UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC	**)**	**Docket Nos. RR10-1-000**
RELIABILITY CORPORATION	**)**	**RR13-3-000**

ANNUAL REPORT OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION ON WIDE-AREA ANALYSIS OF TECHNICAL FEASIBILITY EXCEPTIONS

The North American Electric Reliability Corporation ("NERC") hereby provides the 2017 Annual Report on Wide-Area Analysis of Technical Feasibility Exceptions (the "2017 Annual Report") in compliance with Paragraphs 220 and 221 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Order No. 706[1] and Appendix 4D of the NERC Rules of Procedure ("ROP"). The 2017 Annual Report covers the period from July 1, 2016 through June 30, 2017.

I. INTRODUCTION

In Order No. 706, FERC approved eight Critical Infrastructure Protection ("CIP") Reliability Standards and, among other things, directed NERC to develop a set of conditions or criteria that a Responsible Entity must follow to obtain a Technical Feasibility Exception ("TFE") from specific requirements in the CIP Reliability Standards.[2] The Commission stated that the TFE process must include: mitigation steps, a remediation plan, a timeline for eliminating the use of the TFE unless appropriate justification is provided, regular review of the continued need for the

[1] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No.706, 122 FERC ¶ 61,040 (2008) ("Order No. 706").

[2] *Id.* at P 178.

TFE, internal approval by senior managers, and regional approval through the Electric Reliability Organization ("ERO").[3]

Order No. 706 also required that NERC submit an annual report to the Commission that provides a wide-area analysis of the use of TFEs and their effect on Bulk-Power System reliability. The Commission stated:

> The annual report must address, at a minimum, the frequency of the use of such provisions, the circumstances or justifications that prompt their use, the interim mitigation measures used to address vulnerabilities, and efforts to eliminate future reliance on the exception. . . [T]he report should contain aggregated data with sufficient detail for the Commission to understand the frequency with which specific provisions are being invoked as well as high level data regarding mitigation and remediation plans over time and by region . . . . [4]

In October 2009, NERC filed amendments to its ROP to implement the Commission's directive in Order No. 706, proposing Section 412 (Requests for Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards) and Appendix 4D (Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards). On January 21, 2010, the Commission approved NERC's amended ROP.[5]

On April 8, 2013, NERC filed revisions to Appendix 4D of the ROP to streamline the TFE approval process, reflecting NERC, Regional Entity and industry experience processing TFE

---

[3] *Id.* at P 222.

[4] *Id*. at P 220.

[5] *North American Electric Reliability Corp.*, 130 FERC ¶ 61,050 (2010), *order on compliance*, 133 FERC ¶ 61,008 (2010) ("October 1 Order"), *order on reh'g*, 133 FERC ¶ 61,209 (2010), *order on compliance*, 135 FERC ¶ 61,026 (2011) ("April 12 Order"). The Commission requested further information and clarification regarding certain aspects of the TFE process. On April 21, 2010, NERC submitted its compliance filing in response to the January 21 Order. On October 1, 2010, the Commission issued an order accepting NERC's April 2010 filing as partially compliant and directing further changes to the TFE Procedure. *See* October 1 Order. On December 23, 2010, NERC submitted a compliance filing in response to the Commission's October 1 Order, which the Commission subsequently accepted.

requests since the inception of the program. On September 3, 2013, FERC approved the proposed revisions and directed limited revisions to Appendix 4D, including modifications to: (1) specify a time frame for reporting Material Changes to TFEs upon identification and discovery; and (2) require the annual TFE report to include information on Material Change Reports and TFE expiration dates.[6] NERC submitted a compliance filing consistent with the directives from the September 2013 Order, which the Commission approved on January 30, 2014.[7] Sections 11.2.4 and 13 of Appendix 4D set forth the requirements for the annual TFE report, as modified in accordance with the September 2013 Order. The 2017 Annual Report includes the information required by the September 2013 Order.

II. NOTICES AND COMMUNICATIONS

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

Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G St., N.W., Suite 600
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net

Tom Hofstetter, CISA, CISSP
Senior CIP Compliance Auditor
North American Electric Reliability Corporation
3353 Peachtree Road NE, Suite 600 – North Tower
Atlanta GA 30326
404-446-2574
tom.hofstetter@nerc.net

III. 2017 ANNUAL REPORT

In accordance with Appendix 4D of the ROP, NERC prepared the 2017 Annual Report in consultation with the Regional Entities. The Regional Entities provided regular reports to NERC regarding the types of Covered Assets for which the Regional Entities have approved TFEs.[8] In

[6] *North American Electric Reliability Corp.*, 144 FERC ¶ 61,180 (2013) ("September 2013 Order").

[7] *North American Electric Reliability Corp.*, Docket No. RR13-3-001 (Jan. 30, 2014) (unpublished delegated letter order).

[8] Appendix 2 of the ROP defines the term "Covered Asset" as "any BES Cyber Asset, BES Cyber System, Protected Cyber Asset, Electronic Access Control or Monitoring System, or Physical Access Control System that is subject to" a TFE.

addition, each Regional Entity provided information on the 10 elements identified in Section 13 of Appendix 4D to be included in the 2017 Annual Report. NERC compiled and analyzed the TFE data provided by the Regional Entities in preparation for the 2017 Annual Report. The following is a discussion of that data.

a. Transition to New and Modified CIP Cybersecurity Reliability Standards

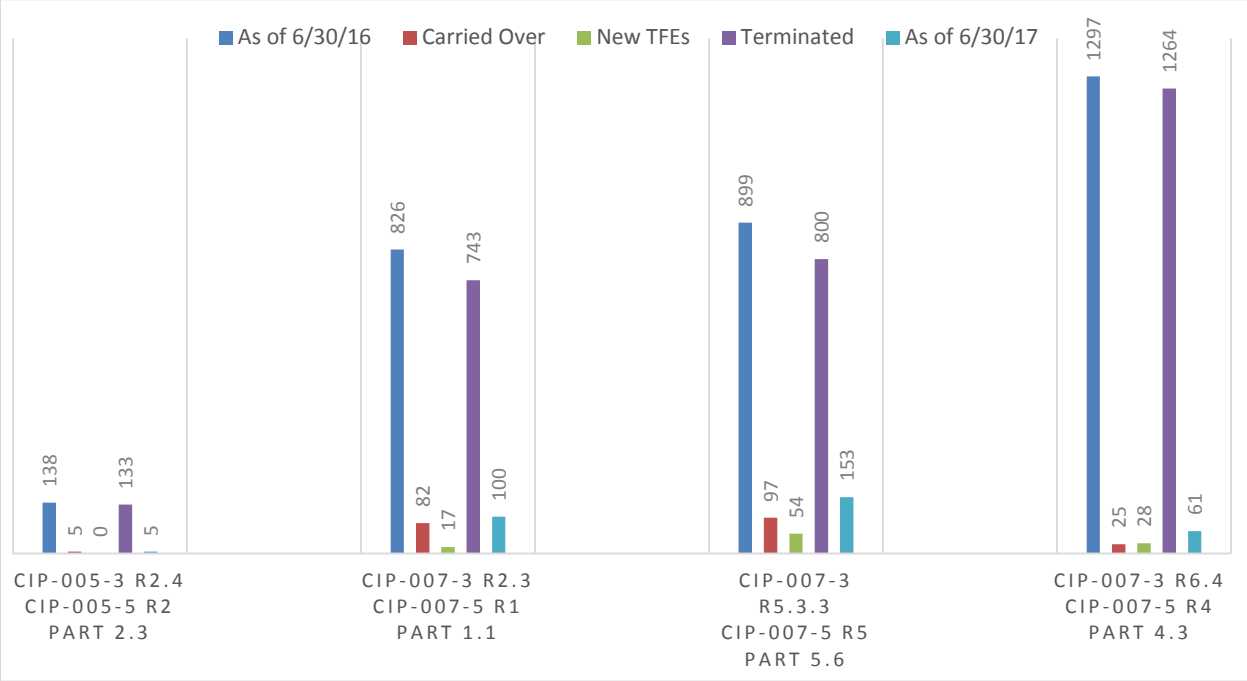
The 2017 Annual Report is the first report that includes TFE data for the suite of CIP cybersecurity Reliability Standards, CIP-002-5.1 through CIP-010-2, approved in Order No. 791, as modified in Order No. 822 which became effective on July 1, 2016.[9] As with the prior versions of the CIP cybersecurity Reliability Standards, the new and modified versions include requirements that provided for TFEs. There is not, however, a direct correlation from the prior versions in every instance (i.e., the requirements from the prior versions that were subject to TFEs may not have an equivalent requirements in the currently-effective version that is subject to a TFE, and vice versa). Where that correlation does exist, the TFE data obtained for the 2017 Annual Report indicates that there has been a significant decrease in the number of TFEs. In large part, this decrease reflects the different approach of the currently-effective CIP Reliability Standards. Under the prior version of the CIP Reliability Standards, the requirements were focused at the asset level, resulting in almost every entity with Critical Cyber Assets ("CCA") submitting a TFE request because one or more of its CCAs were technically incapable of compliance. In contrast, the currently-effective CIP Reliability Standards apply at the system level, permitting the grouping of BES Cyber Assets within BES Cyber Systems. By allowing for a system approach to

[9] *See Version 5 Critical Infrastructure Protection Reliability Standards*, Order No. 791, 145 FERC ¶ 61,160 (2013), order on clarification and reh'g, Order No. 791-A, 146 FERC ¶ 61,188 (2014); *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037 (2016); *see also, Order Granting Extension of Time*, FERC ¶ 61,137 (2016).

compliance, a BES Cyber Asset that previously would have required a TFE under the prior versions because part of a BES Cyber System with overarching security controls that meet requirements of the CIP Reliability Standards, avoiding the need for a TFE.

Figure 1, below, depicts the results of this transition for the TFE requirements that were directly comparable between the currently-effective Reliability Standards and the prior version of those Reliability Standards. Similarly, the overall quantity of TFEs in the 2017 Annual Report is significantly less than prior years. Details of those comparisons are addressed in the following section.

Figure 1 – TFE Requirements Consistent from V3 – V5



b. Elements Required by Appendix 4D, Section 13.1

The following is a summary of the TFE data reported by each Regional Entity for the 10 elements identified in Section 13.1 of Appendix 4D:[10]

1. *The frequency of use of the TFE Request process, disaggregated by Regional Entity and in the aggregate for the United States and for the jurisdictions of other Applicable Governmental Authorities, including (A) the numbers of TFE Requests that have been submitted and approved/disapproved during the preceding year and cumulatively since the effective date of this Appendix, (B) the numbers of unique Covered Assets for which TFEs have been approved, (C) the numbers of approved TFEs that are still in effect as of on or about the date of the Annual Report; (D) the numbers of approved TFEs that reached their TFE Expiration Dates or were terminated during the preceding year; and (E) the numbers of approved TFEs that are scheduled to reach their TFE Expiration Dates during the ensuing year.*

    i. Frequency of Use of the TFE Request Process

The CIP Reliability Standards apply to "Responsible Entities" that are designated in Applicability Section 4.1 of each CIP cybersecurity Reliability Standard (e.g., Balancing Authority, certain Distribution Providers, etc.). From an industry-wide perspective, the number of U.S. entities with registrations to which the CIP Reliability Standards apply has increased under the currently-effective CIP Reliability Standards by nearly nine percent. Figure 2 reflects the number of entities, subject to the CIP cybersecurity Reliability Standards. In addition, Figure 2 shows the number of Responsible Entities with designated high or medium impact BES Cyber Systems and the status of TFEs.

[10] Unless stated otherwise, a table or reference to "2017" refers to the reporting period for this report: July 1, 2016 – June 30, 2017.

Figure 2 - Frequency of Use for V3 and V5 (6/30/2016 to 6/30/2017)

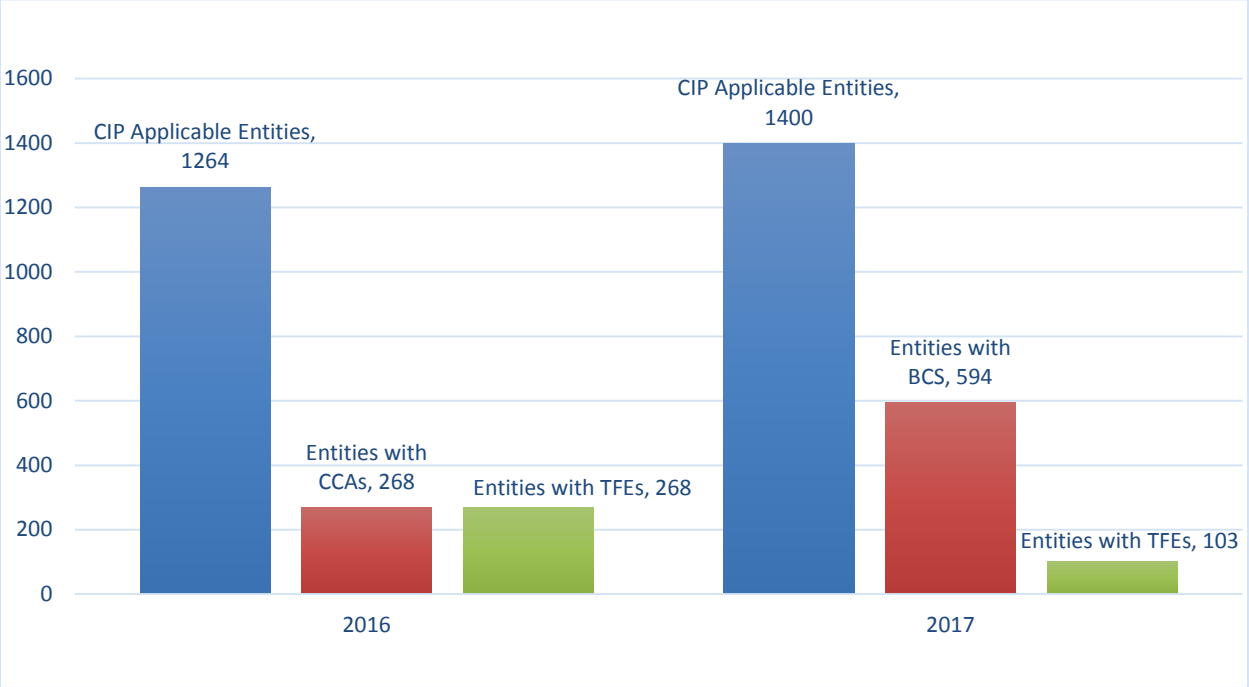
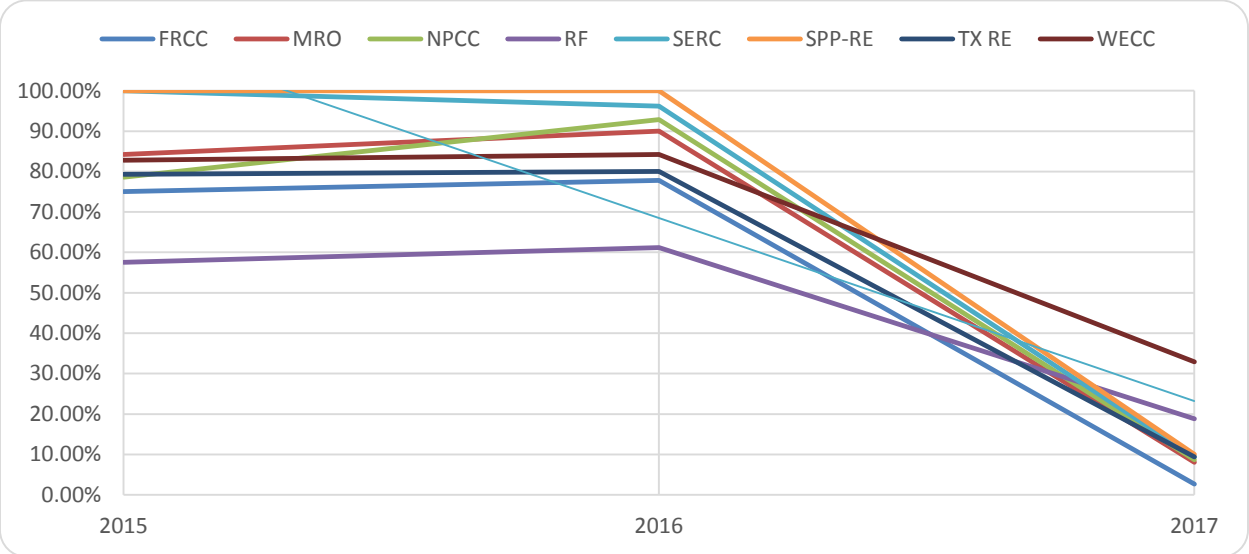


Figure 3, depicts the percentage of Responsible Entities with TFEs from 2015 through 2017. Each Regional Entity shows a large decline in the percentage of Responsible Entities with TFEs from 2016 to 2017.

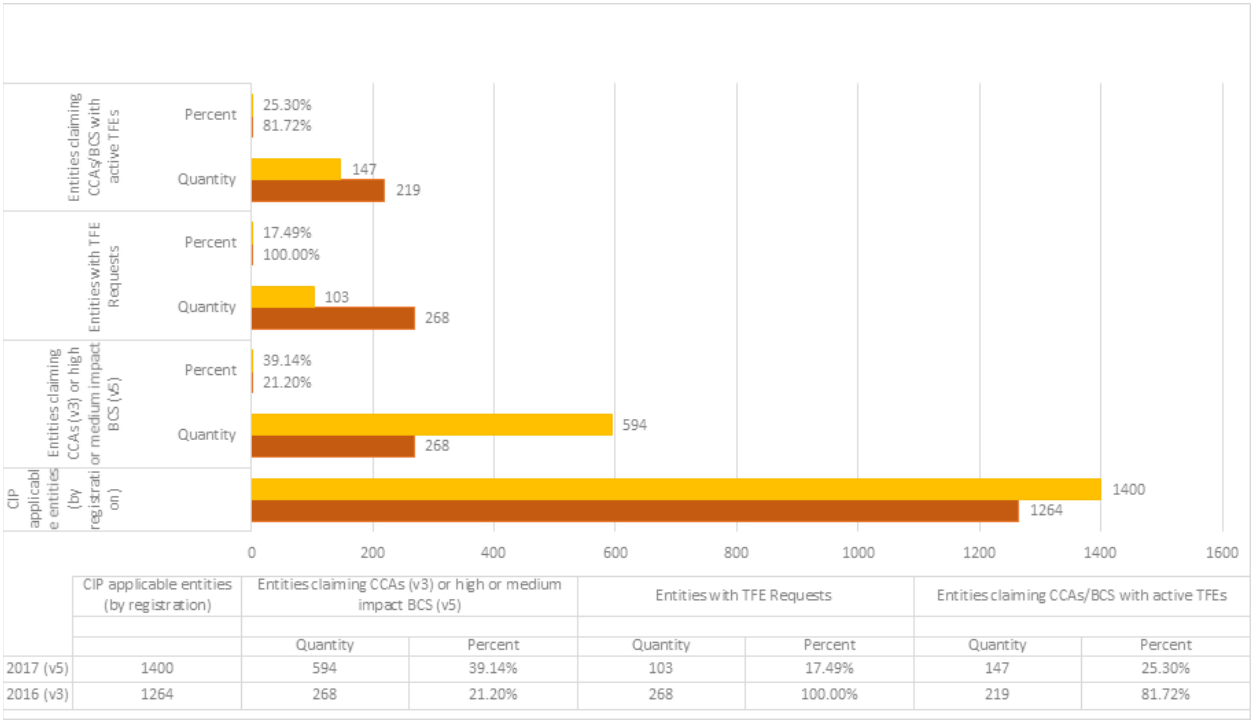
Figure 3 – Percentage of Entities with TFEs



In some cases, legacy TFEs (i.e., approved TFEs from prior version of the Reliability Standard that were automatically updated on July 1, 2016 to reflect the comparable requirement in the currently-effective Reliability Standard) are included in the number of entities with "active" TFEs. Thus, the number of Responsible Entities with active TFEs was not limited to those that submitted new TFE requests during the report period itself. There were also cases where legacy TFEs expired or terminated during the report period, as a result, there are a lower overall number of Responsible Entities with active requests at the end of the report period than the number of entities that submitted requests.

The transition to the currently-effective CIP Reliability Standards shows a marked contrast to the 2016 Annual Report; rather than a one to one ratio of Responsible Entities with TFEs, the 2017 report indicates that 25% of the Responsible Entities that reported owning high or medium impact BES Cyber Systems had TFEs. That difference is due to the fact that the currently-effective requirements are drafted at the system level and provide greater flexibility to Responsible Entities for designing protection mechanisms for a BES Cyber System, as opposed to the prior version's emphasis on individual CCAs. That system focus enables Responsible Entities to design comprehensive security solutions that are also compliant with the CIP Reliability Standards, through such measures as applying a "defense-in-depth" approach or through utilizing an application or appliance that is able to perform the specified control on behalf of an asset. Figure 4 provides a comparison between the 2016 and 2017 TFE reporting periods. The analysis shows that the percentage of Responsible Entities with TFEs has dropped from 81% from the 2016 report to 25% in the 2017 report, even though the percentage of entities to which the currently effective CIP Reliability Standards apply has increased by over 10%.

Figure 4 – Frequency of Use V3 and V5



	CIP applicable entities (by registration)	Entities claiming CCAs (v3) or high or medium impact BCS (v5)		Entities with TFE Requests		Entities claiming CCAs/BCS with active TFEs	
		Quantity	Percent	Quantity	Percent	Quantity	Percent
2017 (v5)	1400	594	39.14%	103	17.49%	147	25.30%
2016 (v3)	1264	268	21.20%	268	100.00%	219	81.72%

ii. TFE Requests that have been Submitted and Approved/Disapproved

As previously indicated, the 2017 Annual Report is unlike previous years' reports due to the impact of the revised CIP Reliability Standards. The transition to the currently-effective CIP Reliability Standards did not result in a complete replacement of all TFEs, but it did have a significant effect on the quantity of TFEs. A majority of the active TFEs are reported from three Regional Entities (WECC, RF, and NPCC). Figure 5 depicts TFE activity by Regional Entity.

Figure 6 reflects activity for TFEs that were initiated during the report period (i.e., not among the "legacy" TFEs that were updated administratively to cite a new requirement number). The data in Figure 7 reflects the same TFE activity during the report period that is depicted in Figure 6, breaking it down by requirement. The majority of the TFE activity during the report period pertained to Reliability Standard CIP-007-6 Requirement R5, Part 5.6, and Part 5.7. TFEs pertaining to Part 5.6, are more common because of assets such as RTUs, relays, network devices, PACS systems (card readers, security panels), Storage Area Network (SAN) devices,

time/frequency devices, or hardware chassis components with hard coded passwords that cannot be changed, or password changes would create issues with other systems. In the case of TFEs requested for Part 5.7, Cyber Assets are not able to limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful authentication attempts. Examples listed in TFEs include PACs devices (card readers, security panels), network devices (such as security defense appliances), time/frequency devices, and Storage Area Network ("SAN") devices.

Figure 5 – Active TFEs

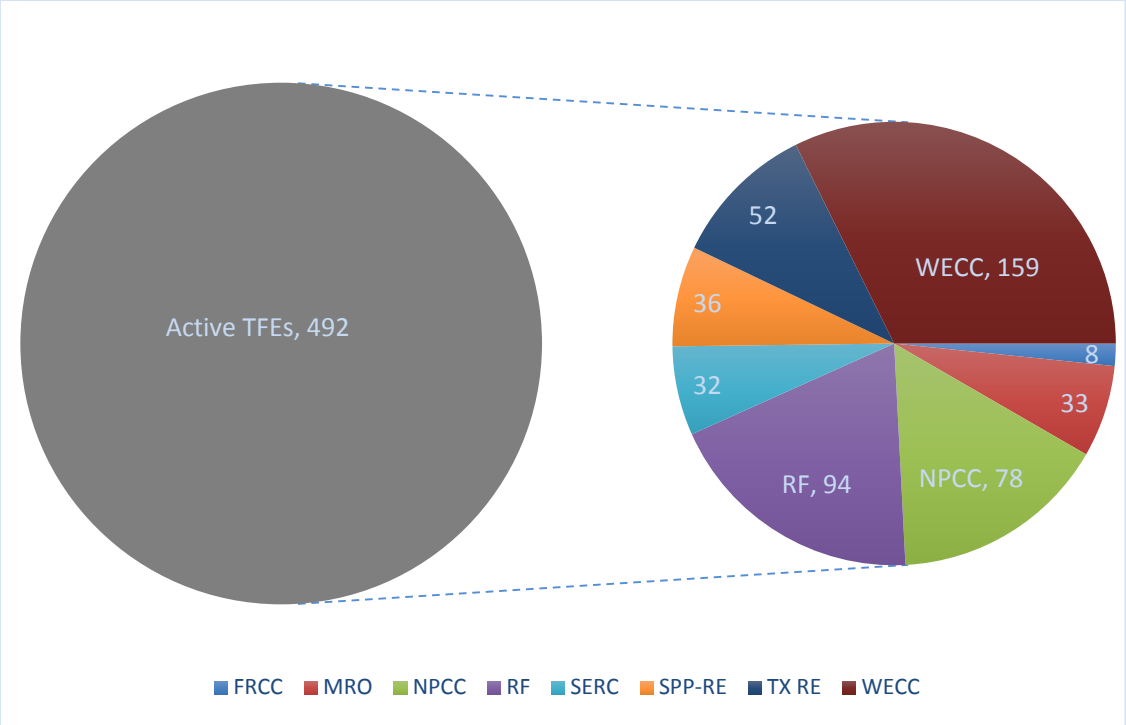


Figure 6 - TFE Requests / Changes 7/1/2016 - 6/30/2017

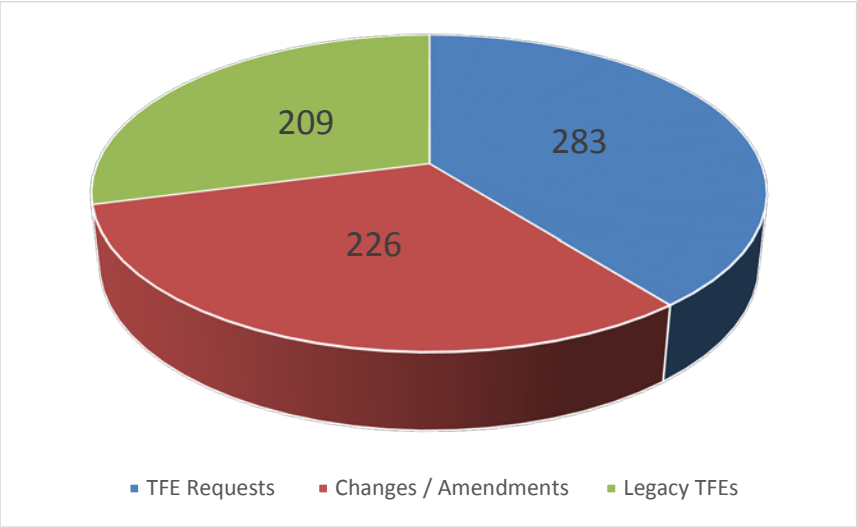
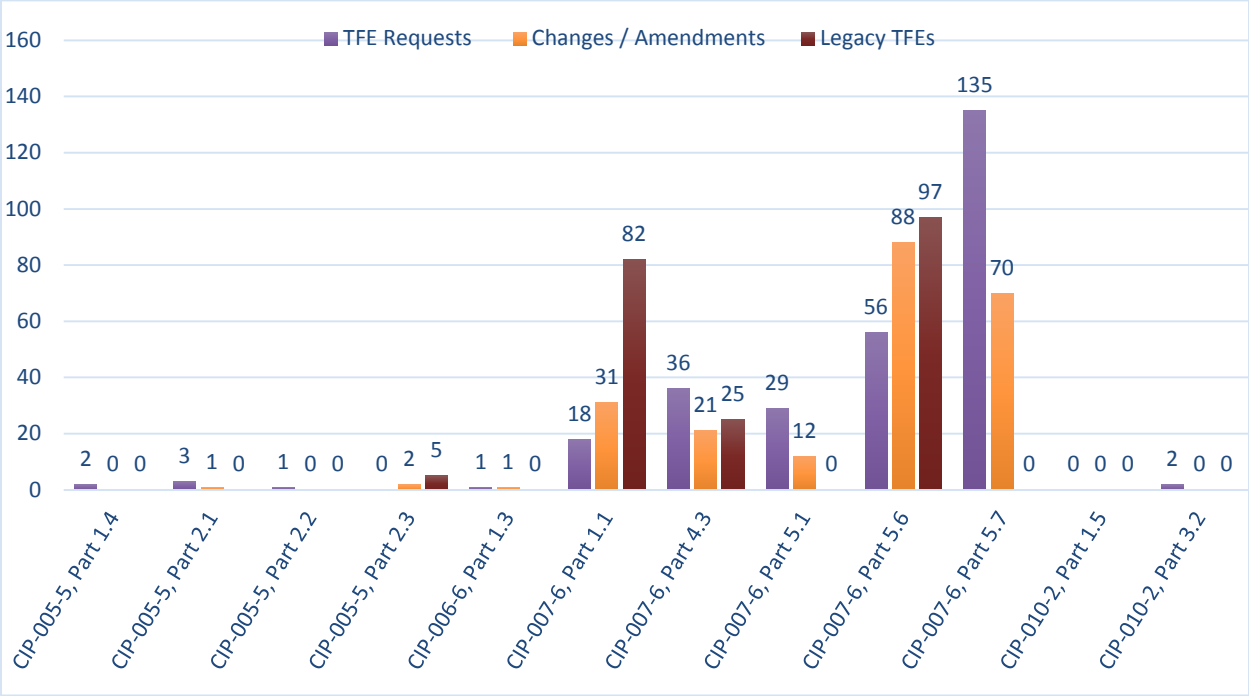


Figure 7 – TFE Requests / Changes by Requirement



Modifications to existing TFEs are tracked and reported separately from new requests but follow a similar process in their submission, review, and action. Figure 8 reflects the quantities of both new requests as well as the changes and amendments to existing requests, by requirement. In

many cases, a "single" TFE can be subjected to multiple modifications as Responsible Entities submit requests to report and track minor changes, such as updates to the quantity of assets that are the subject of the TFE.

Figure 9 pertains to modification requests that were submitted during the report period, irrespective of whether the underlying request was a new or a legacy TFE. Change requests typically due to inadvertent errors (e.g., the Responsible Entity discovers a "new" asset on the TFE change request is already part of a previously approved request) or to administratively "clear" the change request from the tracking system, such as when a Responsible Entity determines that further modifications to a pending request are necessary before the Regional Entity completes its review.

Figure 8 – ERO TFE Modifications

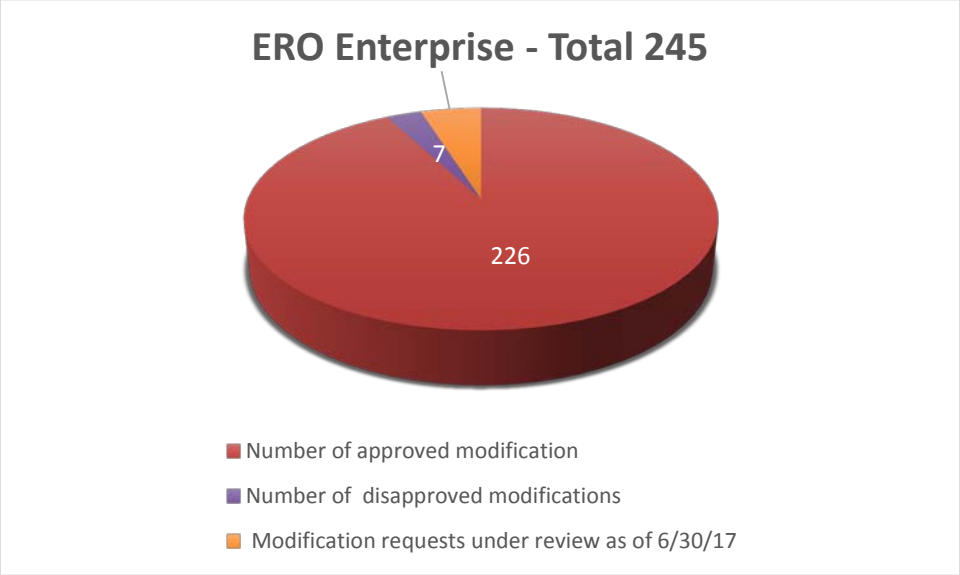
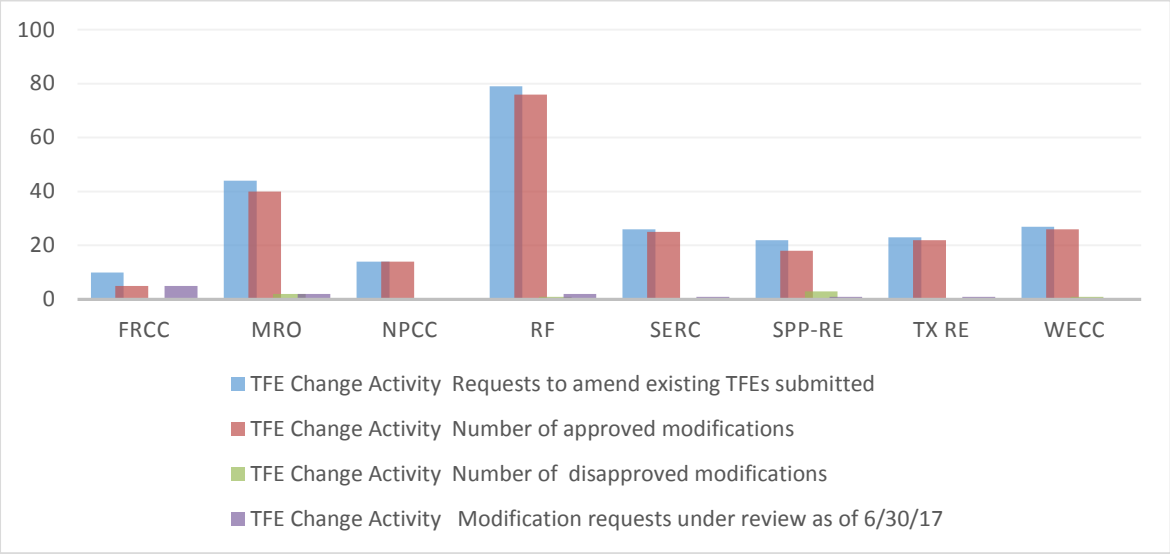


Figure 9 – ERO TFE Modifications



The total quantity of TFEs processed and in place during the 2017 Annual Report period is significantly lower than previous report periods. The results from the 2017 Annual Report period are depicted in Figure 5 and Figure 7; of particular note is the quantity of TFEs for the currently-effective version of the standards as compared to the same data from the previous year's report: a 90% decrease in the overall quantity of active TFEs. As described previously, the significant drop is considered to be a result of the currently-effective requirements providing flexibility to Responsible Entities to design protection mechanisms that address BES Cyber Systems rather than individual CCAs.

iii. Number of Unique Covered Assets for which TFEs have been Approved

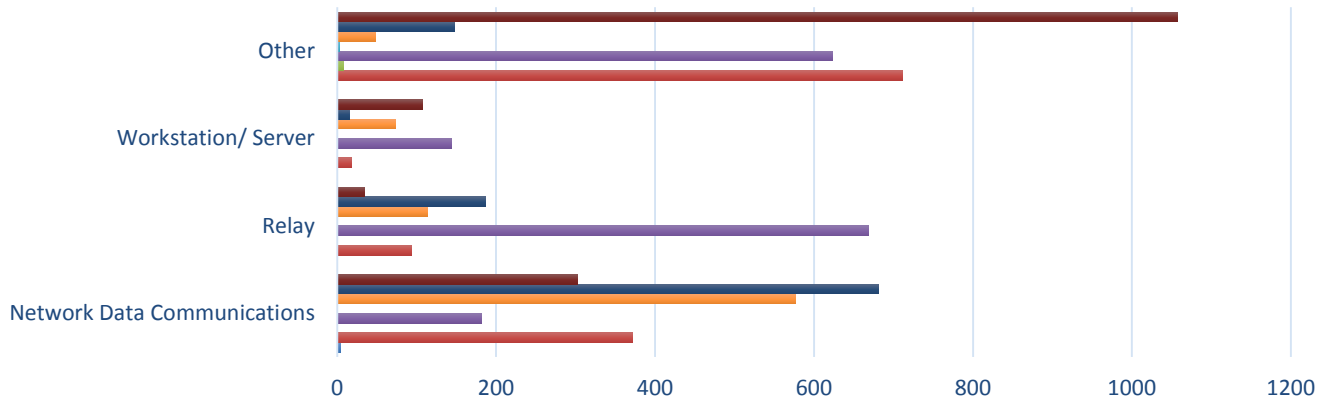
Identifying the quantity and type of unique Covered Assets for approved TFEs for prior years' reports was fairly direct, insofar as TFEs were requested on the basis of asset type, with Responsible Entities assigning each TFE request to one of four asset categories: network/data communications; relay; workstation/server; or "Other." The first three categories comprise the majority of TFE requests, and are the basis for being listed separately as category types in the TFE

request process. The “Other” category included less common assets, such as intrusion detection systems, input/output devices, etc.

The 2017 report contains similar data, with a caveat that the quantity of “other” assets in both Figure 10 and Figure 11 may include TFEs for BES Cyber Systems. A BES Cyber System could be comprised of assets that were considered “other” in past reports, but also may contain assets that would otherwise be assigned to one of the more prevalent asset categories. Figure 10 reflects the regional breakdown of assets reported for each category; Figure 11 depicts each associated CIP Reliability Standard requirements for that data.

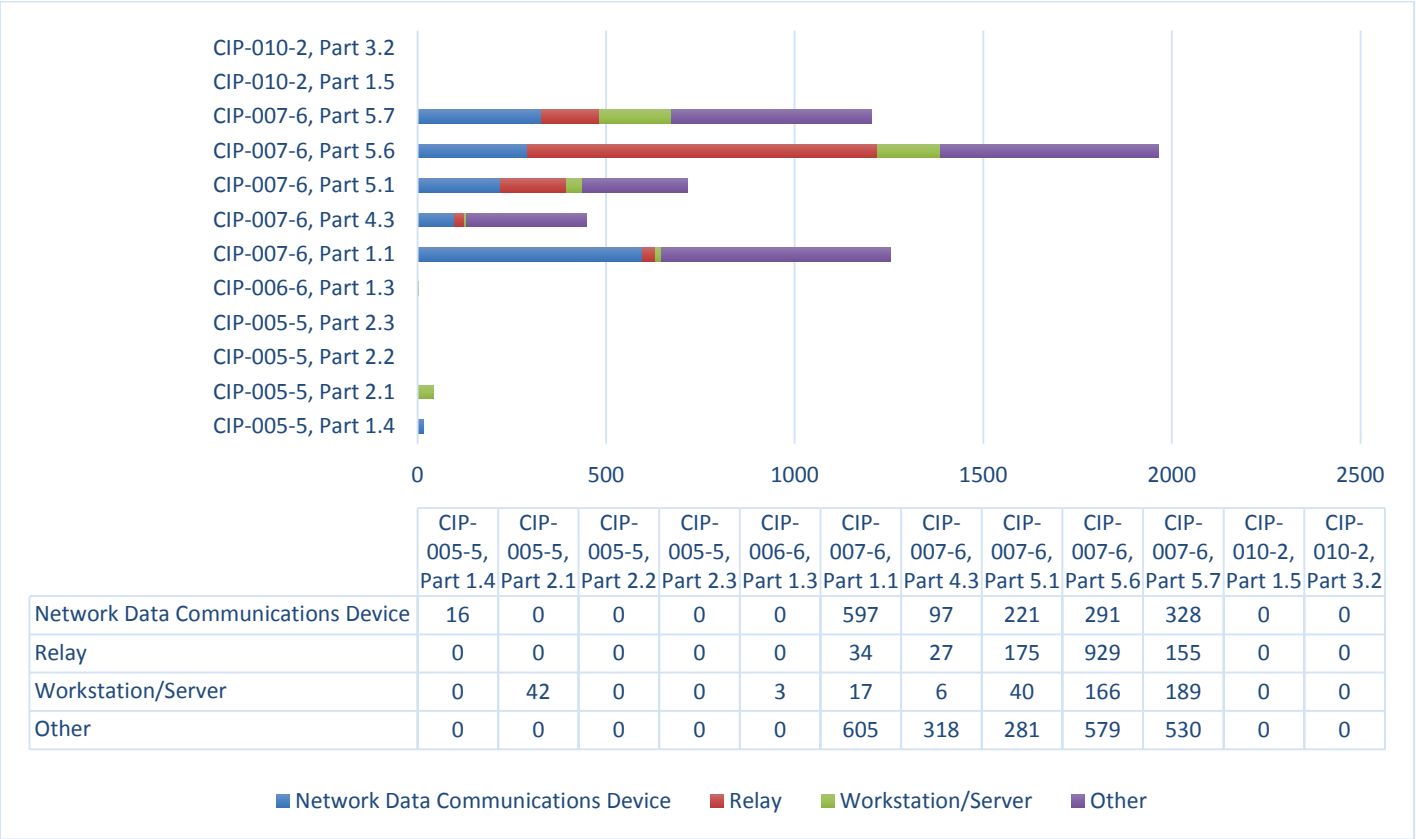
For future annual reports, the TFE Task Force (discussed elsewhere in this report) will identify methods for tracking and reporting pertinent data in support of this topic; in addition, system upgrades currently being developed within the ERO will include enhanced reporting capabilities to further identify the assets within the BES Cyber System.

Figure 10 – Number of Unique Assets with TFEs



	Network Data Communications	Relay	Workstation/ Server	Other
WECC	302	34	107	1057
TX RE	681	187	16	147
SPP-RE	577	114	73	49
SERC	0	0	0	3
RF	182	669	144	624
NPCC	0	0	0	8
MRO	372	94	18	711
FRCC	4	0	0	0

Figure 11 – TFEs by Standard / Requirement



	CIP-005-5, Part 1.4	CIP-005-5, Part 2.1	CIP-005-5, Part 2.2	CIP-005-5, Part 2.3	CIP-006-6, Part 1.3	CIP-007-6, Part 1.1	CIP-007-6, Part 4.3	CIP-007-6, Part 5.1	CIP-007-6, Part 5.6	CIP-007-6, Part 5.7	CIP-010-2, Part 1.5	CIP-010-2, Part 3.2
Network Data Communications Device	16	0	0	0	0	597	97	221	291	328	0	0
Relay	0	0	0	0	0	34	27	175	929	155	0	0
Workstation/Server	0	42	0	0	3	17	6	40	166	189	0	0
Other	0	0	0	0	0	605	318	281	579	530	0	0

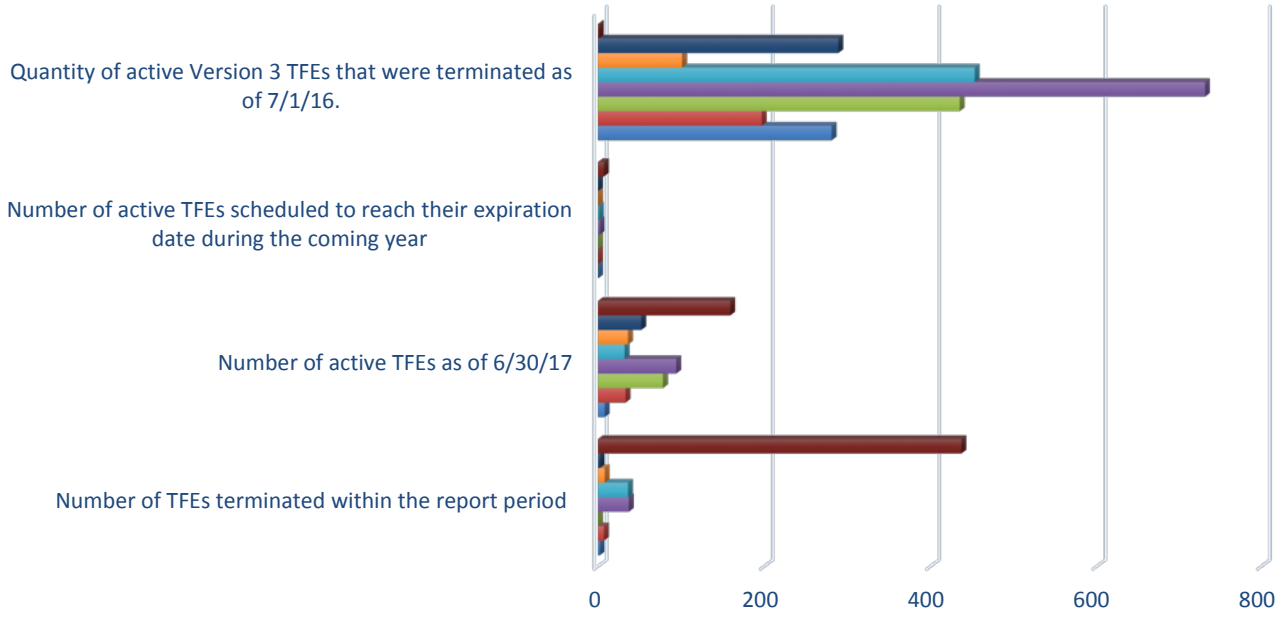
iv. Numbers of Approved TFEs Still in Effect as of the 2017 Annual Report

As depicted and discussed previously, there has been a significant decrease in the number of active TFEs as a result of the implementation of the currently-effective CIP Reliability Standards. At the end of the 2016 reporting period, there were over 3600 active TFEs; as of the end of the 2017 reporting period, that quantity decreased 80% to just under 500 active TFEs.

v. Number of TFEs that Expired or Terminated During the Reporting Period

Figure 12 shows the number of TFEs that expired or terminated during the reporting period, highlights the details of those changes, and provides the number of TFEs expected to expire or be terminated during the coming year. As noted, a significant factor in the total number of TFEs that expired or terminated is the transition to the currently-effective CIP Reliability Standards. Once the underlying requirements were superseded, the TFE was terminated.

Figure 12 - TFEs Expired or Terminated during the Reporting Period



	Number of TFEs terminated within the report period	Number of active TFEs as of 6/30/17	Number of active TFEs scheduled to reach their expiration date during the coming year	Quantity of active Version 3 TFEs that were terminated as of 7/1/16.
WECC	437	159	7	1
TX RE	2	52	0	289
SPP-RE	8	36	0	101
SERC	36	32	1	453
RF	37	94	2	731
NPCC	0	78	0	435
MRO	7	33	0	197
FRCC	2	8	0	281

vi. Number of Approved TFEs Scheduled to Reach their Expiration Dates during the Ensuing Year

See preceding section and data provided in Figure 12.

2. *Categorization of the submitted and approved TFE Requests to date by broad categories such as the general nature of the TFE Request, the Applicable Requirements covered by submitted and approved TFE Requests, and the types of Covered Assets that are the subject of submitted and approved TFE Requests.*

NERC and the Regional Entities continue to categorize submitted and approved TFEs by Applicable Requirement and type of Covered Asset. Figure 7 and Figure 9 specify the Applicable

Requirements for which the ERO has approved or disapproved TFEs. Figure 10 and Figure 11 specify the types of Covered Assets that are subject to TFE requests.

3. *Categorization of the circumstances or justifications on which the approved TFEs to date were submitted and approved, by broad categories such as the need to avoid replacing existing equipment with significant remaining useful lives, unavailability of suitable equipment to achieve Strict Compliance in a timely manner, or conflicts with other statutes and regulations applicable to the Responsible Entity.*

The transition to the currently-effective CIP Reliability Standards has not impacted the rationale used by entities for requesting TFEs. As indicated in reports from past years, a TFE request tends to be based on one of the first three criteria that are mentioned below. That pattern remains unchanged since the inception of the TFE program. To date, there have been no reports of TFEs that were approved based on any of the last three criteria:

- Not technically possible;
- Operationally infeasible;
- Precluded by technical limitations;
- Adverse effect on bulk electric system reliability;
- Cannot achieve by compliance date;
- Excessive cost that exceeds reliability benefit;
- Conflicts with other statutory or regulatory requirement; and
- Unacceptable safety risks.

4. *Categorization of the compensating measures and mitigating measures implemented and maintained by Responsible Entities pursuant to approved TFEs, by broad categories of compensating measures and mitigating measures and by types of Covered Assets.*

The ERO continues to evaluate the extent and effectiveness of compensating measures that are described in TFE requests. To address this issue, the ERO formed a "TFE Task Force," comprised of representatives from each Regional Entity as well as NERC, to review TFE requests from the entire ERO to verify sufficiency and consistency. The Task Force will perform substantive reviews of TFEs to identify positive approaches to mitigating TFEs and provide feedback in situations where it is needed. As the TFE Task Force members complete the reviews

and NERC performs oversight activities for this CMEP responsibility, information that is pertinent for the annual TFE report will be included for future reporting periods.

Although reviews are expected to be useful for identifying and sharing effective mitigating measures, auditors have observed that Responsible Entities continue to apply more than one strategy to mitigate the risk posed by a TFE. Many entities have developed defense-in-depth security controls within their CIP environments, with compensating and mitigating measures that leverage those controls. For example, a Responsible Entity may apply additional physical and logical controls that exceed the requirements, such as real-time configuration monitoring for BES Cyber Systems and having escorts call the security desk in addition to performing the required one or two-factor authentication when entering a Physical Security Perimeter.

5. *For each TFE Request that was rejected or disapproved, and for each TFE that was terminated, but for which, due to exceptional circumstances as determined by the Regional Entity, the TFE Termination Date was later than the latest date specified in Section 5.2.6, or 9.3, as applicable, a statement of the number of days the Responsible Entity was not subject to imposition of findings of violations of the Applicable Requirement or imposition of Penalties or sanctions pursuant to Section 5.3.*

All eight Regional Entities stated that there were no instances of rejection, disapproval, or termination of TFE requests during the 2017 reporting period that caused the effective date to be extended beyond the latest date specified in Section 5.2.6, or 9.3 of Appendix 4D, as applicable.

6. *A discussion, on an aggregated basis, of Compliance Audit results and findings concerning the implementation and maintenance of compensating measures and mitigating measures, and the implementation of steps and the conduct of research and analyses to achieve Strict Compliance with the Applicable Requirements, by Responsible Entities in accordance with approved TFEs.*

Appendix 4D to NERC's Rules of Procedure ("Procedure For Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards") is part of the Compliance Monitoring and Enforcement Program ("CMEP") that forms the framework for

Regional Entities to review and audit TFE requests. During a compliance audit, a Responsible Entity that has a TFE for a particular requirement is *not* evaluated against the applicable Reliability Standard for which a TFE was accepted and approved. Instead, the Responsible Entity is evaluated against the alternative compliance obligations assumed by the Responsible Entity (*i.e.*, compensating and mitigating measures).

All eight Regional Entities have conducted Compliance Audits where approved or terminated TFEs were in scope. Typically, an audit of a Registered Entity with TFEs will be managed according to the TFEs that need to be reviewed (i.e., based on factors such as quantity, locations, etc.). Reviews include interviewing subject matter experts specifically about TFEs, sampling evidence pertaining to a TFE's mitigating and compensating measures, etc. As was indicated in previous annual reports, Regional Entities continue to report that Responsible Entities are managing and maintaining their TFEs within the procedural requirements of Appendix 4D of the ROP. Regional Entities have also issued audit findings that identify TFEs to be processed consistent with the CMEP.

7. *Assessments, by Regional Entity (and for more discrete areas within a Regional Entity, if appropriate) and in the aggregate for the United States and for the jurisdictions of other Applicable Governmental Authorities, of the Wide-Area impacts on the reliability of the Bulk Electric System of approved TFEs in the aggregate, including the compensating measures and mitigating measures that have been implemented.*

Members of the TFE Task Force, described above, are the ERO subject matter experts in issues and concerns that are relevant to TFEs. In assessments that they have conducted and audits where they have participated, they state that the availability and utilization of TFEs in lieu of strict compliance has not had an adverse impact on BES reliability.

The Regional Entities have reported similar experiences with the execution and management of the TFE process and the manner in which it impacted the reliability of the BES. Regional Entities reported that a large majority of Responsible Entities have implemented multiple

compensating and mitigating measures for Covered Assets, and, in general, the mitigating and compensating measures of approved TFEs that were implemented in lieu of strict compliance with applicable CIP Reliability Standards accomplished the stated alternate compliance objective. As a result, the level of security for the BES achieved through the TFE process is comparable to strict compliance with the applicable Reliability Standards.

8. *Discussion of efforts to eliminate future reliance on TFEs.*

The value of a technical feasibility exception is the safe harbor it provides from violations when strict compliance is not achievable. However, the Responsible Entity merely provides a different type of compliance evidence when filing a TFE. The mitigations required by the TFE, compliance through other means, is still necessary while strict compliance is not met. Given that the significant decrease in the total filed TFEs, ERO compliance staff will provide feedback on the adequacy of the TFEs or whether alternate methods to comply may exist. Therefore, it is NERC's recommendation to continue emphasizing internal control processes that identify, evaluate, and implement measures that support effective security.

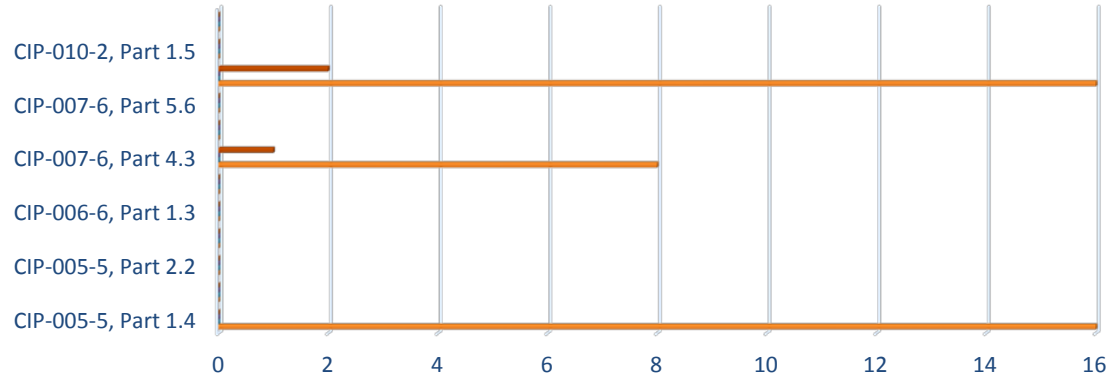
9. *Data and information regarding Material Change Reports, including the number of Material Change Reports filed annually and information regarding the types of circumstances or events that led to Material Changes, as well as any additional information NERC believes would be useful.*

When Responsible Entities update a system, replace equipment, or add assets to inventory, requests to modify existing TFEs are submitted via a "Material Change Report" ("MCR"). An MCR does not require approval by the respective Regional Entity, but the information it contains is available to the Regional Entity, which can then refer to current data when undertaking compliance activities (e.g., audits, spot checks, self-certifications, etc.). Figure 12 above includes data about active TFEs that were amended or changed during the reporting period. As indicated above, most changes are needed for asset count changes and administrative updates.

10. *Additional information about TFEs and their TFE Expiration Dates, including the number of TFEs by expiration year and CIP Standard requirement, the percentage of currently approved TFEs without TFE Expiration Dates, and the number of new TFEs approved without expiration dates annually.*

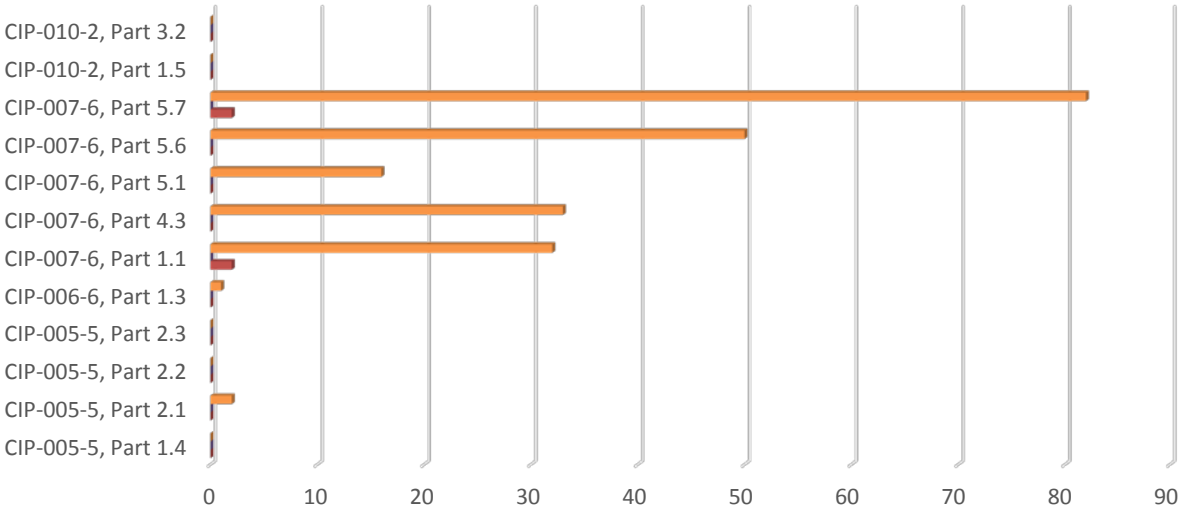
In its September 2013 Order, the Commission directed NERC to provide additional information in the annual reports related to TFEs with and without expiration dates. As has been reported previously, most TFEs do not have expiration dates. Figure 13 contains information about TFEs that are scheduled to expire before June 30, 2018; Figure 14 lists the number of TFEs that will expire later than that date.

Figure 13 – TFEs Scheduled to Expire before 6/30/2018, by Requirement



	CIP-005-5, Part 1.4	CIP-005-5, Part 2.1	CIP-005-5, Part 2.2	CIP-005-5, Part 2.3	CIP-006-6, Part 1.3	CIP-007-6, Part 1.1	CIP-007-6, Part 4.3	CIP-007-6, Part 5.1	CIP-007-6, Part 5.6	CIP-007-6, Part 5.7	CIP-010-2, Part 1.5	CIP-010-2, Part 3.2
Other	0	0	0	0	0	0	1	0	0	2	0	0
Workstation/Server	0	0	0	0	0	0	0	0	0	0	0	0
Relay	0	0	0	0	0	0	0	0	0	0	0	0
Network Data Communications Device	16	0	0	0	0	0	8	0	0	16	0	0

Figure 14 – TFE Expiring at a Later Date



	CIP-005-5, Part 1.4	CIP-005-5, Part 2.1	CIP-005-5, Part 2.2	CIP-005-5, Part 2.3	CIP-006-6, Part 1.3	CIP-007-6, Part 1.1	CIP-007-6, Part 4.3	CIP-007-6, Part 5.1	CIP-007-6, Part 5.6	CIP-007-6, Part 5.7	CIP-010-2, Part 1.5	CIP-010-2, Part 3.2
No Expiration Date	0	2	0	0	1	32	33	16	50	82	0	0
Firm date after 6/30/19	0	0	0	0	0	0	0	0	0	0	0	0
Expires 7/1/18 - 6/30/19	0	0	0	0	0	2	0	0	0	2	0	0

c. Consistency in Review, Approval and Disapproval of TFE Requests

Appendix 4D of the ROP requires that NERC and the Regional Entities collaborate to assure "consistency in the review, approval and disapproval of TFE Requests…."[11] Also, as noted above, Section 11.2.4 of the NERC Rules of Procedure requires that NERC submit with each Annual Report certain information concerning the manner in which Regional Entities have made determinations to approve or disapprove TFE requests. The scope document for the TFE Task Force that is mentioned above describes activities and deliverables that support this effort:

- Review Regional Entities' processes and performance in administering TFE Requests and Material Change Reports;
- Evaluate whether the administration of TFE activities among the Regional Entities yields consistent results;

[11] Section 11 of Appendix 4D of the NERC Rules of Procedure.

- Assess compensating and mitigating measures described in TFEs for quality and sufficiency;

- Review approved and disapproved TFE Requests or Material Change Reports for consistency; and

- Monitor active TFEs throughout their life cycle to determine whether they remain necessary and effective.

IV. CONCLUSION

For the foregoing reasons, NERC respectfully requests that the Commission accept the 2017 Annual Report.

Respectfully submitted,

/s/ Shamai Elstein

Shamai Elstein
Senior Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
shamai.elstein@nerc.net

Counsel for the North American Electric Reliability Corporation

September 28, 2017

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service list compiled by the Secretary in this proceeding.

Dated at Washington, D.C. this 28th day of September, 2017.

/s/ Shamai Elstein

Shamai Elstein
Counsel for the North American Electric Reliability Corporation