Agenda Item 5
Board of Trustees Compliance Committee
Open Session
February 11, 2015

# Compliance Exception and Self-Logging Report Q4 2014

## Action

Information

## Introduction

Beginning in November 2013, NERC and the Regional Entities began exercising their inherent discretion whether to initiate a formal enforcement action by identifying minimal risk noncompliance that does not warrant a penalty and which would be recorded and mitigated without triggering an enforcement action. Noncompliance that is not pursued through an enforcement action by the ERO Enterprise is referred to as a "compliance exception."[1]

The compliance exception disposition track builds on the success of the Find, Fix, Track, and Report (FFT) program, which was the first step in implementing a risk-based strategy that recognizes that not all instances of noncompliance require the same type of enforcement process.

In 2013 and 2014, the use of compliance exceptions (as the alternative disposition for noncompliance posing a minimal risk to the reliability of the bulk power system) was limited to allow the testing of the new process. In 2015, this disposition track became available throughout the ERO Enterprise. Utilization of compliance exceptions as a disposition track has increased steadily, as shown in the following graphs.

On a quarterly basis, NERC will provide information regarding the utilization of the compliance exception disposition track, as well as relevant information that could be used by registered entities to understand the types of issues being treated as compliance exceptions and avoid similar noncompliance. Information on the utilization of the self-logging program will also be included.

[1] For more information about compliance exceptions, please visit http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Compliance%20Exception%20Overview.pdf

## Utilization of Compliance Exceptions

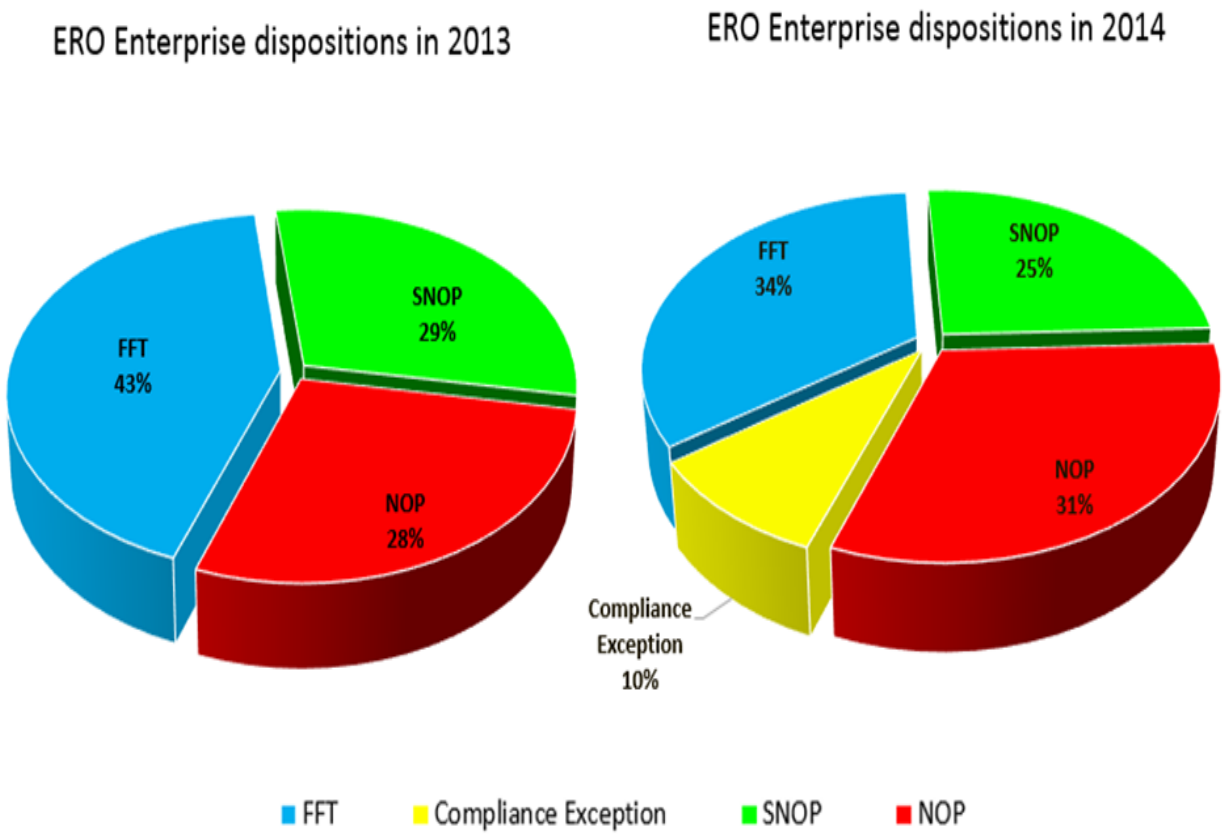


**Figure 1: ERO Enterprise Disposition Methods 2013 vs. 2014**

In 2013, 43% of noncompliance was disposed through the FFT process. In 2014, 34% of noncompliance was disposed through the FFT process, and 10% were provided compliance exception treatment (see Figure 1). The utilization of streamlined disposition tracks for lesser risk issues remains steady and reflects the continued use of these tracks as well as an initial shift of usage of compliance exceptions in lieu of FFTs. The small increase in the percentage of matters disposed of through an NOP in 2014 reflects the natural variation of the caseload as well as a minor increase in the number of serious violations processed in 2014 compared to 2013.[2]

Figure 2 shows the utilization of compliance exceptions at the Regional Entities. In cases where Regional Entities coordinated the processing of compliance exceptions such that one Regional Entity was responsible for processing them, these items will not appear in the percentages of the other Regional Entities involved. This is the case, for example, of certain compliance exceptions processed by RF on behalf of SPP RE and Texas RE.

[2] See breakdown of violations by risk in the Key Compliance Enforcement Metrics and Trends update, item 4 in this same package.

This data reflects the end of the pilot phase for compliance exceptions. Staff expects that the full-year 2015 data will show a more even distribution of the utilization of the compliance exception disposition track. It should also, consistent with the initial data in Table 1, show an increase in utilization of compliance exceptions and a corresponding reduction of minimal risk issues processed as FFTs, compared to 2014.

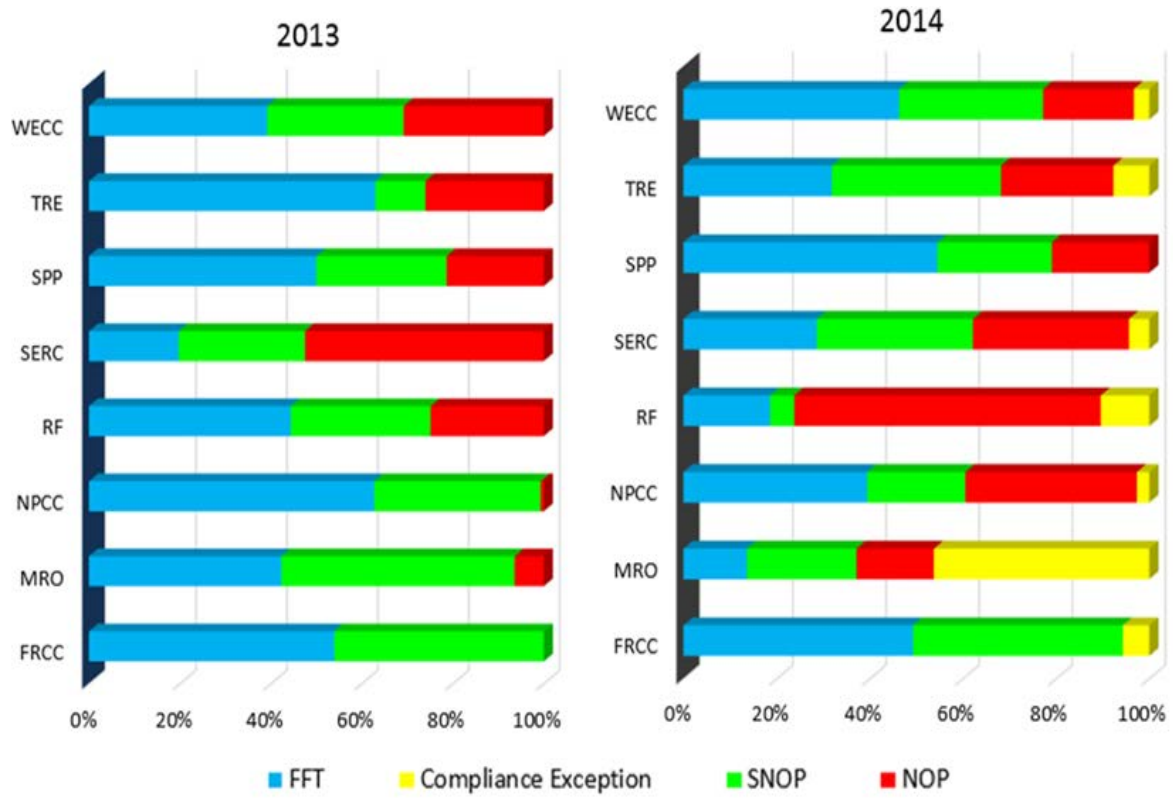


**Figure 2: Disposition Methods Used by the Regional Entities 2013 vs. 2014**

## Utilization of Self-Logging

As of January 1, 2015, 19 registered entities have been permitted to self-log minimal risk noncompliance (see Figure 3 below). The self-logging program (formerly known as the aggregation program) allows any registered entities that have demonstrated effective management practices to keep track of minimal risk noncompliance (and related mitigation) on a log that is periodically reviewed by the Regional Entity. Minimal risk noncompliance added to the log is presumed to be disposed of as a compliance exception.

The program is now available to any registered entity that would like to be evaluated by its Regional Entity in accordance with the program requirements.[3]

[3] For more information about self-logging of minimal risk issues, including program requirements, please visit http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/Self-logging%20of%20Minimal%20Risk%20Issues%20Program%20Overview.pdf

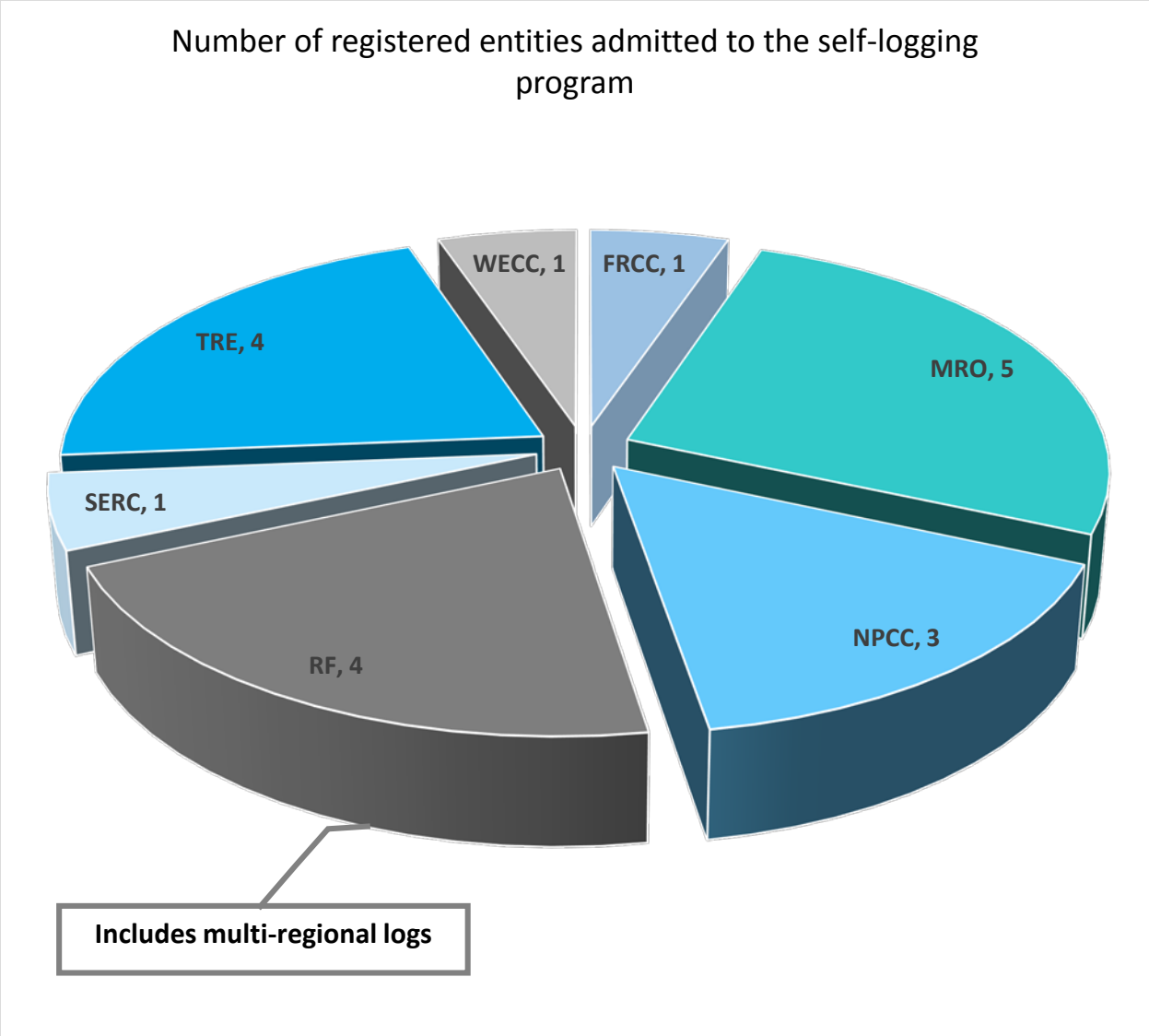


**Figure 3: Number of Registered Entities Participating in Self-Logging By Regional Entity**

## Compliance Exception Trends

The ERO Enterprise disposed of 116 instances of noncompliance as compliance exceptions in 2014. The Regional Entities used the discretion path for issues discovered in 2014 as well as those discovered in past years (see Figure 4).

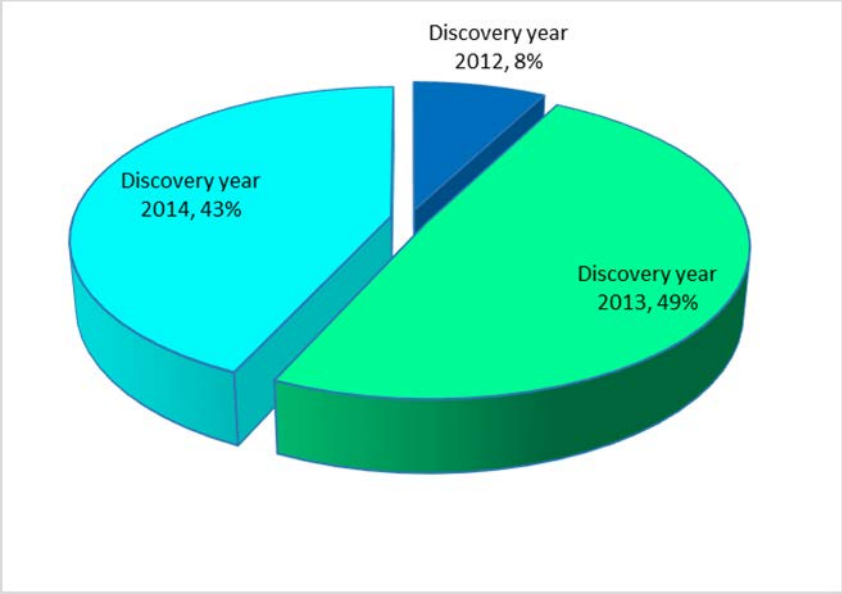


**Figure 4: Compliance Exceptions by Discovery Year**

Compliance exceptions may come from any of the Reliability Standards. Fifty-three percent of the compliance exceptions related to non-CIP Reliability Standards. Forty-seven percent of the compliance exceptions related to CIP Reliability Standards. Most of the compliance exceptions were internally discovered by the registered entity (see Figure 5 below).

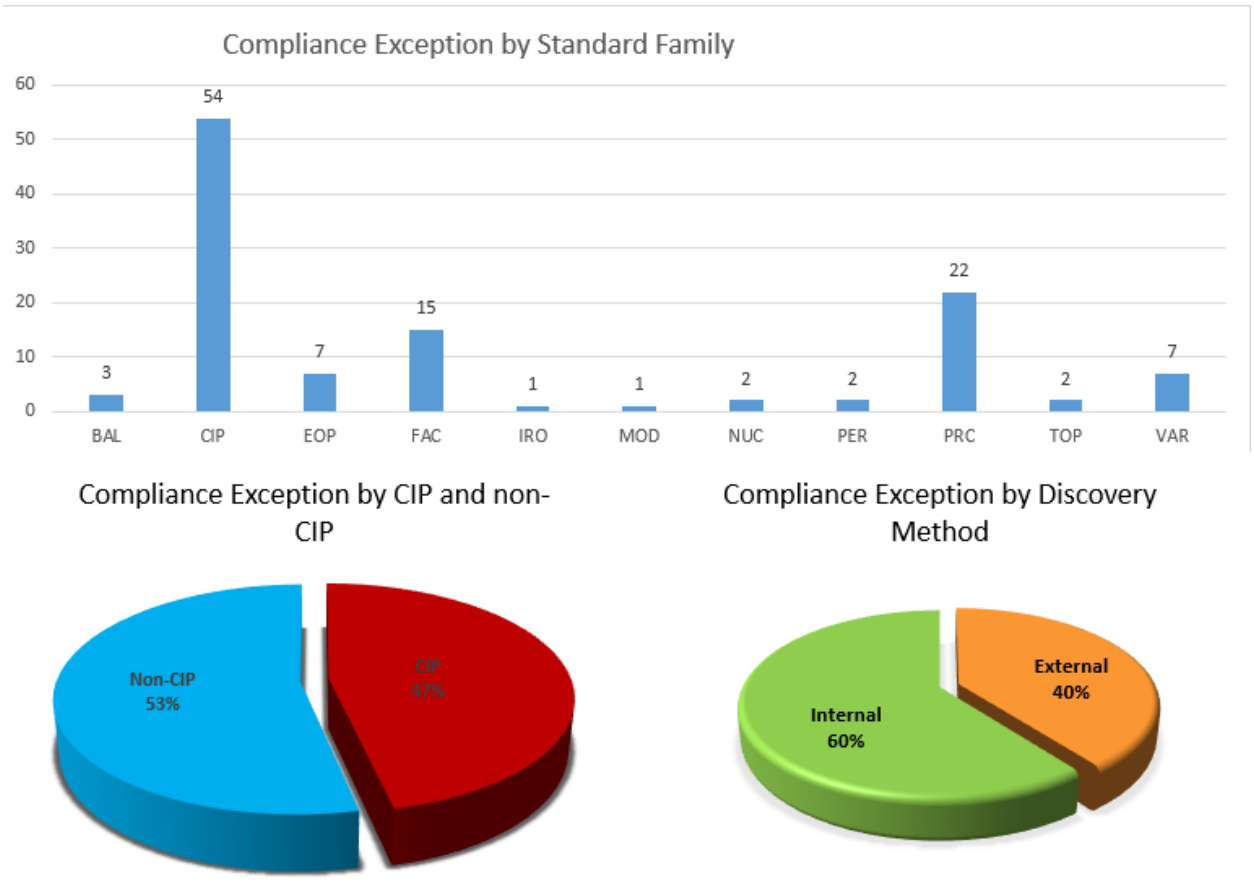


**Figure 5: Compliance Exception by Standard Family and Discovery Method**

Table 1 below shows a list of the Reliability Standards most frequently involved in noncompliance disposed of as compliance exceptions. The list is similar to the list of Reliability Standards most frequently involved in noncompliance disposed of as FFTs in the past.

A significant number of compliance exceptions relate to CIP-007, CIP-006, and CIP-005. For that reason, NERC is providing some observations related to those compliance exceptions.[4]

[4] CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets (CCAs), as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). CIP-006 is intended to ensure the implementation of a physical security program for the protection of CCAs. CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all CCAs reside, as well as all access points on the perimeter.

| Table 1: Count of Compliance Exceptions by Reliability Standard | |
|---|---|
| **Standards** | **Number of Compliance Exceptions** |
| CIP-007 | 16 |
| PRC-005 | 16 |
| CIP-006 | 12 |
| CIP-005 | 11 |
| CIP-004 | 9 |
| FAC-008 | 9 |
| VAR-002 | 6 |
| CIP-003 | 4 |
| EOP-008 | 4 |
| FAC-009 | 4 |

### Observations and Examples

Below are a number of examples of compliance exceptions processed by the ERO Enterprise. These are grouped into two primary themes: documentation issues and isolated issues.

### The Registered Entity had Documentation Issues

A CIP-007-3a R4 related compliance exception involved the registered entity's failure to update a Technical Feasibility Exception (TFE) in a timely manner.[5] The registered entity maintained TFEs for devices that do not support anti-virus or antimalware technologies; however, the registered entity self-discovered that it did not include a complete list of Cyber Assets as amendments to its TFEs. Specifically, the registered entity failed to include 11 Cyber Assets on its antivirus and malware device list. The registered entity was required to update its existing TFE document but failed to do so on time. The registered entity had compensating measures in place.

The compliance exception involved a documentation issue and posed a minimal risk to the BPS. Some of the compensating measures in place included the following: (a) access to the devices was restricted to authorized personnel, (b) malware prevention was installed at all access points to the Electronic Security Perimeter (ESP), and (c) the devices were within a Physical Security Perimeter (PSP).

The Mitigation Activities involved training staff on the TFE process, updating the TFEs, and updating the change control and configuration management form.

In a CIP-006-3c R2-related compliance exception, the registered entity did not update its physical access control (PAC) system account management procedure within 30 days as required by the

[5] **R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).

Reliability Standard.[6] The registered entity self-discovered that it did not update its PAC system procedure as required by the Reliability Standard. The noncompliance involved a delay in removing steps from the PAC procedure and could not have resulted in granting of unwanted physical access privileges. To mitigate this issue, the registered entity revised and approved a new procedure.

A CIP-007-3a R3 compliance exception involved the registered entity's failure to document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades for four patches.[7] The four patches were not evaluated within the 30-calendar-day window as required.

The registered entity self-discovered the issue within two months of the start date of the noncompliance through its internal controls. The registered entity concluded that a system administrator failed to evaluate four security patches within the 30-day time requirement because of failed oversight to verify the four security patches were evaluated within the 30-day time requirement. To date, all patches released have been evaluated. Additionally, all patches identified as relevant through evaluation have been applied, and the registered entity is now compliant with the evaluation of patches. In addition to self-discovering the noncompliance in a timely manner via controls, the registered entity had compensating measures in place.

The registered entity has several other physical and electronic access controls in place to provide supplemental measures to prevent potential exposure to any Critical Cyber Assets (CCAs), curtailing any possible or actual adversities to the system. The registered entity's CCAs are protected by a PAC system that creates the PSP per CIP-006; its CCAs have electronic access points that are created and managed by a separate system that creates the ESP per CIP-005; and The CCAs that reside inside the ESPs use additional authentication mechanisms per CIP-007.

In a CIP-005-3a R1.5-related compliance exception, the registered entity did not follow its change management process in the completion of a checklist when it replaced a Cyber Asset used in electronic access control and monitoring (EACM).[8] The new Cyber Asset was previously tested and configured on the ESP network. However, the registered entity reconnected the device to

---

[6] **R2.** Protection of Physical Access Control Systems — Cyber Assets that authorize and log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
**R2.1.** Be protected from unauthorized physical access.
**R2.2.** Be given the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

[7] **R3.** Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all Cyber Assets within the Electronic Security Perimeter(s).

[8] **R1.** Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

the ESP to replace another device and did not complete the add/remove checklist as required by its policy. The registered entity had compensating measures in place.

The risk was reduced as the new EACM Cyber Asset was given all the required protections of the Reliability Standards before connection to the production network. Furthermore, the device did not have control of any BPS asset. This was a documentation error in not completing the procedural checklist until after the EACM was connected to the production ESP network and elevated to a production status.

The registered entity mitigated the noncompliance by completing the checklist, updating the coversheet on the checklist to clarify expectations, and trained support staff.

### The Registered Entity Self-Reported an Isolated Instance of CIP Noncompliance

In another compliance exception, the registered entity self-discovered a noncompliance with CIP-006-3c R1.[9] The registered entity detected a series of invalid access attempts at a site when staff was alerted by alarms from the facility's PAC system. Security personnel who were requested to investigate the alarm gained unescorted access to a PSP without prior approval. While investigating the alarm, the security personnel discovered a door that was not secure. The security personnel entered the PSP, unescorted, to verify that no suspicious activity was taking place.

The registered entity personnel immediately discovered the unescorted access because it was actively monitoring closed-circuit television of the area. The registered entity personnel asked the security personnel at the site to leave the area. The security personnel secured the control room door and exited the PSP within five minutes. Although the registered entity demonstrated

[9] **R1.** Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
**R1.1.** All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
**R1.2.** Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.
**R1.3.** Processes, tools, and procedures to monitor physical access to the perimeter(s).
**R1.4.** Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
**R1.5.** Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.
**R1.6.** A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
**R1.6.1.** Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.
**R1.6.2.** Continuous escorted access of visitors within the Physical Security Perimeter.
**R1.7.** Update of the physical security plan within 30 calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.
**R1.8.** Annual review of the physical security plan.

quick identification of the noncompliance, it failed to implement its visitor control program for visitors to a PSP as required by the Reliability Standard; however, as detailed above, the visitors were security personnel who were there to investigate an alarm. The registered entity demonstrated appropriate usage of controls that served as compensating measures.

The registered entity immediately detected and corrected the noncompliance, which limited its duration to approximately five minutes. Although the security personnel failed to follow certain procedures, the deviation occurred under the circumstances because the security officers had determined the door lock was not secure and the investigation of the suspicious activity was time-sensitive.

To mitigate the noncompliance, the registered entity updated its emergency response procedure to declare a response to an alert from the PACS an emergency so that armed security personnel may respond accordingly.

For another CIP-006-3c R1 and R1.6.2-related compliance exception, the registered entity self-reported that it failed to provide continuous escorted access of a visitor within the PSP as required by its visitor control program.

At a monthly meeting, a presenter who was an employee of the registered entity did not have unescorted access privileges in the area where a meeting was being held, which was also within a PSP. Upon completing the presentation, the employee left the PSP unescorted and proceeded to leave the building. The visitor was unescorted for approximately three minutes. The registered entity had compensating measures in place.

The employee did not have access to areas that contain ESPs. In addition, additional badge access is required to enter any areas where an ESP exists. In addition, the employee in question had a background check performed approximately three years before the issue.

In a similar compliance exception, the registered entity self-reported an issue with CIP-006-3c R1 because it had failed to provide continuous escorted access to visitors within a PSP. Specifically, the registered entity did not escort a visitor within a PSP for 13 minutes.

The mitigating factors concerning the noncompliance included the short duration of the violation and the unescorted visitor who was in the training room and not a more sensitive location.
To mitigate the issue, the registered entity investigated the event and trained staff. Specifically, it investigated to ensure that no harm occurred by reviewing PSP access records, login records of the equipment in the training room, and interviewed the individuals involved to understand the facts and circumstances of the noncompliance. In addition, the registered entity retrained staff on its security procedures.

## Additional Resources

- Analyzing Enforcement Data
- Violation Statistics
- Compliance Exception Overview
- Self-logging Overview