operate and monitor the BES, malicious actors have demonstrated capabilities to infiltrate systems that are not Internet-facing. Examples of this includes systems designed to run autonomously with minimal human interaction and other mission-critical applications that perform supervisory control that, if misused, could result in serious reliability issues. Additionally, remote devices susceptible to compromise that remotely access a Cyber Asset can serve as a gateway for cyber-criminals to attack networks.

Additionally, malicious code penetration attempts on both the Information Technology (IT) and Operational Technology (OT) systems are on the rise. This Area of Focus brings industry's attention to potentially reduce the attack vectors of hackers, malicious code exploitation, and ransomware penetration.

Mitigation of the identified area's risks is through awareness and technical controls. Entities need to enhance security awareness to include specific topics on social engineering and insider threat. Entities can proactively reduce the insider and external threats by implementing detection and monitoring tools as technical controls. Further, a formalized insider threat management program in place can vastly reduce the associated risk.

[8] US-CERT TA18-074A

Areas of Focus

Table 2: Management of Access and Access Controls			
Standard	**Requirement**	**Entities for Attention**	**Asset Types**
CIP-003-7 CIP-003-8 (eff. 4/1/2020)	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Back up Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-004-6	R4, R5	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-005-5 CIP-005-6 (eff. 7/1/2020)	R1, R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-006-6	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-007-6	R1, R2, R3	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-010-2 CIP-010-3 (eff. 7/1/2020)	R1, R4	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations

CIP-011-2	R1	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	Backup Control Centers Control Centers Data Centers Generation Facilities Substations
CIP-013-1 (eff. 7/1/2020)	R2	Balancing Authority Distribution Provider Generator Operator Generator Owner Reliability Coordinator Transmission Operator Transmission Owner	

Insufficient Long-Term and Operations Planning Due to Inadequate Models

Planning and system analyses are performed for the integration and management of system assets. This includes the analyses of other emerging system issues and trends (e.g., significant changes to the use of demand-side management programs, the integration of inverter-based resources and variable energy resources, changes in load characteristics, increasing dependence on natural gas deliverability for gas-fired generation, increasing uncertainty in nuclear generation retirements, and essential reliability services). NERC's annual Long-Term Reliability Assessment[9] forms the basis of NERC's assessment of emerging reliability issues. The ERO continues to raise awareness on inverter-based resource performance through NERC alerts[10] and industry outreach. Compliance monitoring should seek to understand how entities manage the risk of planning in this changing environment.

Insufficient long-term planning can lead to increased risks to reliability. Adequately modeled planning cases become increasingly critical as a changing resource mix, deployment of new technologies, etc., affect the risk to BPS reliability. For instance, the models should reflect if the power electronic controls of utility-scale inverter-based resources, such as PV resources, give these resources the ability to provide both real and reactive power. As stated in the 2018 RISC report,[11] since the rate of change of the resource mix is increasing, planners will place more emphasis on interconnection-wide studies that require improvement to and integration of regional models. In addition, enhancements to models will be needed to support probabilistic analysis to accommodate the energy limitations of resource additions (such as variable renewable resources). Resource adequacy must look beyond the calculation of reserve margins that assume actual capacity available during peak hours.

Insufficient operational planning can lead to increased risks to reliability. More comprehensive dynamic load models will be needed to sufficiently incorporate behind-the-meter generation and distributed load resources such as demand-side management programs. One of the ways in which the industry can better understand the system is by monitoring load characteristics and the changing nature of load due to Distributed Energy Resources (DER). The NERC Load Modeling Task Force developed a reliability guideline that provides Transmission Planners (TPs) and

[9] https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2018_12202018.pdf

[10] https://www.nerc.com/news/Documents/Inverter%20Alert%20Announcement.pdf

[11] ERO Reliability Risk Priorities; February 2018

Transmission Owners (TOs) with insights into end-use load behaviors and how to capture them in the composition of dynamic load models.[12]

In order to achieve performance expected by the planning models, generating plant protection schemes and their settings should be coordinated with transmission protection, control systems, and system conditions to minimize unnecessary trips of generation during system disturbances.[13]

Planning models are reliant on correct Facility Ratings. See the "Gaps in Program Execution" risk element later in this document for more information.

Additional studies have similarly shown a need to more accurately understand and model inverter-based resource characteristics. NERC has identified adverse characteristics of inverter-based resources in two separate Alerts.[14,15] With the recent and expected increases of both utility-scale solar resources and distributed generation, the causes of a sudden reduction in power output from utility-scale power inverters needs to be widely communicated and addressed by the industry. Entities with increasing inverter-based resources should be aware and addressing this within their models.[16]

Areas of Focus

Table 3: Insufficient Long-Term and Operations Planning Due to Inadequate Models

Standard	Requirements	Entities for Attention	Rationale
MOD-033-1[20]	R1, R2	Planning Coordinator Reliability Coordinator Transmission Operator	Validating planning power flow models.
PRC-023-4	R1, R2, R6	Transmission Owner Generator Owner Planning Coordinator	Ensure protective relay settings do not limit transmission loadability.

[12] NERC Modeling Improvements Initiative Update; May 2018

[13] Industry Recommendation: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings; June 2017

[14] Industry Recommendation: Loss of Solar Resources during Transmission Disturbances due to Inverter Settings - II; May 2018

[15] NERC Modeling Notification: Recommended Practices for Modeling Momentary Cessation Distribution; April 2018

[16] Considerations for Power Plant and Transmission System Protection Coordination, July 2015

PRC-024-2	R1, R2	Generator Owner	Ensure resources stay available during applicable voltage and frequency excursions, especially inverter-based resources.
TPL-001-4	R1	Planning Coordinator Transmission Planner	Ensure accurate System models.

Loss of Major Transmission Equipment with Extended Lead Times

There are several scenarios that can damage expensive, long-lead time transmission equipment which can reduce contingency margins while industry implements emergency procedures and works towards replacing the equipment. These reasons include:

- aging infrastructure coupled with less than adequate maintenance
- failure of large power transformers due to the effects of a Geomagnetic disturbance or other weather-related effect
- any type of intentional (or unintentional) physical or cyber-security breach, including the impacts of an EMP

As the BPS ages, less-than-adequate infrastructure maintenance is a reliability risk that continues to grow. The RISC report identifies that the failure to maintain equipment is a reliability risk exacerbated when an entity either does not have replacement components available or cannot procure needed parts in a timely fashion. The failure to properly commission, operate, maintain, prudently replace, and upgrade BPS assets generally could result in more frequent and wider-spread outages, and these could be initiated or exacerbated by equipment failures.

Spare equipment strategy is an important aspect of restoration and recovery. The strategy should encompass identifying critical spare equipment as part of a national or regional inventory. For example, as part of the changing resource mix supplying power to the BPS, many Blackstart units are being retired; remaining Blackstart units become more critical to ensure proper and timely system recovery. The strategy should also account for the transportation and logistics requirements for replacing critical assets. An improved spare equipment strategy or plan will lead to better contingency planning and possibly faster response times for restoration and recovery. A spare equipment strategy can help strengthen the resiliency for responding to potential physical threats and vulnerabilities.[17]

[17] CIP-014-2 Guidelines and Technical Basis, Requirement R5

Areas of Focus

Table 4: Loss of Major Transmission Equipment with Extended Lead Times			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
EOP-005-3	R7	Transmission Operator	Assess whether unavailability of Blackstart units and their associated systems, including Blackstart paths have been considered in the entity's spare equipment strategy.
TPL-001-4	R2.1.5	Planning Coordinator Transmission Planner	Ensure that unavailability of major Transmission equipment has been considered in the entity's spare equipment strategy.

Inadequate Real-time Analysis during Tool and Data Outages

Without the right tools and data, operators may not make decisions that are appropriate to ensure reliability for the given state of the system. NERC's ERO Top Priority Reliability Risks 2014-2017 notes that "stale" data and lack of analysis capabilities contributed to the blackout events in 2003 ("August 14, 2003 Blackout") and 2011 ("Arizona-Southern California Outages"). Certain essential functional capabilities must be in place with up-to-date information available for staff to use on a regular basis to make informed decisions.

Specifically, entities are to be encouraged to have realistic plans to continue real-time analysis during outages of tools, loss of data, or both. The 2018 RISC report[18] identifies that loss of situational awareness can be a precursor or contributor to a BPS event. This risk element is made more important in situations where planning models may not keep pace with increasing BPS complexity and accurately reflect area-specific dependencies on inverters, natural gas, or other items identified in the other 2020 risk element "Insufficient Long-Term and Operations Planning Due to Inadequate Models". Forecasting BPS resource requirements to meet customer demand is becoming increasingly difficult due to the penetration of DER which can mask the customer's electric energy use and the operating characteristics of distributed resources without sufficient visibility.

Registered entities should be able to clearly demonstrate their plan and the capability and feasibility of the entities skilled workforce to implement the plan within a reasonable time frame. Compliance monitoring should include a keen eye on events and the human evaluation rather than simply looking at RTCA scans. RTCA is a tool to help achieve the intent of these requirements, but RTA is the human evaluation of computer generated results and other relevant inputs. While the two are linked in this process, simply having RTCA running in the background does not constitute an assessment of the system (i.e., an RTA).

This risk element will be reevaluated pending the results of ongoing activities. The ERO Enterprise and FERC staff are seeking to better understand the strategies and techniques used by entities to perform RTAs during events where the entity or their Reliability Coordinator or Transmission Operator has experienced a loss or degradation of data or of their primary tools used to maintain situational awareness. A team of staff from NERC, FERC, and the Regional Entities (REs) are collaborating with a small number of entities in 2019 to focus on the practices and controls to evaluate the effectiveness of RTA implementation as related to the Reliability Standard requirements (e.g., IRO-008 and TOP-001).

[18] ERO Reliability Risk Priorities; February 2018

Aggregated information on potential industry best practices and concerns will be outlined in a public report after completion of the activity.

Areas of Focus

Table 5: Inadequate Real-time Analysis during Tool and Data Outages			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
IRO-008-2	R4	Reliability Coordinator	Ensuring situational awareness is maintained regardless of RTCA status
TOP-001-4	R13	Transmission Operator	Ensuring situational awareness is maintained regardless of RTCA status

Improper Determination of Misoperations

Protection systems are designed to remove equipment from service so the equipment will not be damaged when a fault occurs. Protection systems that trip unnecessarily can contribute significantly to the extent of an event. When protection systems are not coordinated properly, the order of execution can result in either incorrect elements being removed from service or more elements being removed than necessary. Such coordination errors occurred in the Arizona-Southern California Outages (see recommendation 19),[19] the August 14, 2003 Blackout (see recommendation 21),[20] and the Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015 (see recommendation 2).[21]

Furthermore, a protection system that does not trip–or is slow to trip–may lead to the damage of equipment (which may result in degraded reliability for an extended period of time), while a protection system that trips when it should not can remove important elements of the power system from service at times when they are needed most. Unnecessary trips can even start cascading failures, as each successive trip can cause another protection system to trip.

The 2018 RISC report[22] includes a key point that the ERO Enterprise, the impacted organizations, and the respective forums and trade organizations should perform post-event reviews to capture lessons learned and how to reduce the impact of future events. These reviews will be incomplete if not every event is noticed because the relay operations were not reviewed by qualified personnel. The report also identifies the risk posed by the increasing complexity in protection and control systems, further emphasizing the importance of a skilled workforce analyzing events and relay operations. Understanding how an entity uses controls can help promote best practices in this area.

Areas of Focus

Table 6: Improper Determination of Misoperations			
Standard	**Requirements**	**Entities for Attention**	**Rationale**
PRC-004-5(i)*	R1, R3	Generator Owner Transmission Owner	Ensure proper analysis of protection system operations.

[19] See Arizona-Southern California Outages on September 8, 2011

[20] See Final Report on the August 14, 2003 Blackout

[21] See Washington, D.C., Area Low-Voltage Disturbance Event of April 7, 2015

[22] ERO Reliability Risk Priorities; February 2018

Gaps in Program Execution

The ERO Enterprise has observed an increase in FAC-003-3 R2 violations resulting in vegetation contacts. These violations result from vegetation management programs that have less than adequate procedures to address identified problems or that fail to adapt to changing conditions, e.g., increased precipitation that accelerates vegetation growth.[23]

Change management weaknesses have also led to significant violations related to Facility Ratings and maintenance of Protection System devices. Some registered entities have Facility Ratings based on inaccurate equipment inventories, or ratings are not being updated during projects or following severe weather. Where records are not kept up to date, inaccurate models and damaged equipment can result. Failing to keep accurate inventories of equipment, following asset transfers, addition of new equipment, or mergers and acquisitions, is also resulting in incomplete Protection System Maintenance and Testing Programs that jeopardize the functionality of the equipment to respond to faults or disruptions on the electric system.

Areas of Focus

Table 7: Gaps in Program Execution

Standard	Requirements	Entities for Attention	Rationale
CIP-002-5.1a	R1, R2	Balancing Authority Generator Owner Transmission Operator Transmission Owner Reliability Coordinator	Ensuring entities maintain complex programs which handle large amounts of data, e.g., accurate inventories of equipment, following asset transfers, addition of new equipment, etc.
CIP-010-2 CIP-010-3 (eff. 7/1/2020)	RI	Balancing Authority Generator Owner Transmission Operator Transmission Owner Reliability Coordinator	
FAC-003-4	R1, R2, R3, R6, R7	Generator Owner Transmission Owner	
FAC-008-3	R6	Generator Owner Transmission Owner	
PRC-005-6	R3	Generator Owner Transmission Owner	

Texas RE: Resource Adequacy

This risk element is primarily focused on the Texas interconnection, although facts and circumstances of entities elsewhere may warrant similar focus. This risk element aims ensuring the available resources are appropriately managing frequency control and voltage control aspects in the Interconnection. The need to actively monitor reactive resources within the system to ensure that voltage variations are minimized, preventing outages and damage to BES equipment, has been recognized as a risk. While voltage is generally a localized concern, there have been changes in the ERCOT Interconnection that have facilitated the use of more dynamic and static reactive devices in more areas. Additionally, there are several load pockets where the management of reactive resources plays a significant role in

[23] *See* Notices of Penalty filed June 27, 2019 in FERC Docket No. NP19-13-000, August 30, 2018 in FERC Docket No. NP18-23-000, and May 31, 2018 in FERC Docket Nos. NP18-11-000, NP18-12-000, and NP18-13-000

ensuring reliability. While frequency control metrics are being maintained at a high level, the shift in resource mix warrants appropriate compliance monitoring. The impact on system inertia is a risk as the resource mix continues to evolve. The load growth coupled with record breaking wind penetration puts an emphasis on managing the frequency before, during, and after events. Resources should have appropriate controls in place to support reliable operations as the resource mix within this Interconnection continues to change. All entities should have proper plans in place to act and react to operational risks.

Areas of Focus

Table 8: Texas RE: Resource Adequacy

Standard	Requirements	Entities for Attention	Rationale
BAL-001-TRE-1	R9, R10	Generator Owner	(Where applicable) Ensure generating resources achieve expected frequency response.
PRC-024-2	R2	Generator Owner	Ensure proper availability of generating resources.
VAR-002-4.1	R2	Generator Owner	Ensure generating resources maintain their given generator voltage or Reactive Power schedule.

Agenda Item 3
Compliance Committee
Open Meeting
November 1, 2019

Compliance Monitoring and Enforcement Program Quarterly Report

Action
Update

Background
As part of the Compliance Monitoring and Enforcement Program quarterly report, NERC staff will discuss recent activities related to the harmonization of internal control evaluations and Compliance Oversight Plans, as well as streamlining activities in enforcement.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Agenda Item 3

Compliance Monitoring and Enforcement Program Quarterly Report

Q3 2019

November 1, 2019

RELIABILITY | RESILIENCE | SECURITY




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

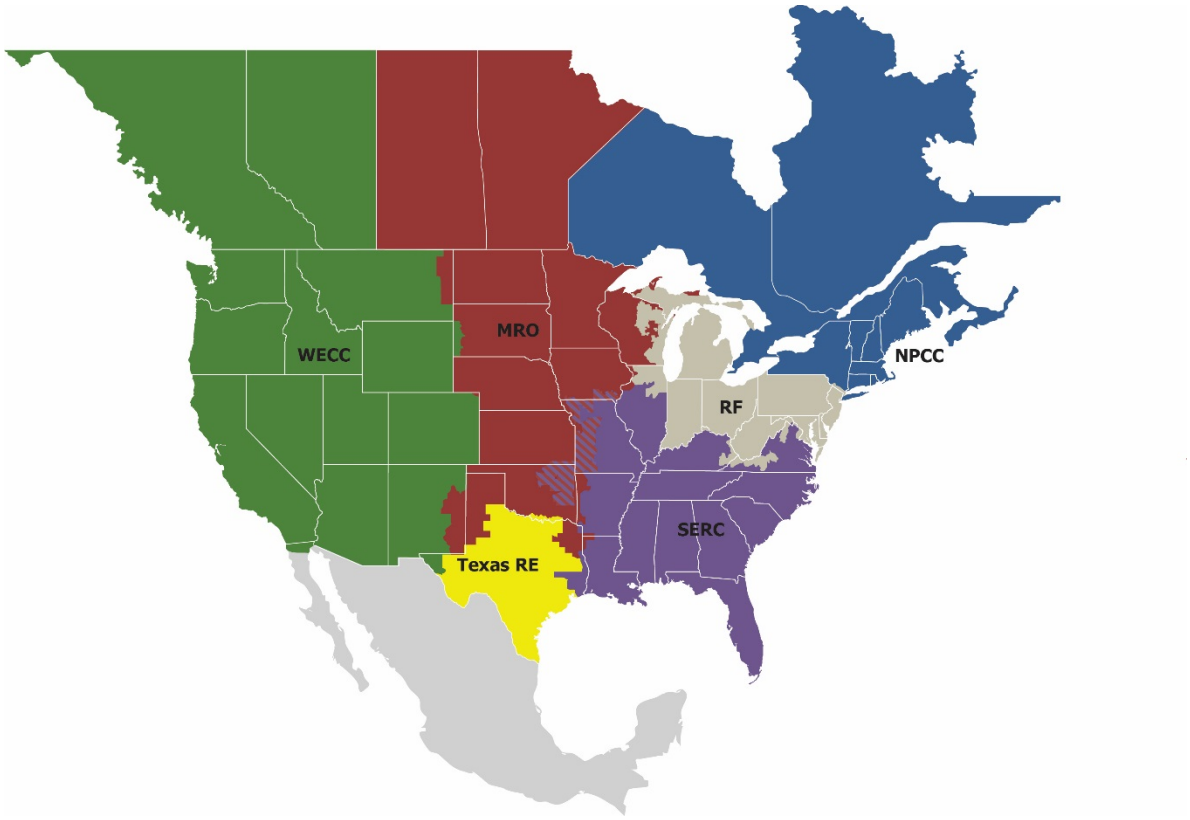
Table of Contents

Preface

Electricity is a key component of the fabric of modern society, and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is divided into six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners/Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Executive Summary

This report highlights key ERO Enterprise[1] Compliance Monitoring and Enforcement Program (CMEP) activities that occurred in Q3 2019 and provides information and statistics regarding those activities.

In Q3 2019, CMEP activities throughout the ERO Enterprise reflected continued implementation of a risk-based approach and program alignment. The ERO Enterprise:

- Approved two multi-region registered entities (MRREs) for entry into the Coordinated Oversight Program,
- Certified one new Reliability Coordinator and reviewed one already-certified and operational registered entity,
- Processed 46 functional registration changes,
- Completed one Bulk Electric System (BES) Registration Exception Request,
- Filed one Full Notice of Penalty (NOP),
- Filed 12 Spreadsheet Notices of Penalty (SNOP), and
- Began to develop the revised Compliance Oversight Plan template.

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

Chapter 1: CMEP Activities

Program Alignment

The ERO Enterprise is enhancing alignment of CMEP activities under a broader ERO Enterprise Program Alignment Process (Program Alignment).[2] In Q3, NERC staff received two new cases submitted through the Reporting Tool and NERC added four CMEP Practice Guides, resulting in six open issues.

NERC staff, along with Compliance and Certification Committee (CCC) Alignment Working Group (AWG) members, provided Program Alignment outreach at the two-day Compliance and Standards Workshop held in Minneapolis during Q3.

Coordinated Oversight Program

The purpose of the Coordinated Oversight Program is to increase efficiency and eliminate unnecessary duplication of compliance monitoring and enforcement activities for MRREs. A registered entity operating in or owning assets in two or more REs' jurisdictions with one or more NERC Compliance Registry (NCR) identification number is a potential candidate for inclusion in the voluntary Coordinated Oversight Program. In connection with the program, the ERO Enterprise takes into account reliability considerations such as, but not limited to, a registered entity's registered functions, load and generation capacity, transmission assets, and transmission and generation control centers.

In Q3 2019, the ERO Enterprise approved two additional MRREs for entry into the Coordinated Oversight Program, increasing the total count of registered entities participating to 211.[3]

[2] http://www.nerc.com/pa/comp/Pages/EROEnterProAlign.aspx

[3] Appendix B includes further information on the MRREs participating in the Coordinated Oversight Program.

Chapter 2: RE Oversight

Enforcement Oversight

Serious Risk Issues

NERC filed one Full NOP, Docket No. NP19-16 in Q3 of 2019, resolving seven violations of Critical Infrastructure Protection (CIP) Reliability Standards with a $2,100,000 penalty. The entity installed servers, and correctly designated the servers as Critical Cyber Assets requiring specific protections included in the CIP Standards; however, the entity did not realize that the CIP Standards also applied to certain subcomponents of the server separately, apart from the servers. The entity did not use the documentation tools it developed to ensure that the server's subcomponents were given the appropriate and applicable CIP protections.

Spreadsheet NOPs

In Q3 2019, NERC filed 12 SNOPs that included 37 violations of NERC Reliability Standards and carried a total combined penalty of approximately $283,000. Twenty-one of the violations were violations of the CIP Reliability Standards, while the remaining 16 were violations of non-CIP Reliability Standards.

Annual Find, Fix, Track, and Report and Compliance Exception Programs Review

In Q3, NERC filed the closure letter for FY2018 Annual Find, Fix, Track, and Report and CE program review with the Federal Energy Regulatory Commission (FERC). NERC also started planning for the next review for FY2019 in conjunction with FERC.

Compliance Monitoring Oversight

NERC Oversight

In Q3, NERC executed monitoring oversight activities planned for 2019. These activities include the following:

- RE-specific follow-up related to prior oversight recommendations,
- Planned audit observation activities, and
- Recurring oversight coordination specific to ERO Enterprise efforts around Compliance Oversight Plan enhancement and alignment during 2019.

Inherent Risk Assessment Completion and Compliance Oversight Plans

During Q3 2019, RE progress toward completion of initial Inherent Risk Assessments (IRAs) continued on track according to regional plans.[4] By the end of 2019, all REs will have completed initial IRAs for all registered entities and will continue to update existing IRAs. IRA updates and initial IRAs for newly registered entities will consider registered functions, risk priorities, and regional resources. REs continue to conduct internal control review activities and implement processes for conducting reviews of internal controls during CMEP activities, such as Compliance Audits.

Additionally, REs started to develop Compliance Oversight Plans (COPs) using results of the IRA and performance considerations such as internal controls, mitigation plans, compliance history, event analysis trends, or other regional considerations to identify key risks. COPs will include the NERC Reliability Standards associated with identified risks, the interval of monitoring activities, and the type of CMEP tool(s) (such as Compliance Audit, Spot Check, or Self-Certification). NERC will continue to monitor development of COPs throughout the remainder of 2019 to ensure ERO Enterprise alignment.

[4] Additional information regarding the percentage of IRAs completed for all registered entities within each RE across the ERO Enterprise is available in Appendix B. REs will continue to prioritize IRA completions based on registered functions and registration changes throughout the year.

Compliance Guidance

During Q3 2019, the ERO Enterprise received one new proposed Implementation Guidance document. Three Implementation Guidance documents received in late Q2 2019 are in the final stages of the review and endorsement process.

Certification

Q3 Certification Completions

In Q3 of 2019, the ERO Enterprise completed certification of one new Reliability Coordinator in the Western Interconnection and completed the review of changes to the footprint of one already certified and operational Transmission Operator. Additionally, six new entity certifications are in process with one initial site visit not yet completed. Ten certification reviews are in process with three initial site visits scheduled for the fourth quarter. Appendix D provides a breakdown by RE and by function.

Registration

In Q3 of 2019, NERC processed 46 Registration Changes of which 28 were functional activations and 18 were functional deactivations. Of the 18 functional deactivations:

- One was determined not to meet registration criteria,
- Two were due to facility shutdown,
- Four were assets being sold to another registered entity, and
- Eleven were due to compliance responsibility being assumed by another registered entity.

BES Registration Exceptions

In Q3 of 2019, NERC completed one Exception Request in MRO. NERC is currently reviewing one additional Exception Request already approved by WECC and is expecting to complete this review in Q4 of 2019.

Chapter 3: ERO Enterprise Performance Objectives

Priorities for 2019

To guide CMEP Activities throughout 2019, NERC identified the following key objectives in support of the ERO Enterprise Operating Plan goal of risk-informed Entity Registration, Compliance Monitoring, Mitigation, and Enforcement:

- Review effectiveness of the Compliance Guidance program and develop a plan to enhance the program. In Q3, NERC provided a survey to the developers, submitters, reviewers, and users of Compliance Guidance to solicit feedback on the effectiveness of the program and improvement opportunities. NERC will evaluate the responses during Q4 and put together a plan for addressing the feedback by the end of 2019.
- Evaluate opportunities to expand industry-led development of guidance to other program areas as a part of the Compliance Guidance project discussed in the previous bullet. This evaluation will, in part, be accomplished through the survey sent out in Q3.
- NERC has completed its priority to enhance the CMEP Practice Guide development process to solicit and incorporate feedback from NERC Committees (e.g. CCC, Critical Infrastructure Protection Committee). The Practice Guide now includes NERC Committee feedback as part of its workflow in development of CMEP Practice Guides. At the end of Q3, NERC provided four Practice Guides to the CCC AWG for review.
- Track the development and completion of CMEP Practice Guides through the Program Alignment Issues and Recommendations Tracking spreadsheet located on NERC's website. The four Practice Guides provided to the CCC AWG were also added to the Program Alignment Issues and Recommendations Tracking spreadsheet.
- Provide training and education on control evaluations to industry with supporting guidance to the REs for consistent implementation in audits. In Q3, the ERO Enterprise continued to conduct outreach on the revised COP template. The ERO Enterprise has developed common COP outreach that NERC and each RE will provide through a workshop or other forum by the end of 2019. Part of the revisions to the COP includes the integration of controls.
- NERC has completed its priority to present on controls-related topics for industry during the July 2019 Compliance and Standards Workshop. This included presentations by several REs on understanding controls during compliance monitoring activities, a panel discussion on good practices and lessons learned from control implementation by industry members, and a presentation by NERC staff on control integration in the enforcement process; and
- Improve alignment in processes across REs and – when appropriate – memorialize the aligned processes into the design of the CMEP Tool. A key part of the Align project included deliberate review of business practices across all CMEP activities, resulting in harmonization of primary CMEP processes that will be incorporated into Align. For Q3, the ERO Enterprise continued to support the development of Align and discussed evidence-gathering processes and possible solutions related to Align with industry members in October.

Appendix A: Enforcement

CMEP Metrics

Mitigation Completion Status

Figure A.1 shows the current percentage of mitigation completion by discovery year. Table A.1 shows the progress in mitigation completion in Q3 compared to previous quarters. NERC continues to monitor completion status of all violations based on the expected completion dates.

Table A.1: Violations With Mitigation in Progress in 2019

Discovery year	Q3	Q2	Q1
2019	77.4%	86.7%	95.4%
2018	40.1%	51.2%	63.9%
2017	16.6%	21.2%	27.5%
2016	5.5%	6.5%	8.0%
2015	0.8%	0.8%	0.8%

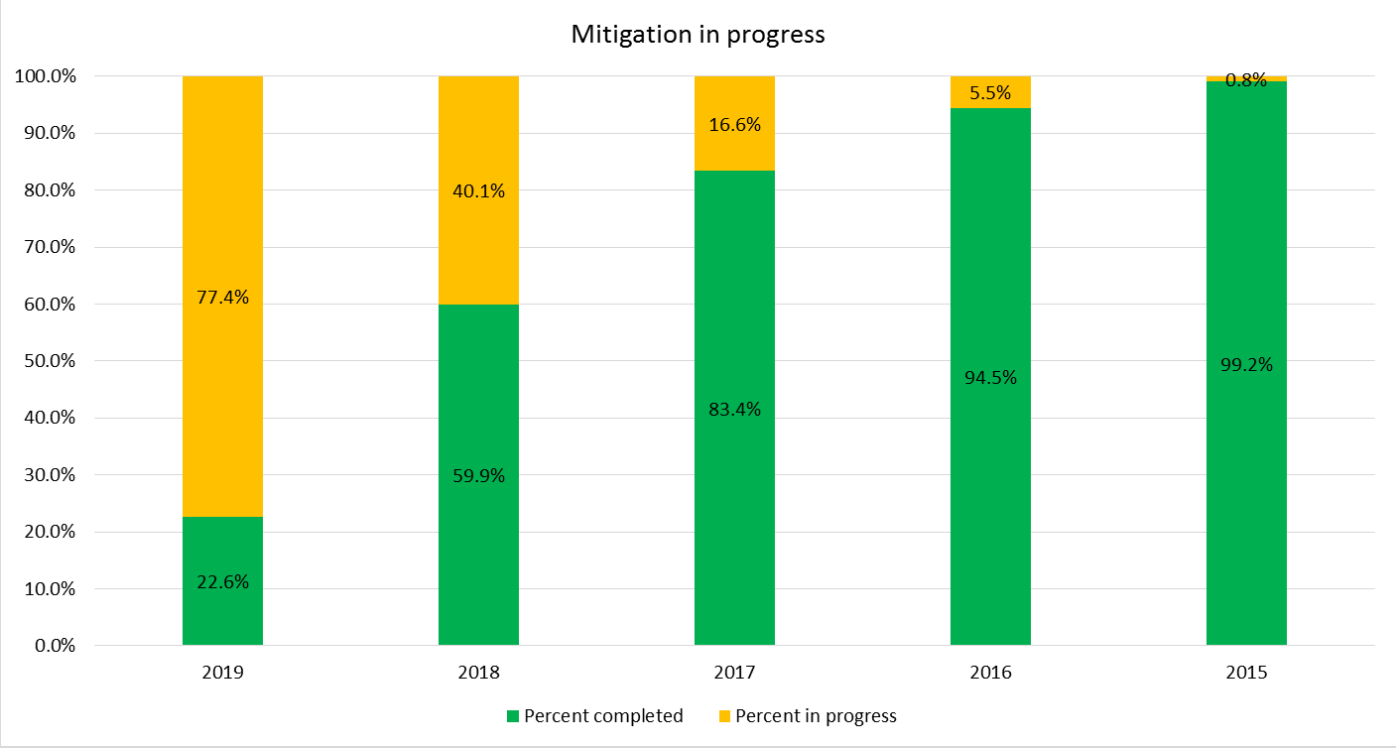


Figure A.1: Mitigation Completion by Discovery Year

Age of Noncompliance in ERO Enterprise Inventory

Figure A.2 shows all noncompliance in the ERO Enterprise inventory, organized by discovery year.[5] Twenty percent of the ERO Enterprise inventory is more than two years old. The ERO Enterprise is committed to resolving the oldest violations while also assessing and ensuring mitigation of newly discovered noncompliance.

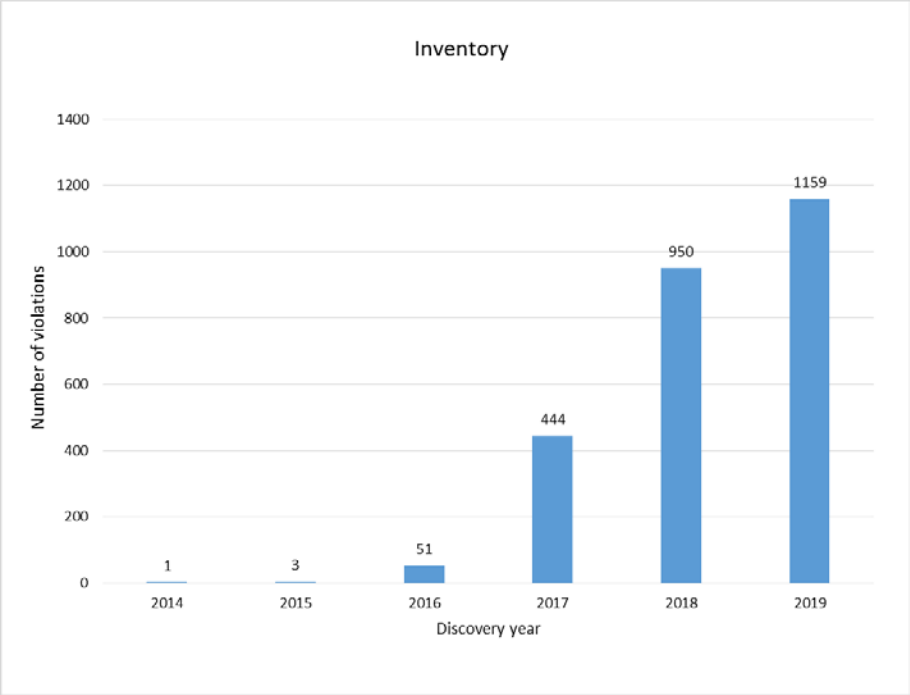


Figure A.2: Age of Noncompliance in the ERO Enterprise Inventory

Disposition of Noncompliance

Figure A.3 shows the percentage of all noncompliance processed by disposition type through the end of Q3 2019. The ERO Enterprise processed a majority of instances of noncompliance in Q3 as Compliance Exceptions.

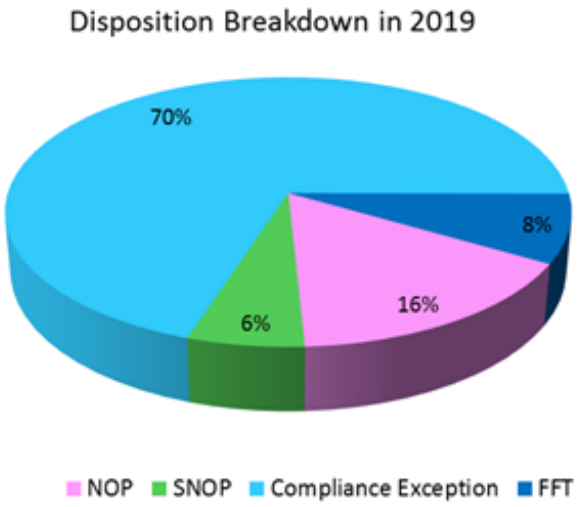


Figure A.3: Disposition Type of Noncompliance Processed in 2019

[5] The number of instances of noncompliance in the inventory is often higher than the number of instances of noncompliance that is unmitigated because registered entities may complete their mitigating activities while enforcement disposition is under review and determination.

Vegetation Management

NERC regularly reports on vegetation-related Sustained Outages. Figures A.4 and A.5 show transmission outages from Category 3 (Sustained Outages caused by vegetation falling into applicable lines from outside the right-of-way) and those outages that resulted in violations of FAC-003.[6] FAC-003 issues are posted on the NERC website. Nineteen sustained outages from vegetation fall-ins from outside of the transmission right-of-way have been reported in 2019.[7]

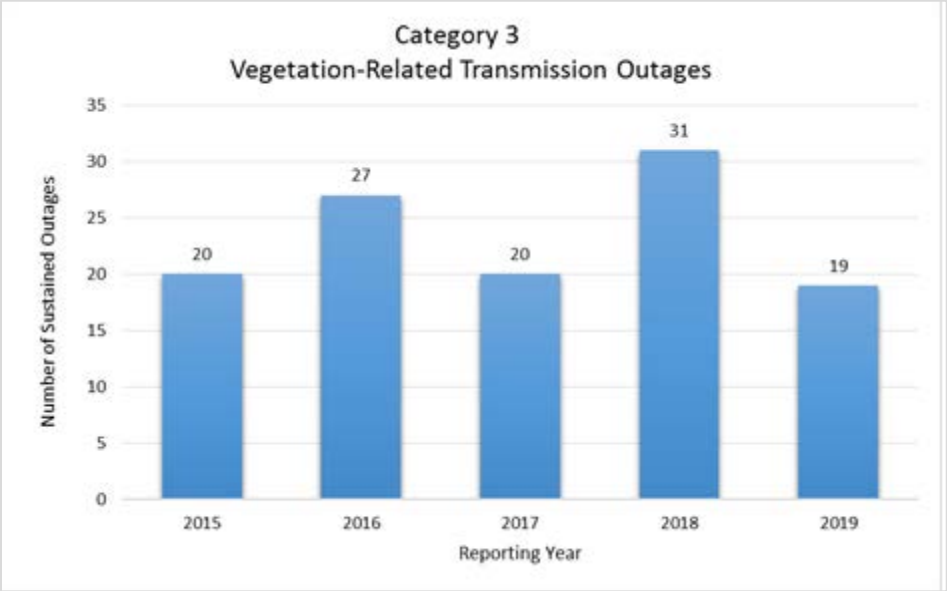


Figure A.4: Category 3 Transmission Outages

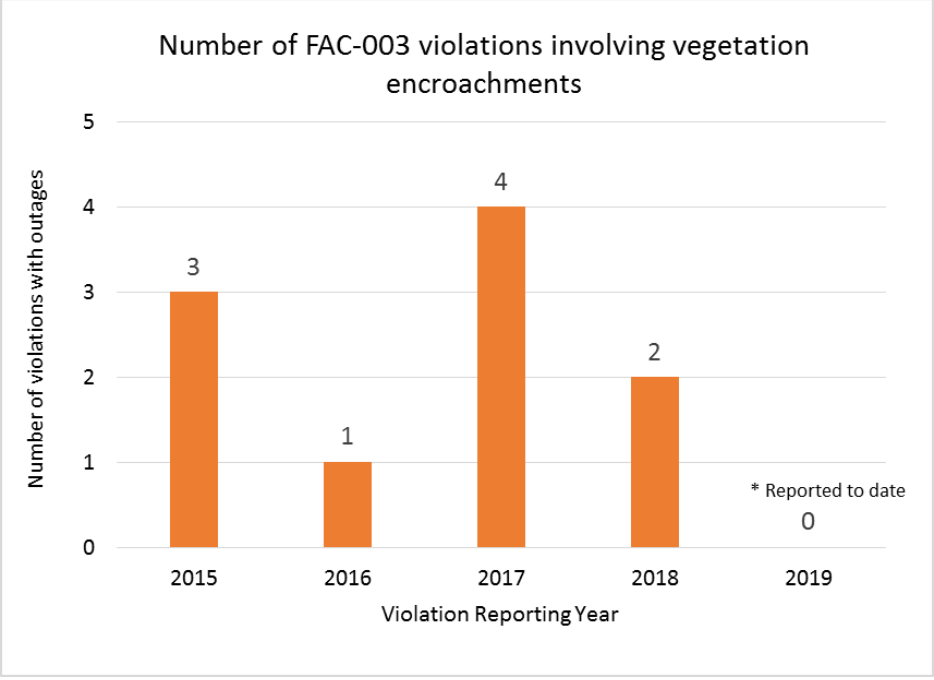


Figure A.5: FAC-003 Violations

[6] Filed violations.

[7] Please note the periodic data reporting timing per FAC-003. The number in this report reflects outages submitted by the end of Q2 2019 periodic data reporting.

Serious Risk Averages

Figures A.6 and A.7 show the percentage of serious risk violations over a rolling three-year average. The percentages are determined based on the number of serious risk violations compared to the total number of noncompliance filed in a given three-year period. Figure A.6 shows the breakdown for non-CIP noncompliance, and Figure A.7 includes CIP violations.

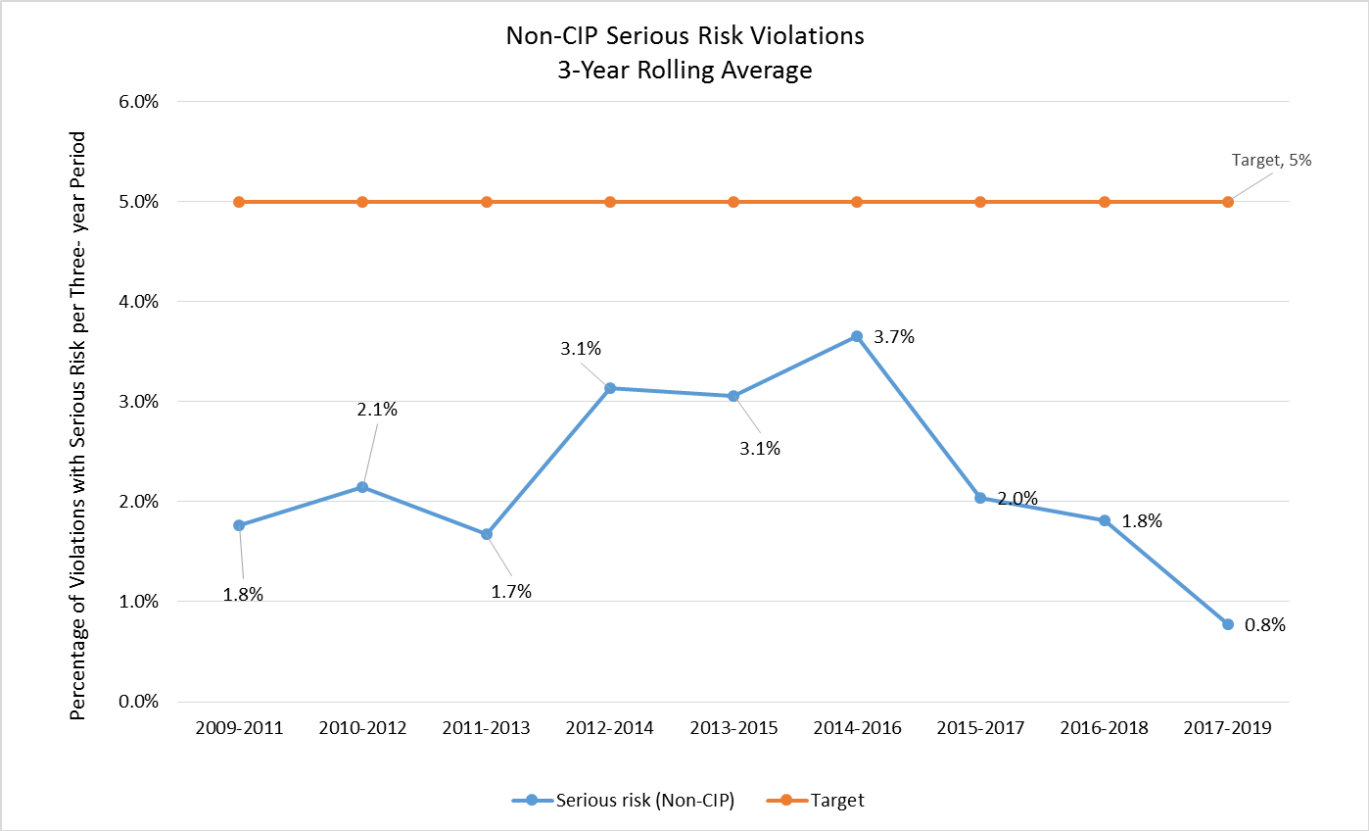


Figure A.6: Rolling Average of Serious Risk Violations (non-CIP)

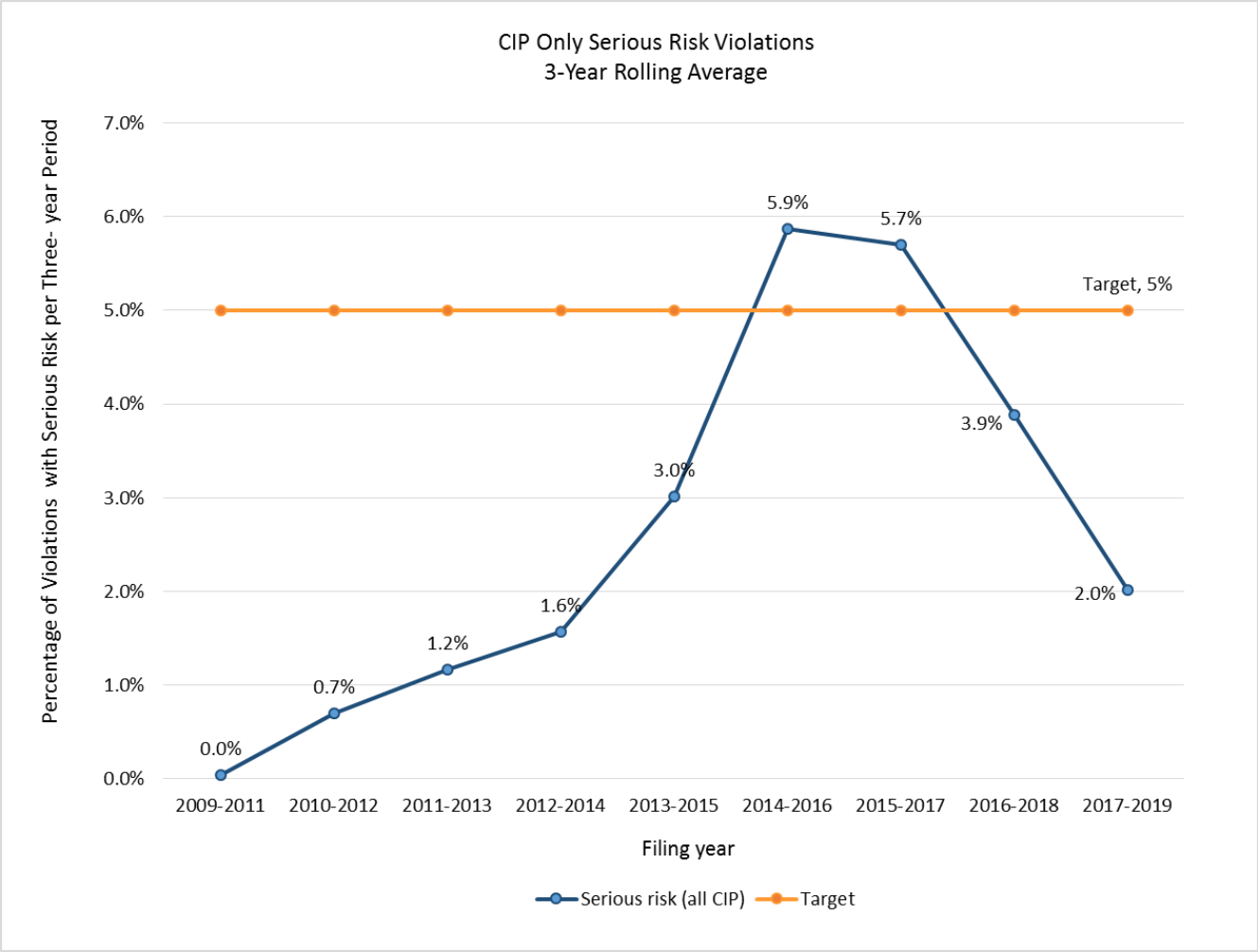


Figure A.7: Rolling Average of Serious Risk Violations (CIP)

Reduced Repeat Moderate and Serious Risk Violations

The ERO Enterprise monitors compliance history (defined as a prior violation of the same Reliability Standard and requirement) and repeat noncompliance with similar conduct (defined as a prior violation that stemmed from similar actions or conduct) to further explore the relationship of prior mitigation to repeat noncompliance and to identify any additional areas of focus and future actions.

Figure A.8 compares three categories of moderate and serious risk noncompliance: noncompliance with compliance history (blue columns), noncompliance with compliance history involving similar conduct (orange line), and all filed moderate and serious risk noncompliance (gray line). Noncompliance with similar conduct is a subset of the wider group of repeat noncompliance. The total moderate and serious noncompliance, shown by the gray line, includes both "new" noncompliance and repeat noncompliance.

The full NOPs filed in 2019 involved violations with similar prior conduct, which also carried larger penalty amounts.

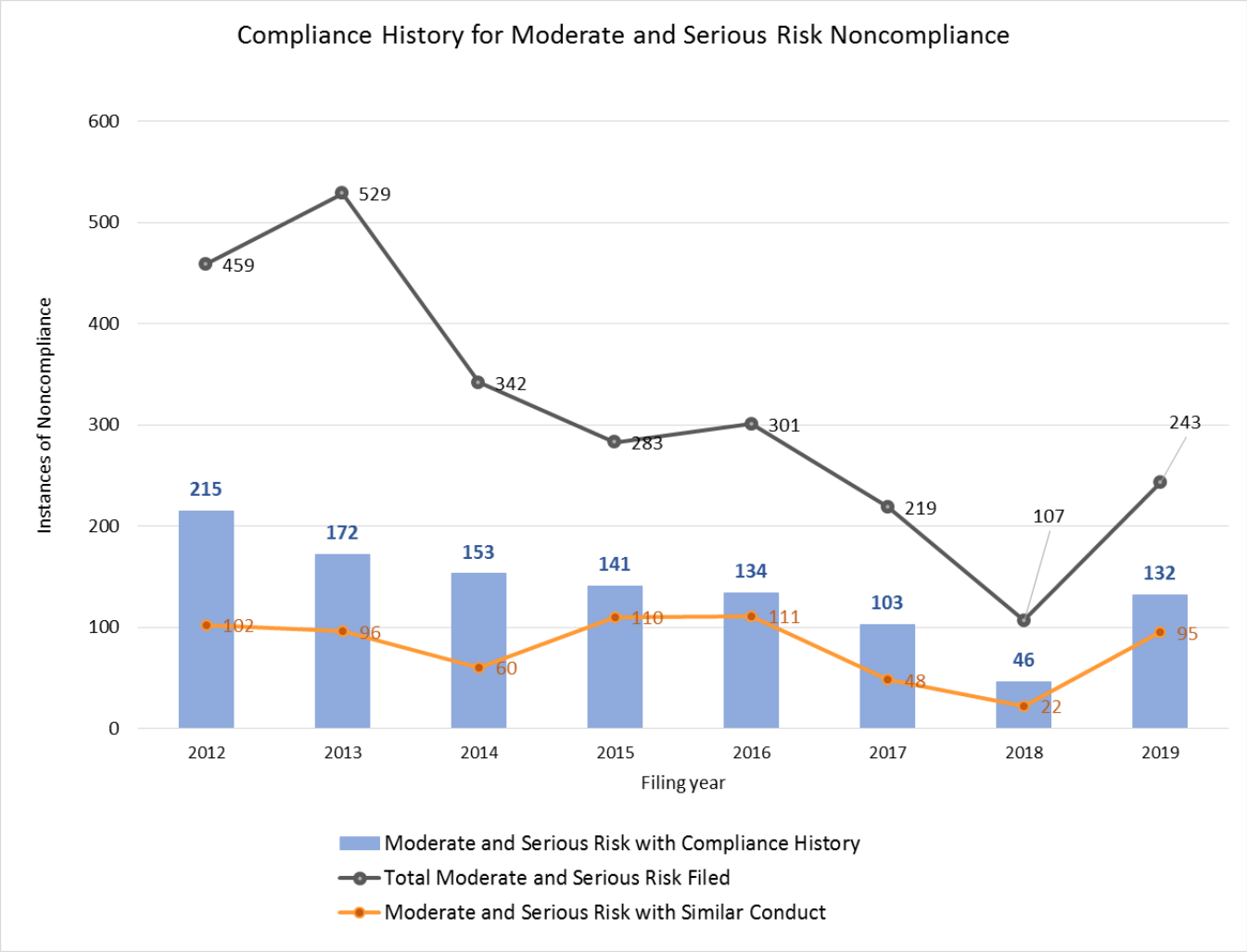


Figure A.8: Compliance History and Similar Conduct for Moderate and Serious Risk Violations

Self-Assessment and Self-Identification of Noncompliance

As part of an effort to reduce risk from noncompliance, the ERO Enterprise is looking beyond the broad categories of internal and external discovery and instead closely monitoring self-reported issues beginning in 2018 and continuing in 2019. Figure A.9 shows the percentage of noncompliance by discovery method. The percentage of self-reported noncompliance varies quarterly but often remains above the threshold. To date, registered entities self-reported 76 percent of noncompliance in 2019.

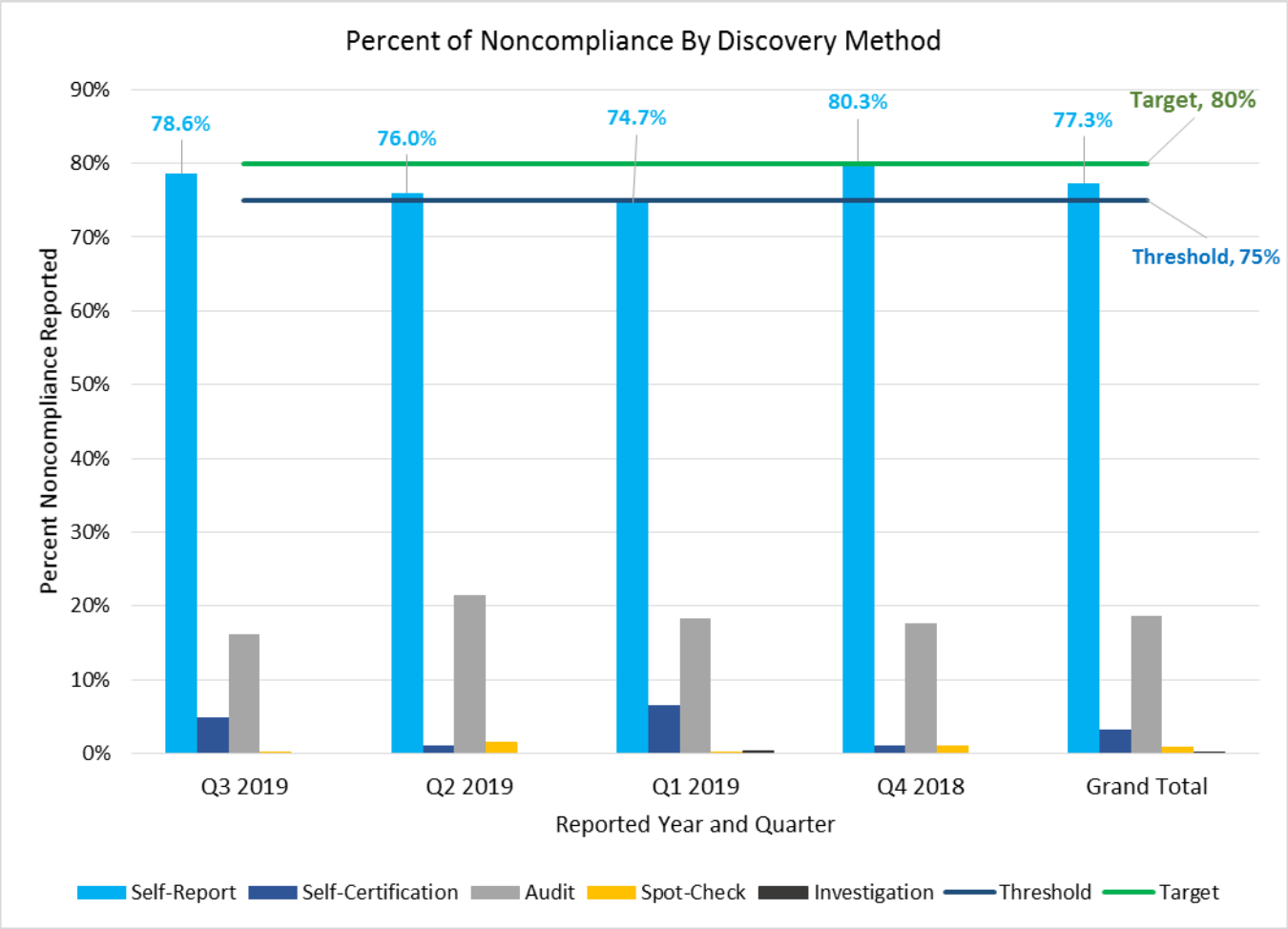


Figure A.9: Percent of Noncompliance by Discovery Method

Appendix B: Compliance Assurance

Coordinated Oversight Program for MRREs

Figure B.1 represents the distribution of the 50 MRRE groups by Lead RE, comprised of 211 MRREs. Figure B.2 represents the distribution of MRREs by registered function.

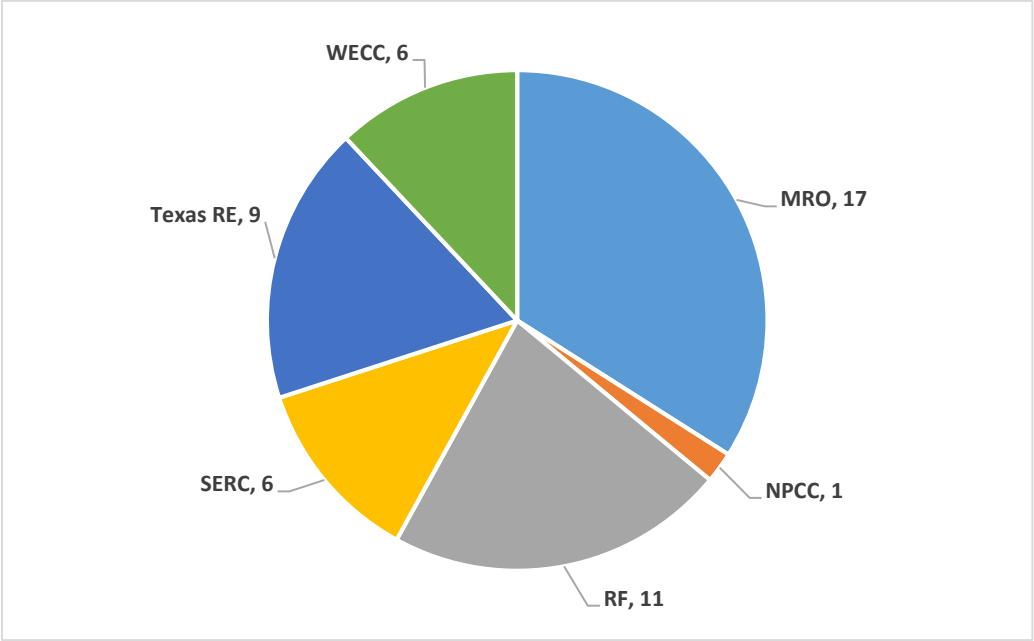


Figure B.1: Distribution of MRREs under Coordinated Oversight by Lead RE

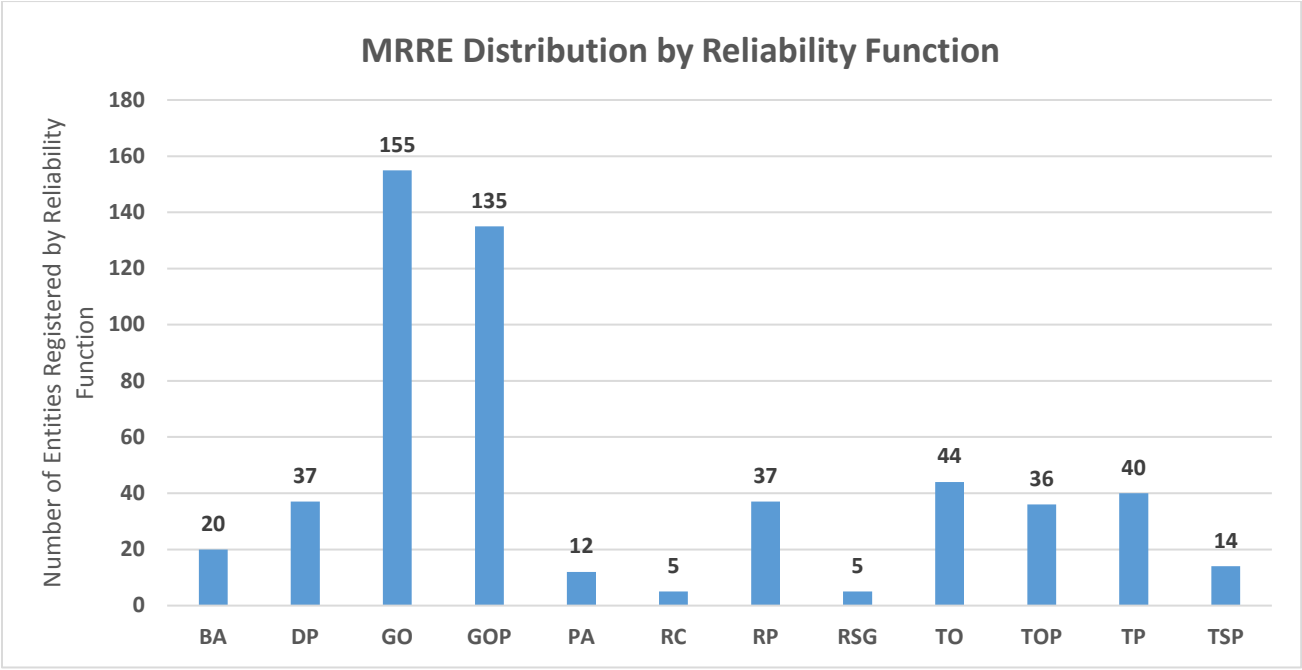


Figure B.2: Coordinated Oversight Distribution by Registered Function

ERO Enterprise Completion of Initial IRAs

Figure B.3 identifies the number of initial IRAs completed by each RE. As of the end of Q3 2019, the REs have completed 1,381 IRAs for 1,504 registered entities.[8] The ERO Enterprise completed IRAs for approximately 92 percent of the total number of registered entities.[9] All REs have completed IRAs for all entities registered as Reliability Coordinators and Balancing Authorities, with one remaining Transmission Operator scheduled for completion in 2019. NERC and the REs anticipate registration changes that will affect overall IRA completion. Therefore, IRA activity prioritization will consider registered functions and registration changes to ensure IRAs are completed.

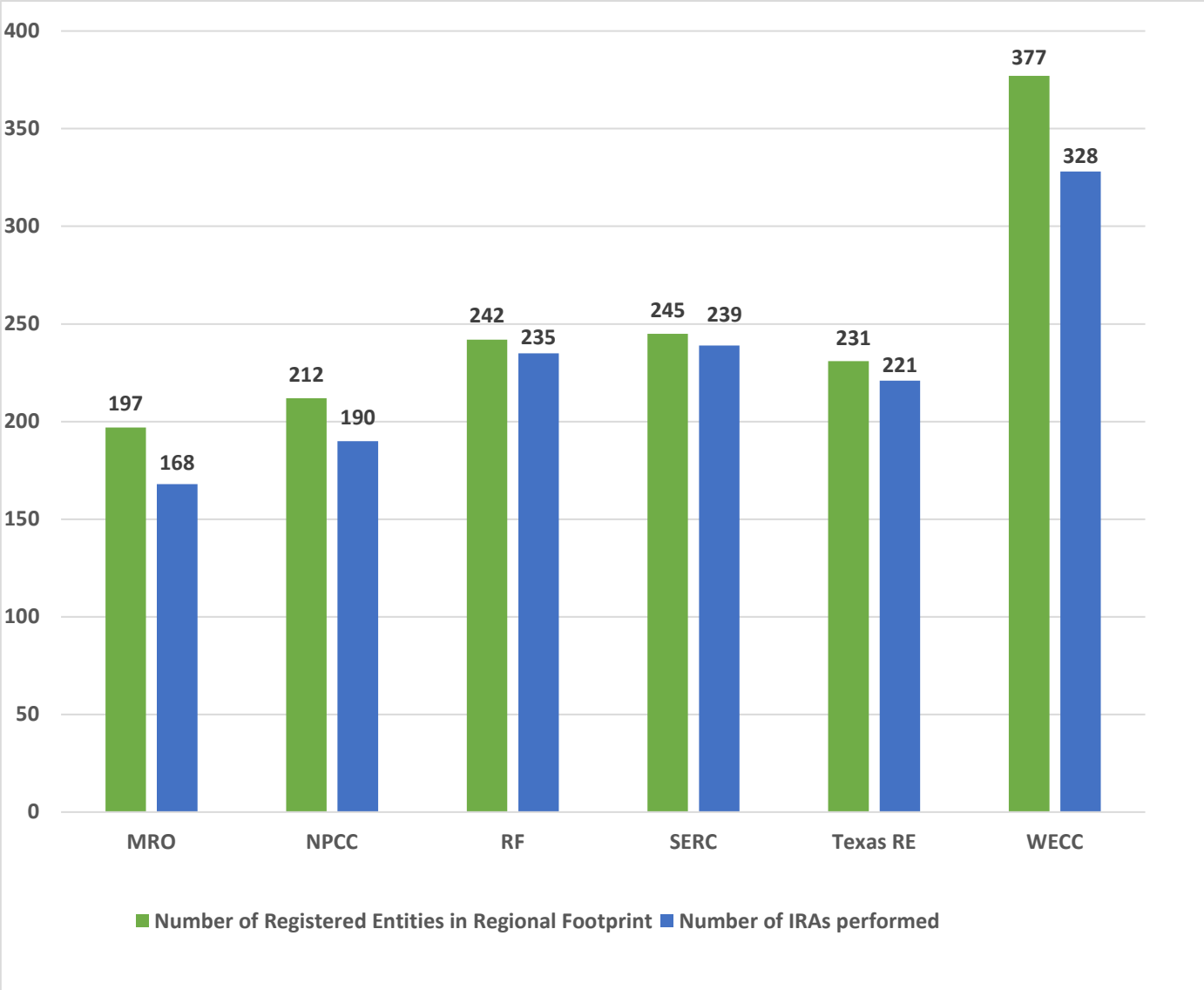


Figure B.3: RE Completion of IRAs

[8] NERC bases the number of registered entities on the registration cut-off date in Q3 2019, which includes all newly registered entities. NERC does not include deregistered entities. The chart does not reflect the number of IRAs that have been updated by the REs.

[9] Some of the registered entities are MRREs in the Coordinated Oversight Program. As such, until the Lead RE completes the IRA for that MRRE, the numbers do not update for the Affected REs. Therefore, some of the REs included in Figure B.3 do not receive credit for competing an IRA until their IRAs of the MRRE is completed by the Lead RE.

Appendix C: Registration

The following charts depict Q3 2019 registration change activity by function.

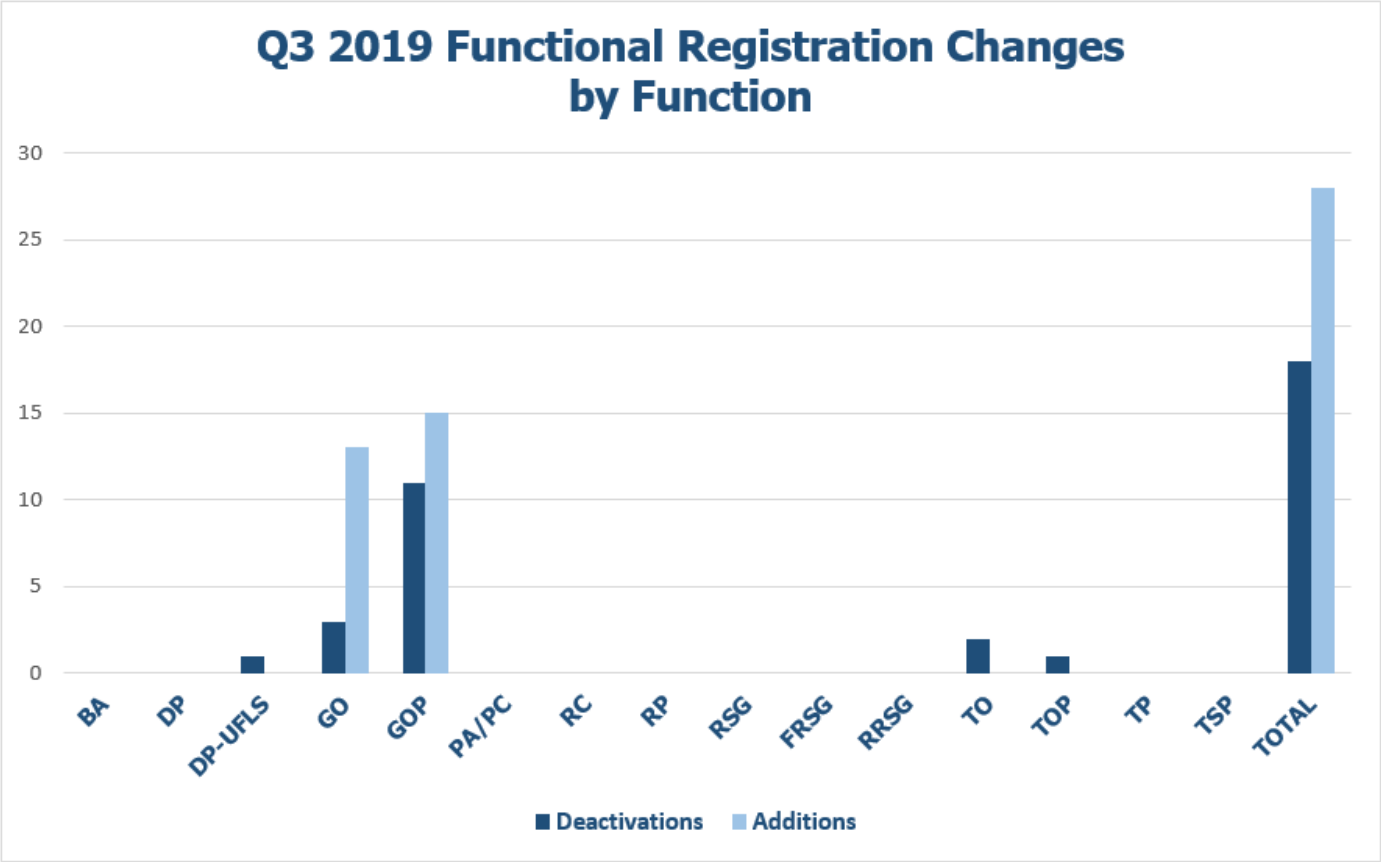


Figure C.1: Q3 2019 Registration Change Activity by Function

Table C.1: Functional Registration Change Activity by Function and Total Q3 2019 Changes						
	DP-UFLS	GO	GOP	TO	TOP	TOTAL
Deactivations	1	3	11	2	1	18
Activations	0	13	15	0	0	28

REs provide justification when approving registration change activity. NERC reviews these justifications before processing is completed. Table C.2 reflects the changes that were processed in Q3 2019.

Table C.2: Q3 2019 Registration Change Basis	
Determined to Not Meet Registration Criteria	1
Facility Shut Down	2
Sold to Another Registered Entity	4
Compliance Responsibility Assumed by Another Registered Entity	11

Appendix D: Certification and Bulk Electric System

ERO Enterprise Organization Certification Utilization

Certification activities are responsive to the number of new entities requiring certification and the types of changes implemented to already-certified and operational entities. Program utilization metrics help to plan resource needs, including staff, travel, and training.

Figure D.1 identifies the number of new entity certifications completed by each RE during Q3 2019 and the number of new entity certifications remaining. Figure D.2 identifies the number of reviews of changes to already-certified and operational entities completed by each RE during Q3 2019 and the number of certification reviews currently remaining. The in-process certification activity for FRCC transitioned to SERC on July 1, 2019.

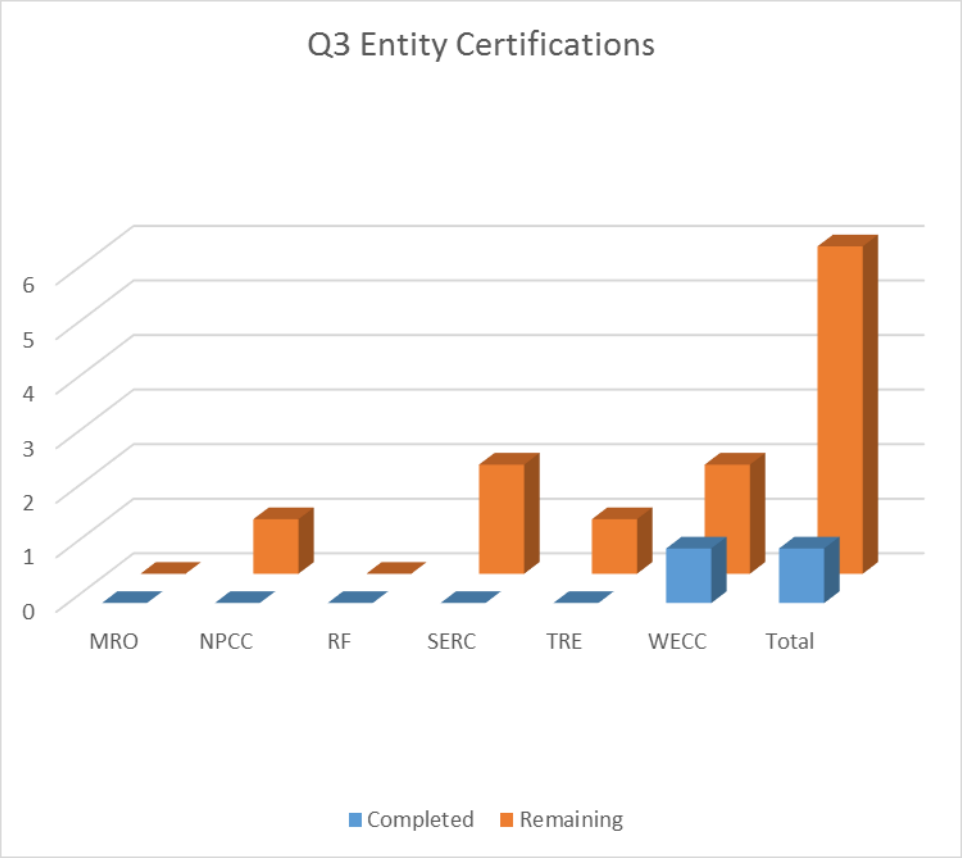


Figure D.1: Q3 2019 New Entity Certifications by RE

Table D.1: Q3 2019 Organization Certification		
Function	Completed	Remaining
Reliability Coordinator	1	1
Transmission Operator	0	3
Balancing Authority	0	2

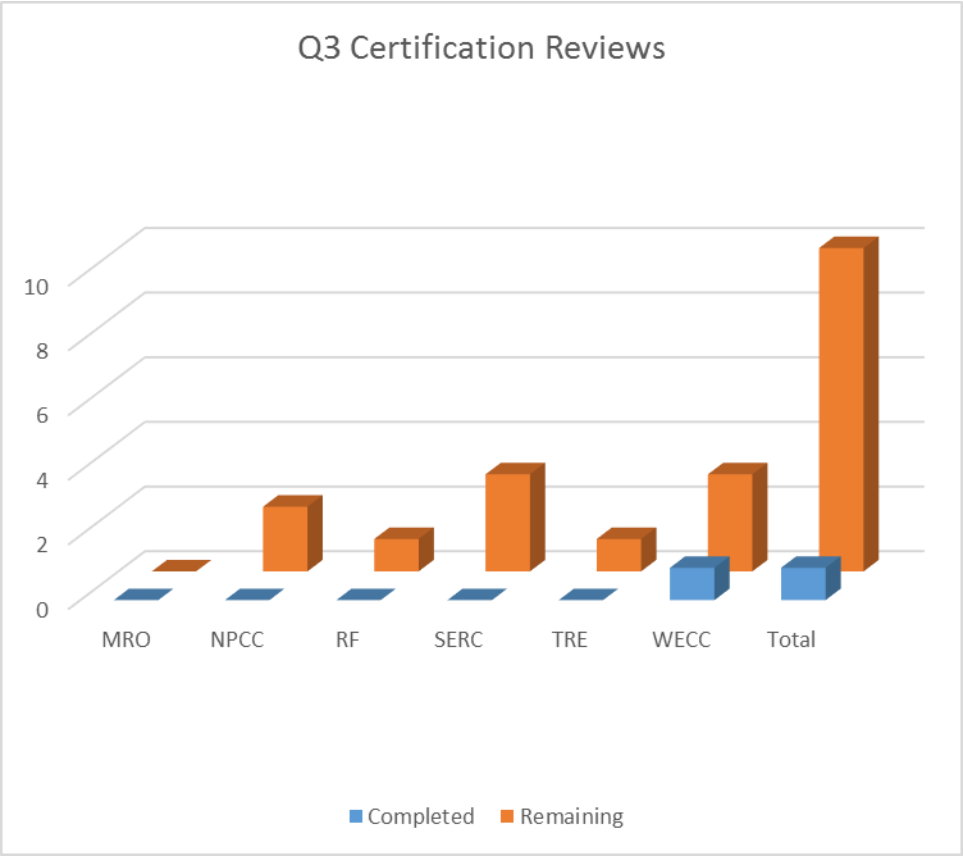


Figure D.2: Q3 2019 Certification Review Activity by RE

Table D.2: Q3 2019 Certification Review		
Change Basis	Completed	Remaining
Changes to a Registered Entity's Footprint	1	1
Relocation of the Control Center	0	4
Changes to Supervisory Control and Data Acquisition (SCADA)/Energy Management System (EMS) System	0	5