

Enforcement Update and Observations

By: Kristen Senk, Managing Counsel Enforcement

Overview of Enforcement Activity

Consistent with trends across the ERO, RF has experienced an increase in the number of violations identified since 2016.

As shown in Figure 1, the number of Operations and Planning violations has remained fairly consistent over the past several years. The driver for the increased volume is CIP, which was expected given the nature of CIP version 5, which went into effect in July, 2016.

However, despite the increased volume, detective controls seem to remain strong, as entities are self-identifying the majority of violations, and often times very quickly. Additionally, the majority of violations are lesser risk issues.

A Closer Look at CIP

Over half of the violations that RF has received in 2018 (through self-reports, audits, or otherwise) have been either **CIP-007** (specifically patch management) or **CIP-010** (change management).

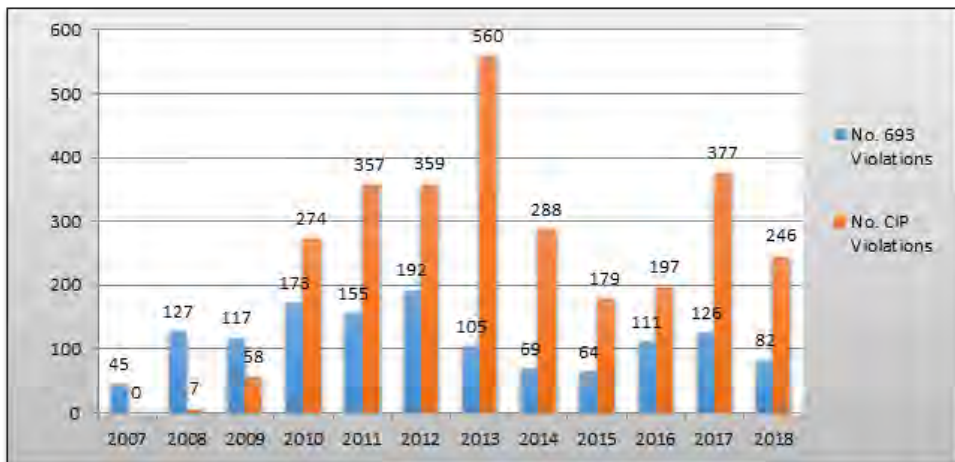


Figure 1

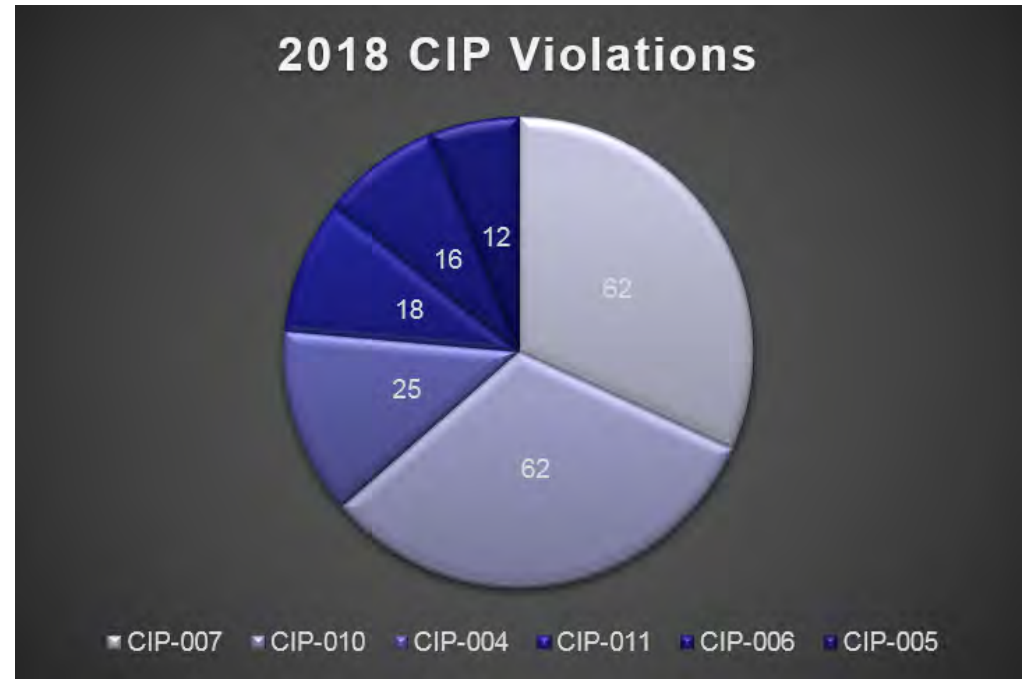


Figure 2

For this reason, and because of the criticality of the security measures covered by these Standards, CIP-007 and CIP-010 are focus areas for RF.

CIP-007 and CIP-010 govern high frequency conduct; that is, they cover multiple assets, people, and business units, and activity that occurs frequently. For this reason, we expect to see more noncompliances in these areas, especially for larger entities that manage thousands of assets and people, but sometimes for smaller entities as well.

In fact, sometimes, noncompliances in these focus areas can be an indication of a healthy compliance and security program, especially where entities are

Enforcement Update and Observations UBC

Continued from page 7

quickly detecting and correcting the issues. However, it's important to note that where entities have experienced significant program deficiencies, CIP-007 and CIP-010 tend to be areas where the entities are struggling.

To effectively manage CIP-007 and CIP-010 programs, because of the nature of these programs, entities need to be strong in asset and configuration management. Entities should also focus on breaking down silos across their organizations.

RF has processed many violations in these areas where the causes related to lack of communication or miscommunication between the multiple groups responsible for managing the assets.

A Closer Look at Operations and Planning

While the Operations and Planning noncompliances account for a relatively small portion of the total noncompliances we process, we would like to share some observations regarding the activity we're seeing with **Vegetation Management, Facility Ratings, and Protection System Maintenance and Testing**.

Regarding **Vegetation Management**, the ERO has experienced several sustained outages related to vegetation contacts in the past few years. In light of this activity and the criticality of vegetation management, RF will increase targeted and general outreach in this area and work with its entities, Regional partners, and NERC to share best practices and lessons learned.

Regarding **Facility Ratings** and **Protection System Maintenance and Testing**, although the overall number of noncompliances has not increased significantly over the past few years, the Regions have identified some significant cases in these areas. Still, the majority of the noncompliances in these areas tend to be minimal risk.

Regarding maintenance and testing, some entities are identifying equipment that has never been tested. Depending on the criticality of the equipment and other factors, these issues may pose a higher risk to the system.

These noncompliances are generally due to insufficient asset and configuration management practices relating to old equipment or incorporating new equipment or changes into the entities' maintenance and testing programs.

Similarly, with Facility Ratings, some entities are identifying equipment that was not part of the ratings calculations (such as jumpers, risers, or secondary equipment) or identifying errors in their methodologies for calculating ratings.

RF is working with the entities who have identified these noncompliances to understand the causes and ways to expedite identification of these issues in the future. Stay vigilant and stay tuned for more outreach activities in the coming months!

