UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION	**)** **)**	**Docket No. RR10-1-001**

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

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

September 28, 2011

TABLE OF CONTENTS

I. INTRODUCTION

The North American Electric Reliability Corporation ("NERC")[1] hereby provides the first Annual Report on Wide-Area Analysis of Technical Feasibility Exceptions ("TFEs") in compliance with Paragraphs 220 and 221 of the Federal Energy Regulatory Commission's ("FERC" or "Commission") Order No. 706,[2] FERC's January 21, 2010 Order Approving TFE Procedures and Ordering Compliance Filing,[3] and Appendix 4D of the NERC Rules of Procedure.

In Order No. 706, NERC was directed to submit an annual report to the Commission that provides a wide-area analysis regarding use of the TFEs ("Annual Report") and the effect on Bulk-Power System reliability. In FERC's January 21 Order, FERC renewed its directive and ordered NERC to modify Appendix 4D of the NERC Rules of Procedure to direct the inclusion of specific criteria in the Annual Report. Currently, Appendix 4D of the NERC Rules of Procedure, as approved by FERC, requires NERC to submit its first Annual Report covering the initial period from January 1, 2010 through June 30, 2011. By this informational filing, NERC submits the Annual Report, in accordance with Order No. 706, FERC's January 21 Order, and Appendix 4D of the NERC Rules of Procedure.

In support of this first Annual Report, NERC submits supporting spreadsheets detailing the TFE data provided to NERC by the Regional Entities. (*See,* **Exhibit A**).

---

[1] The Federal Energy Regulatory Commission ("FERC" or "Commission") certified NERC as the electric reliability organization ("ERO") in its order issued on July 20, 2006 in Docket No. RR06-1-000. *North American Electric Reliability Corporation*, "Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing," 116 FERC ¶ 61,062 (July 20, 2006).

[2] Mandatory Reliability Standards for Critical Infrastructure Protection, 122 FERC ¶ 61,040 (January 18, 2008) ("Order No. 706").

[3] *Order Approving Technical Feasibility Exception Procedures and Ordering Compliance Filing*, 130 FERC ¶ 61,050 (January 21, 2010) ("January 21 Order").

II. NOTICES AND COMMUNICATIONS

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

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins*
Assistant General Counsel for Standards and Critical Infrastructure Protection

Willie L. Phillips*
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W., Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules to permit the inclusion of more than two people on the service list.

III. DISCUSSION

A. Background

In Order No. 706, FERC approved eight Critical Infrastructure Protection ("CIP") Reliability Standards and directed NERC to develop a set of conditions or criteria that a responsible entity must follow when relying on the TFE contained in specific Requirements of the CIP Reliability Standards.[4] The criteria to determine a "technical feasibility" exception are

[4] *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 FERC ¶ 61,040 at P 178 (January 18, 2008) ("Order No. 706").

intended to address "long-life equipment in place that is not readily compatible with a modern environment where cyber security issues are an acknowledged concern."[5]

Order No. 706 also provides:

> 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 . . . .[6]

On October 20, 2009, NERC submitted a petition for approval to amend the NERC Rules of Procedure to include: (i) a new Section 412, Requests for Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Reliability Standards; and (ii) a new Appendix 4D, Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards.[7]

Under the proposed TFE procedure, Appendix 4D provides that a TFE request must demonstrate that strict compliance with an applicable requirement, evaluated in the context of the Responsible Entity's covered asset that is the subject of the TFE request, is not technically feasible or is operationally infeasible. A covered asset is defined in Appendix 4D as: "A Cyber Asset or Critical Cyber Asset that is subject to an Applicable Requirement."[8]

The NERC-proposed TFE procedure also required an Annual Report that would include, at a minimum: (i) the frequency of use of the TFE Request process, (ii) categorization of the

---

[5] *Id.* at P 180.
[6] *Id*. at P 220.
[7] *Petition for Approval of Amendments to the Rules of Procedure of the North American Electric Reliability Corporation – New Section 412 and Appendix 4D, "Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards,"* Docket No. RR10-1-000 (October 29, 2009) ("NERC Petition").
[8] Section 2.9, Appendix 4D of the NERC Rules of Procedure.

submitted and approved TFE Requests to date by broad categories, (iii) categorization of the circumstances or justifications on which the approved TFEs to date were submitted and approved, (iv) categorization of the compensating measures and mitigating measures implemented and maintained by Responsible Entities, (v) a discussion of Compliance Audit results and findings concerning the implementation and maintenance of compensating measures and mitigating measures, (vi) assessments, and (vii) discussion of efforts to eliminate future reliance on TFEs.

In addition, the NERC proposal required that information on the frequency of use of the TFE process include: (a) the numbers of TFE requests that have been submitted, accepted/rejected, and approved/disapproved, (b) the number of approved TFEs that are still in effect as of on or about the date of the Annual Report, (c) the numbers of approved TFEs that reached their expiration dates, or were terminated, and (d) the number of approved TFEs that are scheduled to reach expiration date during the ensuing year.[9]

On January 21, 2010, FERC issued an order approving NERC's proposed TFE procedures and directing a compliance filing.[10] With respect to the information to be included in the Annual Report, the January 21 Order directed that:

> … NERC's report must also distinguish the number of TFEs approved from the number of assets with approved TFEs. In addition, in NERC's annual report the information required by section 12.1(iii) and (iv) must be detailed enough to allow the Commission to evaluate the level of consistency among the Regional Entities in both the justification for granting TFEs and the accepted mitigation measures among similar approved TFEs. This information should be provided to the Commission in such a way as to avoid security concerns accompanying individual asset identification. Further, NERC's annual report also should include for each TFE request that was granted an Effective Date beyond the outer limits to be set forth in sections 5.1.5 and 5.2.6, due to exceptional circumstances, the number of days the request was not subject to imposition of any

[9] NERC Petition at Appendix 4D, § 12.1(i).
[10] January 21 Order at P 14.

> findings of violations or imposition of penalties or sanctions under section 5.3.[11]

On April 21, 2010, NERC submitted a compliance filing in response to the January 21 Order that included a revised Appendix 4D. On October 1, 2010, FERC issued an order directing NERC to, among other things, revise section 12.1, "Contents of Annual Report."

On December 23, 2010, NERC filed another compliance filing revising Appendix 4D in response to FERC's October 1, 2010 Order.[12] In its April 12, 2011 Order, FERC accepted NERC's December 23, 2010 filing as compliant with its directives.[13] Therefore, Appendix 4D now provides that NERC must report annually on the consistency within the TFE process and on the criteria of TFE requests. Specifically, Section 11.2.4 of Appendix 4D, which provides reporting requirements regarding consistency within the TFE process, and Section 13, which provides criteria to be included in each annual report, state:

> **Section 11.2.4**
> NERC will submit to the FERC and to other Applicable Governmental Entities an annual informational report containing the following information concerning the manner in which Regional Entities have made determinations to approve or disapprove TFE Requests based on the criteria of Section 3.1:
>
> (i) whether any issues were identified during the period covered by the informational report with respect to the consistency of the determinations made based on the criteria in Section 3.1, either within a Regional Entity or among Regional Entities;
>
> (ii) a description of any such identified consistency issues;
>
> (iii) how each consistency issue was resolved;
>
> (iv) the numbers of TFE Requests for which reconsideration was requested pursuant to Section 5.2.9 based on purported inconsistencies in determinations applying the criteria in Section 3.1 and the numbers of such

[11] January 21 Order at P 57.
[12] *Compliance Filing of the North American Electric Reliability Corporation in Response to October 1, 2010 Commission Order Concerning Appendix 4D to the NERC Rules Of Procedure – "Procedure for Requesting and Receiving Technical Feasibility Exceptions to NERC Critical Infrastructure Protection Standards"* Docket No. RR10-1-001 (December 23, 2010)
[13] *Order on Compliance Filing*, 135 FERC ¶ 61,026 (April 12, 2011).

requests which resulted in TFE Requests being approved, disapproved and rejected; and

(v) whether NERC has developed or is in a position to develop a uniform framework for Regional Entities to use to appraise the reliability benefits of Strict Compliance when making determinations based on the criteria in Section 3.1(iv) and (vi).

Section 13

(i) 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, accepted/rejected, 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 Expiration Dates or were terminated during the preceding year; and (E) the numbers of approved TFEs that are scheduled to reach their Expiration Dates during the ensuing year;

(ii) 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;

(iii) 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;

(iv) 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;

(v) 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 Effective Date was later than the latest date specified in Section 5.1.5, 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.

(vi) 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;

(vii) 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; and

(viii) Discussion of efforts to eliminate future reliance on TFEs.

Each of these criteria is addressed below in Section III.B.

B. Summary of Annual Report

In accordance with Appendix 4D of the NERC Rules of Procedure, Regional Entities submit confidential quarterly reports to NERC regarding the types of Covered Assets for which TFE Requests are approved. In addition to providing quarterly reports, each Regional Entity submitted responses to the eight criteria identified in Section 13.1 of Appendix 4D to be included in the Annual Report. NERC has compiled and analyzed the vast amount of TFE data provided by the Regional Entities in preparation for this Annual Report.

The following is a summary of the TFE data reported by each Regional Entity for the eight criteria. **Exhibit A** to this filing provides a detailed breakdown of the compiled TFE data for criteria (i) through (v). The exhibit includes both aggregated information for the ERO and disaggregated information by Regional Entity.

1. Criterion (i): 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, accepted/rejected, 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 Expiration Dates or were terminated during the preceding year; and (E) the numbers of approved TFEs that are scheduled to reach their Expiration Dates during the ensuing year;

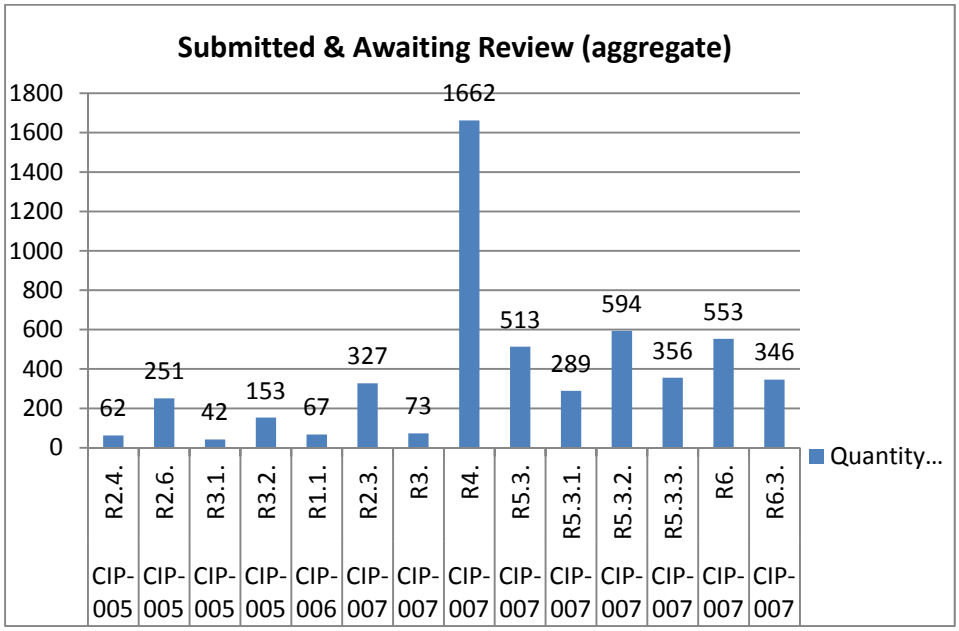
The total aggregate number of TFE requests that were in the initial stages of the review process as of June 30, 2011, is 5,288. A breakdown of TFE requests at this stage by Regional Entity is: FRCC (339), MRO (314), NPCC (0), RFC (1,173), SERC (751), SPP-RE (225), TRE (569), and WECC (1,917).

The total aggregate number of TFE requests that have been accepted since the process was initiated on January 1, 2010 is 3,492. A breakdown of TFE Requests accepted by Regional Entity is: FRCC (297), MRO (311), NPCC (27), RFC (1,065), SERC (662), SPP-RE (222), TRE (539), and WECC (369). Table 1 below provides the aggregate number of TFEs accepted, and indicates that TFEs are most frequently accepted for Reliability Standard CIP-007, Requirement (R) 4.[14]

[14] CIP-007, R 4 provides:

> 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).

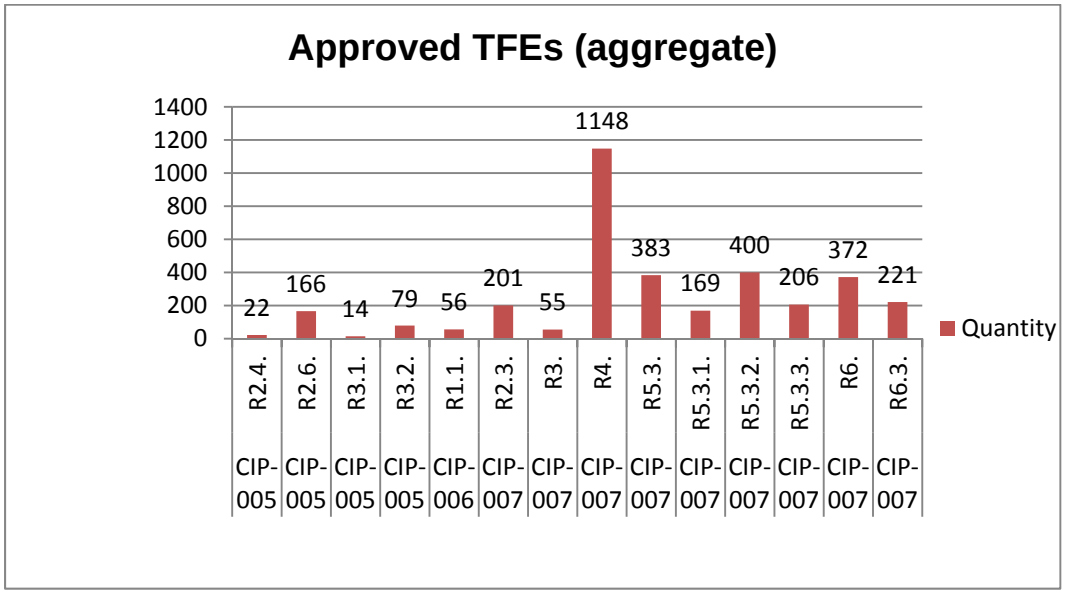
Table 1



The total number of TFE requests that have been rejected is 448. A breakdown of TFE Requests rejected by Regional Entity is: FRCC (6), MRO (1), NPCC (2), RFC (105), SERC (62), SPP-RE (1), TRE (30), and WECC (241).

The total number of TFE Requests that have been accepted and approved are 3,369. A breakdown of the TFE Requests accepted and approved by Regional Entity is: FRCC (199), MRO (304), NPCC (385), RFC (943), SERC (362), SPP-RE (146), TRE (459), and WECC (568). As shown in Table 2 below, TFEs for CIP-007, R4, are the most frequently accepted and approved TFEs.

Table 2



The total number of TFE Requests that have been accepted and disapproved is 782. A breakdown of the TFE Requests accepted and disapproved by Regional Entity is as follows: FRCC (30), MRO (7), NPCC (0), RFC (53), SERC (160), SPP-RE (41), TRE (80), and WECC (411). "Accepted and disapproved" means that the proposed TFE met the initial filing requirements for acceptance, but upon subsequent detailed review was determined not to qualify.

To date, the number of unique Covered Assets for which TFEs have been approved is 68,323. A breakdown of approved Covered Assets by Regional Entity is: FRCC (1,988), MRO (7,577), NPCC (9,715), RFC (22,116), SERC (9,535), SPP-RE (2,433), TRE (7,647), and WECC (7,311).

The numbers of approved TFEs that are active and still in effect as of this report are 2,416. A breakdown of TFE Requests active and still in effect by Regional Entity is: FRCC (195), MRO (235), NPCC (385), RFC (771), SERC (368), SPP-RE (104), TRE (324), and WECC (34).

The number of approved TFEs that reached their expiration dates or were terminated during the preceding year is 565. A breakdown of TFE requests that reached their expiration dates or were terminated by Regional Entity is: FRCC (4), MRO (79), NPCC (26), RFC (172), SERC (15), SPP-RE (119), TRE (135), and WECC (15).

The number of approved TFEs that are scheduled to reach their expiration dates during the ensuing year is 166. A breakdown of TFE Requests to reach their expiration dates during the ensuing year by Regional Entity is: FRCC (3), MRO (23), NPCC (4), RFC (80), SERC (17), SPP-RE (8), TRE (5), and WECC (26).

2. Criteria (ii): 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.

As indicated in the Table 3 below, CIP-007, R4, includes the single largest category of TFE's, with 5,063 submitted and approved Covered Assets. CIP-007, R5 – when combining CIP-007, R5, R5.3.1, R5.3.2, and R5.3.3 – also accounts for 7,048 of the total submitted and approved Covered Assets. A significant amount of Covered Assets were also submitted and approved for CIP-005, R2 (868) and CIP-007, R3 (465).

The three largest categories of submitted and approved Covered Assets include: Network Data Communications Devices (3,215), Industrial Process Control Systems (3,064), and Servers (2,403). As one Regional Entity (FRCC) reported, the ubiquitous presence of Microsoft Windows operating system has been an issue for Responsible Entities in meeting password requirements. Moreover, Regional Entities report that TFEs for CIP-007, R4, include multiple devices that will likely not have anti-malware available in the near future. (*e.g.*, relays, remote terminal units (RTU), programmable logic controllers (PLC), and printers).

Table 3

Asset Categories (per Part A of TFE request)	Quantity of TFEs - submitted & approved														
	CIP-005				CIP-006	CIP-007									
	R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R5.3.1	R5.3.2	R5.3.3	R6	R6.3	Total
Data Storage Device	0	16	0	3	0	3	2	104	12	33	52	5	13	10	270
Digital Protective Control Device	0	1	0	0	0	5	0	20	4	1	6	2	7	1	70
Electronic Access Control System	6	74	0	12	6	2	6	249	7	9	28	16	3	1	482
Electronic Access Monitoring System	3	16	5	2	2	0	2	212	9	13	66	25	8	0	387
Industrial Process Control System	0	10	0	6	0	558	2	644	592	17	60	54	588	563	3214
Mainframe Computer	2	0	0	0	0	0	0	2	0	0	1	0	0	0	5
Network Data Communications Devices	5	44	3	24	7	38	12	1631	459	34	217	38	470	233	3440
PC Laptop	2	4	0	0	5	16	31	21	136	2	90	14	4	8	353
Peripheral Device	0	5	0	3	0	27	1	99	52	35	35	21	81	52	489
Physical Access Control System	3	127	3	15	2	7	2	135	82	12	43	20	16	14	528
Physical Access Monitoring System	1	10	3	16	11	9	2	74	21	14	36	12	8	7	227
Physical Security Perimeter	0	1	0	2	21	1	0	7	0	1	3	1	1	1	46
Relay	0	4	0	0	0	7	0	218	16	2	15	7	13	4	315
RTU	0	8	0	9	0	17	0	240	22	7	9	7	33	19	427
Servers	1	1	3	1	4	30	396	980	250	19	564	34	60	61	2475
Telecommunications Device	3	20	0	11	4	22	1	51	4	23	26	12	29	16	247
Transmitters	0	0	0	0	0	4	0	4	2	2	2	0	4	0	21
Valve Controllers	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
Other	0	18	8	3	120	45	3	211	55	64	110	70	108	84	1040
Total	33	405	32	135	185	868	465	5303	1779	322	1418	374	1573	1145	14037

3. Criteria (iii): 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.

In Table 4 below, the categories of circumstances or justifications on which the TFEs to date were submitted and approved include:

- Not technically possible (2,814)
- Operationally infeasible (227)
- Precluded by technical limitations (774)
- Adverse effect on BES reliability (41)
- Cannot achieve by compliance date (94)
- Excessive cost that exceeds reliability benefit (21)
- Conflicts with other statutory or regulatory requirement(74)
- Unacceptable safety risks (3)

When assessing proposed TFEs, the Regional Entities considered the criteria that each Responsible Entity used as the basis for each request. A large majority of TFEs (nearly 3,000) cited "not technically possible" as the basis for the request. The figures below show the aggregate percentages for each of the cited categories:

- Not technically possible 71%
- Precluded by technical limitations 19%
- Operationally infeasible 6%
- Cannot achieve by compliance date 2%
- Adverse effect on BES reliability 1%
- Excessive cost that exceeds reliability benefit <1%
- Conflicts with other statutory or regulatory requirement <1%
- Unacceptable safety risks <1%

Table 4

Asset Categories (per Part A of TFE request)	Aggregate - Approved TFEs - Basis								
	Not technically possible	Operationally infeasible	Precluded by technical limitations	Adverse effect on BES reliability	Cannot achieve by compliance date	Unacceptable safety risks	Conflicts with other statutory or regulatory requirement	Excessive cost that exceeds reliability benefit	Total
Data Storage Device	88	4	8	0	9	0	0	0	109
Digital Protective Control Device	40	0	1	0	3	0	2	0	46
Electronic Access Control System	208	9	38	0	4	0	1	5	265
Electronic Access Monitoring System	127	4	77	2	6	0	0	1	217
Industrial Process Control System	230	21	85	11	5	0	0	0	352
Mainframe Computer	3	2	0	0	0	0	0	0	5
Network Data Communications Device	725	30	113	3	32	0	1	2	906
PC Laptop	43	33	28	5	2	0	0	2	113
Peripheral Device	214	1	40	0	2	0	3	0	260
Physical Access Control System	164	10	37	0	0	0	0	1	212
Physical Access Monitoring System	112	9	38	0	0	0	0	1	160
Physical Security Perimeter	19	5	11	0	1	0	2	1	39
Relay	76	2	5	0	1	0	2	0	86
RTU	149	8	6	0	0	0	0	0	163
Server	194	66	88	19	23	3	0	1	394
Telecommunications Device	153	5	4	0	1	0	0	2	165
Transmitters	6	0	0	0	0	0	0	0	6
Valve Controllers	1	0	0	0	0	0	0	0	1
Other	262	18	195	1	5	0	3	5	489
Total	2814	227	774	41	94	3	14	21	3988

4. Criteria (iv): 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.

Several Regional Entities reported that Responsible Entities employ multiple strategies to protect Covered Assets that are unable to meet applicable Reliability Standards. The principal strategies employed include protecting devices with physical and logical security controls. A significant portion of compensating and mitigating measures involved firewalls, the use of Intrusion Detection and Intrusion Prevention (IDS/IPS) systems, and strong access policies.

Responsible Entities may use similar compensating and mitigating measures, but implementation of those measures amongst those Responsible Entities can vary. For example, an entity with a security center manned 24-hours a day may rely on security personnel so that only authorized personnel can gain access to a device. Another entity that does not have round-the-clock coverage in its security center may use physical monitoring, but also rely on security cameras and motion detectors.

Table 5 below shows the categorization of mitigation and compensation measures. The largest category is Electronic Security Perimeter (ESP) (2,386). Other significant compensating and mitigating measures deployed include Physical Security Perimeter (PSP) (1,582), Authentication (795), IDS/IPS (502), and System Status Monitoring (338).

Table 5

Asset categories (per Part A of TFE request)	Aggregate - Approved TFEs - Risk Mitigation/Compensation Strategies									
	ESP	PSP	IDS/ IPS	Training	System Status Monitoring	Malware Prevention	Authentication	Encryption	Physical Monitoring	Total
Data Storage Device	64	54	26	8	23	19	22	0	5	221
Digital Protective Control Device	23	24	12	1	7	5	16	0	5	93
Electronic Access Control System	140	97	38	30	47	21	62	5	17	457
Electronic Access Monitoring System	110	105	18	54	38	42	64	2	21	454
Industrial Process Control System	253	178	42	28	103	42	77	0	32	755
Mainframe Computer	1	1	1	0	1	1	2	0	1	8
Network Data Communications Device	536	345	135	77	196	117	163	3	65	1637
PC Laptop	52	34	14	10	28	15	19	1	6	179
Peripheral Device	194	105	40	27	64	14	28	0	8	480
Physical Access Control System	124	78	8	20	22	13	35	11	17	328
Physical Access Monitoring System	92	48	11	21	14	9	33	3	28	259
Physical Security Perimeter	3	5	0	2	2	2	3	2	18	37
Relay	60	53	13	1	20	12	36	3	12	210
RTU	108	83	22	0	35	18	25	1	17	309
Server	225	125	53	72	54	39	83	1	26	678
Telecommunications Device	96	81	17	1	31	14	20	1	3	264
Transmitters	6	7	1	0	0	0	0	0	0	14
Valve Controllers	1	1	0	0	1	0	0	0	0	3
Other	298	158	51	97	142	33	107	3	57	946
Total	2386	1582	502	449	828	416	795	36	338	7332

5. Criteria (v) – 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 Effective Date was later than the latest date specified in Section 5.1.5, 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 (FRCC, MRO, NPCC, RFC, SERC, SPP-RE, TRE, and WECC) reported that there were no instances of rejection, disapproval, or termination of TFE requests, where the effective date was extended past the latest date specified in Section 5.1.5, 5.2.6, or 9.3, as applicable, of Appendix 4D to the NERC Rules of Procedure.

6. Criteria 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.

The TFE Procedure, in conjunction with the Compliance Monitoring and Enforcement Program (CMEP), is the framework that Regional Entities utilize to review and audit TFE requests. During a compliance audit where TFEs are in scope, the subject Responsible Entity is *not* evaluated against the applicable 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 in the approved TFE request (*i.e.*, compensating and mitigating measures).

Seven of the eight Regional Entities (FRCC, MRO, NPCC, RFC, SERC, SPP-RE, and WECC) have conducted Compliance Audits where approved or terminated TFEs were in scope. Generally, Regional Entities found that Responsible Entities are managing and maintaining their TFEs within the procedural requirements of Appendix 4D. Only two Regional Entities (MRO

and RFC) have issued audit findings against approved TFEs to be processed as potential violations through the CMEP.

7. Criteria 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.

The wide-area impact of approved TFEs on the reliability of the BES, in the aggregate, has been minimal. The issues identified by the Regional Entities, as a result of the assessment, include: implementation of anti-virus software and malware prevention tools, as required by CIP-007 R4; implementation passwords or specific password criteria, as required by CIP-007 R5.3, R5.3.1, R5.3.2 and R5.3.3; and inability to monitor or log system events related to Cyber Security, as required by CIP-007 R6 and R6.3.

Each Regional Entity reported similar experiences with the execution and management of the TFE process and the manner in which it impacted the reliability of the BES. 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.

Regional Entities reported that a large majority of Responsible Entities have implemented multiple compensating and mitigating measures for Covered Assets. 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. As previously noted, the primary compensating and mitigating measures deployed by Regional Entities include the following Covered Asset protections: ESP, PSP, Authentication, IDS/IPS, and System Status Monitoring.

The following is a summary of the Regional Entity data submitted for Criteria 7.

a) FRCC Region

FRCC reported that it has had over 400 "actionable" TFEs submitted, amended, or resubmitted since the program's inception. While the range of TFEs submitted to FRCC includes all possible requirements, and represents nearly every device type, most TFEs have been identified by the entity as minimal impact to the BES. FRCC has concurred with the majority of those assessments.

Generally, FRCC has found that Responsible Entities are diligent in applying compensating and mitigating measures that are appropriate to the potential impact those systems could have on reliability. Compensating and mitigating measures have typically utilized multiple strategies, ranging from physical isolation of a device to logical isolation behind firewalls that have strict rules, require two factor authentication, and use Intrusion Detection or Intrusion Prevention devices or both. According to FRCC, these efforts have helped ensure that the net effect is equal to or better than strict compliance.

FRCC also reported that Responsible Entities have increased awareness of cyber security requirements through various measures. During compliance audits and spot checks, FRCC determined that the overall effort placed on securing the Critical Cyber Assets (CCAs) has been substantial.

b) MRO Region

MRO has received and processed 314 TFEs, not including Canadian Entity submittals and TFE amendments. After assessing the impact on the reliability of the BES, MRO identified the following three risk areas where Covered Assets cannot:

- Implement anti-virus software and malware prevention tools required by CIP-007 R4. In the MRO footprint these represent 35% of the approved TFEs and 37.5% of all

Covered Assets. Of the TFEs submitted regarding CIP-007 R4, Network and Data Communications devices represent 30% of the Covered Assets.

- Implement passwords or specific password criteria required by CIP-007 R5.3, R5.3.1, R5.3.2 and R5.3.3. In the MRO footprint these Requirements combined represent 30% of the approved TFEs and 15% of the Covered Assets. No specific Covered Asset category represents a large percentage of the Covered Assets submitted against TFEs for these Requirements. The numbers are spread across a wide variety of device types.

- Monitor or log system events related to Cyber Security required by CIP-007 R6 and R6.3. In the MRO footprint, these Requirements combined represent 15% of the approved TFEs and 30% of all Covered Assets. No specific Covered Asset category that represents a large percentage of the Covered Assets submitted against TFEs for these Requirements. The numbers are spread across a wide variety of device types.

The three risk areas identified by MRO represent 80% of its TFEs, and 82.5% of the Covered Assets in TFEs submitted to MRO. According to MRO, an analysis of the device types indicates that most are legacy or proprietary equipment that were never designed or produced with the capability to implement various security controls as defined in applicable CIP Requirements.

MRO concluded that Responsible Entities have implemented a defense-in-depth security model when deploying compensating and mitigating measures. The majority of MRO TFEs detail multiple compensating and mitigating measures deployed or being deployed to achieve at least a comparable level of security for the BES, as would strict compliance with applicable Requirements. The four primary compensating and mitigating measures deployed in the MRO Region are detailed below with their frequency of use: ESP (27.5%), PSP (21%), IDS/IPS (14.5%), and System Status Monitoring (13.5%).

c) NPCC Region

The majority of the TFEs submitted to NPCC were found to have minimal impact to the BES. NPCC determined that the compensating and mitigating measures for those devices further minimizes the exposure of those assets for which the TFEs have been filed. The Part B Substantive Reviews conducted by NPCC revealed that most Responsible Entities have implemented multiple compensating and mitigating measures thereby affording the Responsible Entities a defense-in-depth security model.

d) ReliabilityFirst Region

Reliability*First* Corporation (RFC) has received and processed 1,173 TFEs from Responsible Entities not including TFE amendments. Based upon an assessment of the impact on the reliability of the BES, RFC identified the risk areas where Covered Assets cannot:

- Implement antivirus software and malware prevention tools required by CIP-007 R4. In the RFC footprint these represent 33% of the approved TFEs and 29% of all Covered Assets. Of the TFEs submitted against Requirement CIP-007 R4, Network and Data Communications Devices represent 30% of the Covered Assets.

- Implement passwords or specific password criteria required by CIP-007 R5.3, R5.3.1, R5.3.2 and R5.3.3. In the RFC footprint these Requirements combined represent 41.5% of the approved TFEs and 43% of the Covered Assets. No one Covered Asset category that represents a large percentage of the Covered Assets submitted against TFEs for these Requirements. The numbers are spread across a wide variety of device types.

- Monitor or log system events related to Cyber Security as required by CIP-007 R6 and R6.3. In the RFC footprint these Requirements combined represent 13% of the approved TFEs and 13.5% of all Covered Assets. No one Covered Asset category that represents a large percentage of the Covered Assets submitted against TFEs for these Requirements. The numbers are spread across a wide variety of device types.

The three risk areas identified by RFC represent 87.5% of the TFEs with 85.5% of the Covered Assets in TFEs submitted to ReliabilityFirst. An analysis of the device types indicates that numerous legacy or proprietary equipment were never designed or produced with the capability to implement various security controls as defined in Applicable CIP Requirements.

RFC generally reported that Responsible Entities have implemented a defense-in-depth security model when deploying compensating and mitigating measures. Moreover, RFC found that most TFEs detail multiple compensating and mitigating measures deployed or being deployed to achieve at least a comparable level of security for the BES, as would strict compliance with the applicable requirement. The four primary compensating and mitigating measures deployed to mitigate risks are detailed below with their frequency of use: ESP (33.5%), PSP (19%), IDS/IPS (12%), and System Status Monitoring (15.5%).

e) SERC Region

SERC received and processed 751 TFEs from Responsible Entities within its footprint. Generally, SERC reported that Responsible Entities have implemented effective protective measures that have resulted in limiting reliability impact on the BES. However, SERC reports that the TFE process is burdensome for the Responsible Entities and for Regional resources. For instance, significant resources are spent submitting and reviewing TFEs on certain types of devices that are widely known to be unable to support a feature that is required by applicable CIP Reliability Standards (*e.g.*, anti-virus software on a network printer).

f) SPP-RE Region

In the SPP-RE Region, Responsible Entities reported no significant risks to the reliability of the BES as a result of approved TFEs, such as the loss of situation awareness, system

visibility, or system control. According to SPP-RE, the implementation of compensating and mitigating measures achieve a comparable or better level of protection as strict compliance offsets any potential risks, so that TFEs have a minimal impact on the reliability of the BES within the SPP-RE footprint.

Typical compensating and mitigating measures that have been implemented by Responsible Entities within the SPP RE region include: ESP, PSP, IDS/IPS, Training, Status Monitoring, Host-Based Malware Prevention (where Covered Assets cannot implement antivirus or anti-malware tools, they are protected by all other cyber assets within a defined ESP having these security controls installed and managed), Enhanced Authentication (Access to Covered Assets and all Cyber Assets that reside within a defined ESP are protected by multi-factor authentication services such as RSA SecurID, digital certificates, or biometrics), Data Encryption (when mandatory controls cannot be implemented, data is encrypted between CCAs to protect data confidentiality and integrity), and Physical Monitoring.

g) Texas RE Region

Texas RE received and processed 569 TFEs from Responsible Entities within its footprint. Based upon Texas RE's assessment, the wide-area impact of TFEs on the reliability of the BES is minimal. However, Texas RE reported that the TFE process is burdensome and has not increased the security or reliability of the BES. With respect to compensating and mitigating measures for TFEs, Texas RE did not report any impacts on the BES.

h) WECC Region

WECC received and processed 1,917 TFEs from Responsible Entities within its footprint. WECC reported that the TFE process is not fully developed and is overly burdensome for both

the Regional and Registered Entities. According to WECC, the value of the TFE process to the BES and reliable operations is minimal. With respect to compensating and mitigating measures for TFEs, WECC did not report any impacts on the BES.

8. Criterion 8 - Discussion of efforts to eliminate future reliance on TFEs.

Regional Entities (FRCC, MRO, NPCC, RFC, and WECC) report that many efforts are being considered to eliminate future reliance on TFEs:

- Upgrade or replace Covered Assets that will enable implementation of security controls defined in CIP Standards and Requirements;
- Remove CCAs that covered by approved TFEs that reside within defined ESPs;
- Retire legacy systems that are now subject to coverage by an approved TFE; and
- Implement previously unused or unidentified functionality on Covered Assets that will achieve strict compliance with the Applicable Requirement.

Where applicable, upgrades of Covered Assets will result in strict compliance without having to rely on TFEs. According to one Regional Entity (NPCC), Responsible Entities have researched the means to achieve strict compliance and reduce the number of TFEs required, but many of the devices for which TFEs are submitted cannot and may never be able to achieve strict compliance with the standards as written.

In addition, efforts such as forming committees and discussion groups to determine where a new or existing device should reside, training IT personnel on the expectations of applicable Reliability Standards, and coordination with the Regional Entity compliance monitoring and enforcement staff regarding the need for TFEs, has led to the continuing decline of the number of devices that rely on a TFE for compliance. Moreover, non-essential devices are also being evaluated for continued inclusion within a defined ESP. Where a device does not need to reside within the ESP for operational necessity, Covered Assets have been relocated

outside the ESP, eliminating the need for a TFE and reducing residual risk to devices remaining within the ESP.

The primary barriers identified by Regional Entities to eliminating TFEs include: 1) revising Reliability Standards, 2) certifying vendors, and 3) retaining legacy systems. With respect to revising applicable standards, some regions (notably SERC) report that it can be difficult to establish a minimum threshold, and provide flexibility for technology and changes in security. For example, the current password standards are very specific (*e.g.*, requiring at least six characters) in some cases, but standards can be strengthened to define the required complexity and to allow for strong, non-password technologies such as biometrics or two-factor authentication. With respect to vendors, there is support for developing requirements to use products that are certified as meeting an appropriate security standard. Many legacy systems in operation were built to last, not necessarily built to be compatible with enhanced security features. Applying those types of enhanced security features often means that properly operating equipment would need to be replaced with more modern, secure models. Therefore, in order to eliminate the need for a TFE, replacement costs may become a barrier to implementing enhanced security features.

C. Consistency in Approval and Disapproval of TFE Requests

Appendix 4D of the NERC Rules of Procedure require NERC and the Regional Entities to engage in the activities "for the purpose of assuring consistency in the review, approval and disapproval of TFE Requests…."[15] Also, as noted above, Section 11.2.4 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:

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

Section 11.2.4
(i) whether any issues were identified during the period covered by the informational report with respect to the consistency of the determinations made based on the criteria in Section 3.1, either within a Regional Entity or among Regional Entities;

(ii) a description of any such identified consistency issues;

(iii) how each consistency issue was resolved;

(iv) the numbers of TFE Requests for which reconsideration was requested pursuant to Section 5.2.9 based on purported inconsistencies in determinations applying the criteria in Section 3.1 and the numbers of such requests which resulted in TFE Requests being approved, disapproved and rejected; and

(v) whether NERC has developed or is in a position to develop a uniform framework for Regional Entities to use to appraise the reliability benefits of Strict Compliance when making determinations based on the criteria in Section 3.1(iv) and (vi).

NERC has not received any reports of inconsistency either in assessing the accuracy or validity of TFEs submitted by Responsible Entities, or in the decisions approving or rejecting TFEs. Specifically, no requests were received from Responsible Entities asserting "that the approval, disapproval or rejection by a Regional Entity of a TFE Request submitted by the Responsible Entity constitutes an inconsistent application of the criteria specified in Section 3.1 as compared to other determinations of TFE Requests made by the same Regional Entity or another Regional Entity for the same type of Covered Assets…."[16]

NERC and the Regional Entities formed a group of "TFE Managers" to serve as the committee to review approved and disapproved TFE Requests for consistency. Primary and alternate representatives from each region, facilitated by NERC staff, met regularly to discuss common concerns. Those representatives also led the efforts at their respective regions for receiving, reviewing, and reporting TFE-related data.

[16] Section 5.2.8 of Appendix 4D of the NERC Rules of Procedure.

In addition to the TFE Managers' regularly scheduled conference calls and face-to-face meetings, the TFE Managers communicated regularly by email, and discussed consistency issues at workshops and other meetings. Potential inconsistencies were commonly discussed in a roundtable fashion until a consensus was reached on the pertinent issues.

The TFE management effort also included the development of common tools and processes for the Responsible Entities to use when submitting TFE requests. Specifically, NERC worked with the Regional Entities to leverage their existing portals (used for tracking other compliance-related data) to include confidential TFE processes. The TFE Managers also developed templates for quarterly and annual reports that Responsible Entities submit to NERC.

Appendix 4D requires NERC to develop a "uniform framework for Regional Entities to use to appraise the reliability benefits of Strict Compliance when making determinations based on the criteria in Section 3.1(iv) and (vi)." Those criteria pertain to TFEs that cite safety risks or issues that outweigh the reliability benefits, or that cite the incurrence of costs that far exceed the benefits to reliability.

The TFE management approach outlined above is used for TFE requests citing safety risks; however, very few such TFE requests have been submitted. Of the 3,369 approved TFEs, only 3 cited "safety risks" as a basis, while 21 pointed to "excessive costs." The TFEs that cited safety risks came from an entity with servers used to manage EMS applications that could cause equipment malfunctions if anti-virus software was installed. The Responsible Entity felt that it would ultimately create an unsafe operating condition. In this particular case, however, the Regional Entity determined that other basis categories also could have been cited (*e.g.*, operationally infeasible or adverse effect on reliability), so the region accepted the request as submitted.

Examples of approved TFE requests that cited excessive costs include:

- Unprotected wiring that provides a communication link between discrete electronic security perimeters and not within an ESP for which increased physical security would add no significant reliability benefit.
- A"six wall boundary" around a Physical Security Perimeter had a gap between the top of the wall and the hard ceiling. The opening was needed for proper operation of the building's HVAC system, so the Responsible Entity implemented other physical security measures as an alternative.

For TFE requests that asserted that costs exceeded the benefits to reliability, auditors not only conducted standard interviews with subject matter experts and assessments of compensating or mitigating measures, but also analyzed cost studies provided by Responsible Entities.

IV. CONCLUSION

For the foregoing reasons, NERC respectfully requests that the Commission accept this Annual Report as compliant with the directives contained in Order No. 706 and Appendix 4D of NERC's Rules of Procedure.

Respectfully submitted,

/s/ Willie L. Phillips

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Holly A. Hawkins
Assistant General Counsel for Standards and Critical Infrastructure Protection

Willie L. Phillips
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
holly.hawkins@nerc.net
willie.phillips@nerc.net

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, 2011.

/s/ Willie L. Phillips
Willie L. Phillips
Attorney for North American Electric Reliability Corporation

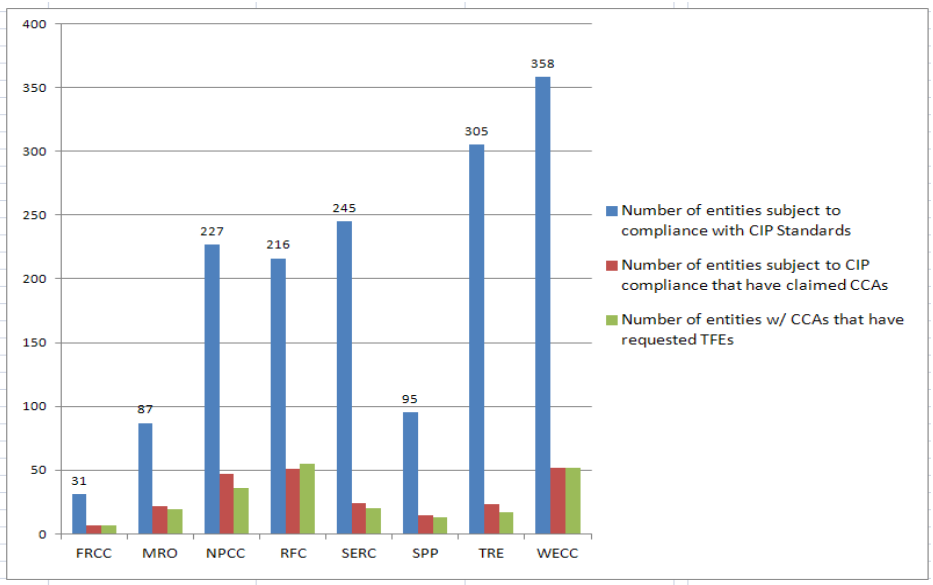
September 28, 2011

Annual Report—Wide-Area Analysis of Technical Feasibility Exceptions

Exhibit A: Supporting Spreadsheets

1. Program Information

	Period Covered:	Jan 1, 2010--Jun 30, 2011	Date of Report:	28-Sep-11	
	Number of entities subject to compliance with CIP Standards	**Number of entities subject to CIP compliance that have claimed CCAs**	**Number of entities w/ CCAs that have requested TFEs**	**TFE Manager**	**Alternate**
FRCC	31	7	7	Steve Kruse	Carlos Valiente
MRO	87	22	19	Steen Fjalstad	Tom Tierney
NPCC	227	47	36	Marie Kozub Peter Scalici	David Cerasoli
RFC	216	51	55	Bob Yates	Ray Sefchik
SERC	245	24	20	Matt Stryker	Mike Almeyda
SPP	95	15	13	Shon Austin	Kevin Perry
TRE	305	23	17	Bill Beaver	Kevin Bunch
WECC	358	52	52	Brent Castagnetto	Kim Israelsson
TOTAL	**1564**	**241**	**219**		



2a. TFE Requests (Aggregate)

Aggregate -- TFE Status

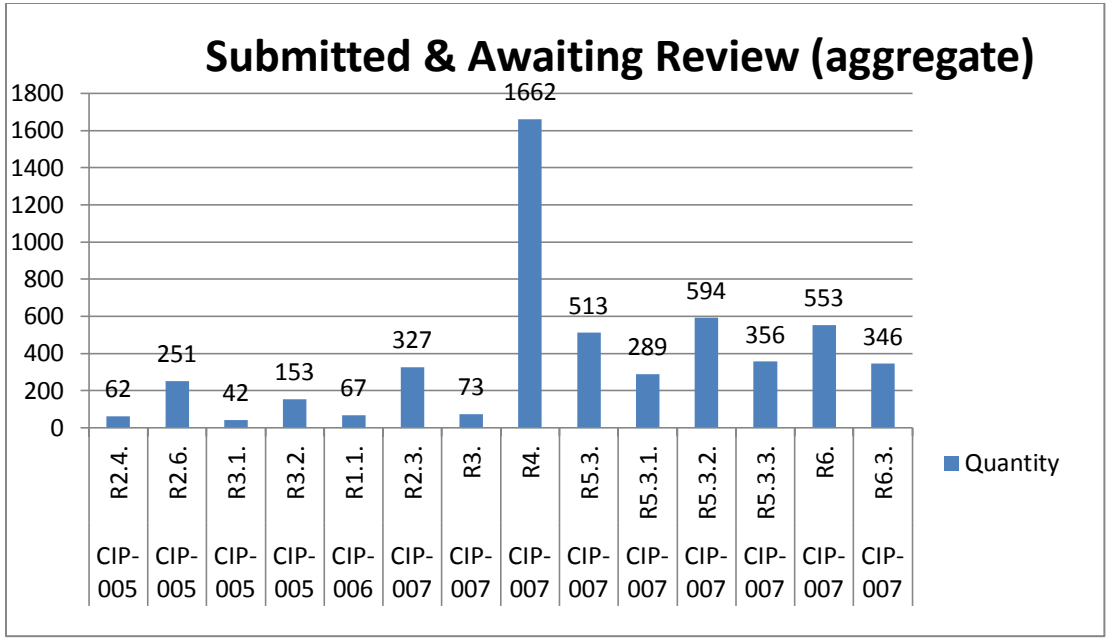
State	CIP Requirement	Total	# of Covered Assets
a. Initial submission & Pending			
CIP-005	R2.4.	62	826
CIP-005	R2.6.	251	3131
CIP-005	R3.1.	42	517
CIP-005	R3.2.	153	1353
CIP-006	R1.1.	67	2099
CIP-007	R2.3.	327	9033
CIP-007	R3.	73	1709
CIP-007	R4.	1662	42241
CIP-007	R5.3.	513	17229
CIP-007	R5.3.1.	289	6592
CIP-007	R5.3.2.	594	15456
CIP-007	R5.3.3.	356	12590
CIP-007	R6.	553	14273
CIP-007	R6.3.	346	7755
b. Accepted (5.1)			
CIP-005	R2.4.	22	393
CIP-005	R2.6.	166	1641
CIP-005	R3.1.	14	102
CIP-005	R3.2.	79	564
CIP-006	R1.1.	56	965
CIP-007	R2.3.	201	6024
CIP-007	R3.	55	1673
CIP-007	R4.	1148	24730
CIP-007	R5.3.	383	11621
CIP-007	R5.3.1.	169	3435
CIP-007	R5.3.2.	400	9425
CIP-007	R5.3.3.	206	9498
CIP-007	R6.	372	8639
CIP-007	R6.3.	221	4418
c. Rejected (5.1)			
CIP-005	R2.4.	20	270
CIP-005	R2.6.	15	401
CIP-005	R3.1.	17	348
CIP-005	R3.2.	23	303
CIP-006	R1.1.	1	3
CIP-007	R2.3.	26	990
CIP-007	R3.	2	38
CIP-007	R4.	62	2827
CIP-007	R5.3.	31	836
CIP-007	R5.3.1.	48	1678
CIP-007	R5.3.2.	85	3236
CIP-007	R5.3.3.	64	2255
CIP-007	R6.	35	973
CIP-007	R6.3.	19	976

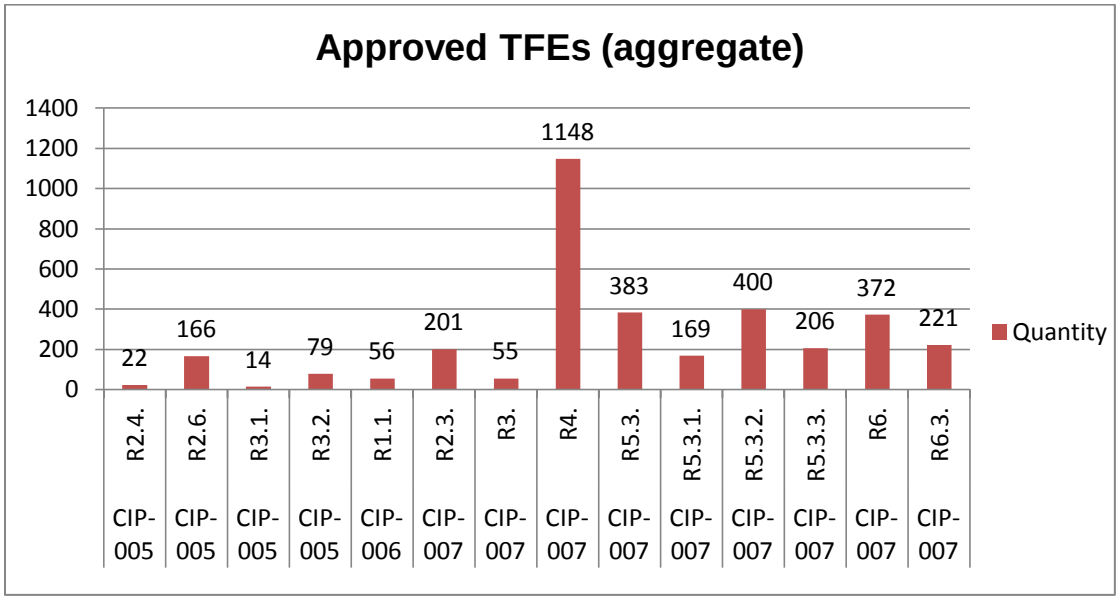
Aggregate -- TFE Status

State	CIP Requirement	Total	# of Covered Assets
d. Approved (5.2)			
CIP-005	R2.4.	25	356
CIP-005	R2.6.	170	1435
CIP-005	R3.1.	16	111
CIP-005	R3.2.	85	651
CIP-006	R1.1.	44	802
CIP-007	R2.3.	173	5500
CIP-007	R3.	60	1953
CIP-007	R4.	1225	23721
CIP-007	R5.3.	317	7388
CIP-007	R5.3.1.	149	2033
CIP-007	R5.3.2.	350	6919
CIP-007	R5.3.3.	195	4266
CIP-007	R6.	331	8322
CIP-007	R6.3.	229	4866
e. Disapproved (5.2)			
CIP-005	R2.4.	5	18
CIP-005	R2.6.	51	1253
CIP-005	R3.1.	3	12
CIP-005	R3.2.	31	220
CIP-006	R1.1.	11	1103
CIP-007	R2.3.	57	1982
CIP-007	R3.	14	330
CIP-007	R4.	182	4525
CIP-007	R5.3.	91	1883
CIP-007	R5.3.1.	62	1655
CIP-007	R5.3.2.	79	2088
CIP-007	R5.3.3.	56	794
CIP-007	R6.	83	2586
CIP-007	R6.3.	57	1237
f. Terminated/expired prior to June 30, 2011 (ON schedule or earlier due to the Responsible Entity's efforts) (9.0)			
CIP-005	R2.4.	6	155
CIP-005	R2.6.	43	260
CIP-005	R3.1.	3	17
CIP-005	R3.2.	31	179
CIP-006	R1.1.	7	24
CIP-007	R2.3.	34	616
CIP-007	R3.	22	349
CIP-007	R4.	163	1110
CIP-007	R5.3.	54	974
CIP-007	R5.3.1.	31	200
CIP-007	R5.3.2.	46	469
CIP-007	R5.3.3.	33	327
CIP-007	R6.	65	472
CIP-007	R6.3.	41	206

Aggregate -- TFE Status

State	CIP Requirement	Total	# of Covered Assets
g. Terminated prior to June 30, 2011 (EARLIER THAN scheduled by Region's direction) (9.0)			
CIP-005	R2.4.	0	0
CIP-005	R2.6.	0	0
CIP-005	R3.1.	0	0
CIP-005	R3.2.	0	0
CIP-006	R1.1.	0	0
CIP-007	R2.3.	0	0
CIP-007	R3.	0	0
CIP-007	R4.	0	0
CIP-007	R5.3.	0	0
CIP-007	R5.3.1.	0	0
CIP-007	R5.3.2.	0	0
CIP-007	R5.3.3.	0	0
CIP-007	R6.	0	0
CIP-007	R6.3.	0	0
h. TFEs scheduled to terminate between July 1, 2011 and June 30, 2012			
CIP-005	R2.4.	5	66
CIP-005	R2.6.	3	22
CIP-005	R3.1.	1	18
CIP-005	R3.2.	5	43
CIP-006	R1.1.	2	2
CIP-007	R2.3.	14	469
CIP-007	R3.	9	100
CIP-007	R4.	48	684
CIP-007	R5.3.	18	141
CIP-007	R5.3.1.	6	72
CIP-007	R5.3.2.	26	281
CIP-007	R5.3.3.	13	168
CIP-007	R6.	13	485
CIP-007	R6.3.	3	38
i. Active TFEs (includes those scheduled to terminate after			
CIP-005	R2.4.	18	255
CIP-005	R2.6.	112	1115
CIP-005	R3.1.	10	96
CIP-005	R3.2.	46	460
CIP-006	R1.1.	37	768
CIP-007	R2.3.	105	4519
CIP-007	R3.	45	1658
CIP-007	R4.	916	19793
CIP-007	R5.3.	244	6290
CIP-007	R5.3.1.	103	1691
CIP-007	R5.3.2.	282	6317
CIP-007	R5.3.3.	142	3846
CIP-007	R6.	214	6970
CIP-007	R6.3.	142	4279


Submitted & Awaiting Review (aggregate)
1800
1600
1400
1200
1000
800
600
400
200
0
62
251
42
153
67
327
73
1662
513
289
594
356
553
346
R2.4.
R2.6.
R3.1.
R3.2.
R1.1.
R2.3.
R3.
R4.
R5.3.
R5.3.1.
R5.3.2.
R5.3.3.
R6.
R6.3.
CIP-005
CIP-005
CIP-005
CIP-005
CIP-006
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
Quantity


Approved TFEs (aggregate)
1400
1200
1000
800
600
400
200
0
22
166
14
79
56
201
55
1148
383
169
400
206
372
221
R2.4.
R2.6.
R3.1.
R3.2.
R1.1.
R2.3.
R3.
R4.
R5.3.
R5.3.1.
R5.3.2.
R5.3.3.
R6.
R6.3.
CIP-005
CIP-005
CIP-005
CIP-005
CIP-006
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
CIP-007
Quantity

2b. TFE Requests, Status (by Region)

State	CIP Standard Requirement	FRCC		MRO		NPCC		RFC		SERC		SPP		TRE		WECC	
		Total	# of Covered	Total	# of Covered	Total	# of Covered	Total	# of Covered	Total	# of Covered	Total	# of Covered	Total	# of Covered	Total	# of Covered
a. Initial submission & Pending Review (4.0)																	
CIP-005	R2.4.	1	2	6	157			6	231	2	6			8	27	39	403
CIP-005	R2.6.	10	80	9	120			43	821	20	310	19	70	56	402	94	1328
CIP-005	R3.1.							13	103			1	10			28	404
CIP-005	R3.2.	3	24	7	53			8	65	5	9	9	39	47	397	74	766
CIP-006	R1.1.	10	124	8	516			16	20	16	282	1	1	6	22	10	1,134
CIP-007	R2.3.	29	480	17	280			43	2969	52	1735	7	210	36	593	143	2,766
CIP-007	R3.	8	216	13	301			13	404	12	462	7	69	3	46	17	211
CIP-007	R4.	81	950	105	2856			407	8199	191	5267	97	1416	134	2133	647	21,420
CIP-007	R5.3.	38	626	25	466			151	3894	124	2523	15	287	30	584	130	8,849
CIP-007	R5.3.1.	19	225	11	56			51	1219	50	2010	9	91	44	648	105	2,343
CIP-007	R5.3.2.	47	733	29	305			162	4314	111	5297	25	523	58	1190	162	3,094
CIP-007	R5.3.3.	23	665	36	395			95	3278	21	1203	8	139	46	676	127	6,234
CIP-007	R6.	34	371	32	1223			111	3423	90	2663	17	491	57	867	212	5,235
CIP-007	R6.3.	36	314	16	989			54	1038	57	1783	10	252	44	444	129	2,935
b. Accepted (5.1)																	
CIP-005	R2.4.	1	2	6	157			4	184	2	6	0	0	8	27	1	17
CIP-005	R2.6.	7	64	8	112	1	1	40	575	22	322	19	70	56	402	13	95
CIP-005	R3.1.							11	85	0	0	1	10			2	7
CIP-005	R3.2.	1	16	6	27			7	51	6	22	8	27	43	348	8	73
CIP-006	R1.1.	10	124	7	515			16	20	15	275	1	1	6	22	1	8
CIP-007	R2.3.	23	308	17	280			42	2625	43	1505	7	210	32	578	37	518
CIP-007	R3.	2	4	13	301			19	786	11	467	7	69	3	46	0	0
CIP-007	R4.	75	825	105	2856	13	119	378	7165	180	4241	95	1156	129	2109	173	6,259
CIP-007	R5.3.	35	606	25	466	3	15	144	3551	110	2448	16	293	28	578	22	3,664
CIP-007	R5.3.1.	16	199	11	56	2	13	45	969	34	919	9	91	41	637	11	551
CIP-007	R5.3.2.	44	707	29	305	1	1	138	3768	96	2640	24	598	53	1157	15	249
CIP-007	R5.3.3.	20	628	36	395	2	13	80	2970	9	157	8	123	42	661	9	4,551
CIP-007	R6.	30	347	32	1223	3	37	97	2846	78	2147	17	440	54	855	61	744
CIP-007	R6.3.	33	301	16	989	2	35	44	766	56	1385	10	252	44	444	16	246
c. Rejected (5.1)																	
CIP-005	R2.4.									0	0					20	270
CIP-005	R2.6.							2	244	0	0					13	157
CIP-005	R3.1.							2	18	0	0					15	330
CIP-005	R3.2.	2	8	1	26			1	14	1	1			4	49	14	205
CIP-006	R1.1.					1	3			0	0					0	0
CIP-007	R2.3.							1	344	8	97			4	15	13	534
CIP-007	R3.									1	7					1	31
CIP-007	R4.	2	87					26	937	8	83	1	2	5	17	20	1701
CIP-007	R5.3.							6	250	2	56			2	6	21	524
CIP-007	R5.3.1.							6	250	11	840			3	11	28	577
CIP-007	R5.3.2.					1	26	24	546	9	2308			5	33	46	323
CIP-007	R5.3.3.	1	31					15	308	10	1013			4	15	34	888
CIP-007	R6.	1	13					12	283	10	90			3	12	9	575
CIP-007	R6.3.							10	272	2	62			0	0	7	642

3a. TFE Requests, Device Categories (Aggregate)

asset categories (per Part A of TFE request)	Aggregate - Quantity of TFEs submitted & approved													
	CIP-005				CIP-006	CIP-007								
	R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
Data Storage Device	0	19	0	3	0	3	2	113	13	33	52	6	14	12
Digital Protective Control Device	0	1	0	0	0	7	0	28	6	2	7	4	14	1
Electronic Access Control System	9	82	0	17	6	3	7	290	9	9	28	16	5	1
Electronic Access Monitoring System	3	17	6	7	2	1	2	226	10	13	66	25	9	0
Industrial Process Control System	0	12	0	6	0	568	3	673	605	24	71	61	613	578
Mainframe Computer	2	0	0	0	0	0	0	2	0	0	1	0	0	0
Network Data Communications Device	6	52	6	31	7	61	12	1751	466	42	223	42	494	247
PC Laptop	2	4	0	0	5	22	31	23	137	3	93	16	6	11
Peripheral Device	0	9	0	6	0	31	1	122	59	38	37	21	100	65
Physical Access Control System	3	131	3	16	2	10	2	151	89	16	49	24	17	15
Physical Access Monitoring System	1	10	3	16	11	10	2	76	21	14	36	12	8	7
Physical Security Perimeter	0	2	0	2	23	1	0	10	0	1	4	1	1	1
Relay	0	4	0	1	0	7	0	226	16	5	19	9	17	11
RTU	0	9	1	11	0	23	1	263	25	8	10	7	49	20
Server	1	6	4	3	4	39	397	1018	252	21	569	38	61	62
Telecommunications Device	4	21	0	11	4	23	1	63	7	23	26	12	33	19
Transmitters	0	0	0	0	0	4	0	5	2	2	3	0	5	0
Valve Controllers	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Other	2	26	9	5	121	55	4	262	62	68	124	80	127	95

3b(1). TFE Requests, Device Categories (by Region)

FRCC

asset categories	Quantity of TFEs submitted & approved													
	CIP-005				CIP-006	CIP-007								
	R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
Data Storage Device	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Digital Protective Control Device	0	0	0	0	0	2	0	2	0	0	2	0	1	1
Electronic Access Control System	1	1	0	0	1	0	0	8	1	0	1	1	0	0
Electronic Access Monitoring System	0	1	0	0	1	0	0	5	0	1	2	0	0	0
Industrial Process Control System	0	0	0	0	0	1	0	2	5	1	2	2	2	3
Mainframe Computer	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Network Data Communications Device	1	1	0	0	2	2	0	26	6	2	8	1	3	3
PC Laptop	0	0	0	0	2	0	0	1	2	0	2	1	0	0
Peripheral Device	0	0	0	0	0	2	0	7	2	3	3	1	5	4
Physical Access Control System	0	3	0	1	1	0	0	5	2	1	3	1	0	0
Physical Access Monitoring System	0	2	0	1	1	0	0	3	1	1	3	1	1	1
Physical Security Perimeter	0	1	0	1	1	0	0	1	0	1	2	1	0	0
Relay	0	0	0	0	0	2	0	2	1	0	0	0	2	2
RTU	0	0	0	0	0	0	0	1	1	0	0	0	1	1
Server	0	0	0	0	1	4	0	9	6	3	11	3	4	6
Telecommunications Device	0	0	0	0	2	0	0	0	0	0	0	0	0	0
Transmitters	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Valve Controllers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	4	3	0	3	2	1	1	1	4	3

MRO

asset categories	Quantity of TFEs submitted & approved													
	CIP-005				CIP-006	CIP-007								
	R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
Data Storage Device	0	1	0	0	0	0	1	7	0	0	0	1	1	1
Digital Protective Control Device	0	0	0	0	0	0	0	2	0	1	1	2	1	0
Electronic Access Control System	2	4	0	0	0	0	4	20	1	1	3	2	2	1
Electronic Access Monitoring System	2	5	0	1	0	0	1	8	2	2	3	3	1	0
Industrial Process Control System	0	0	0	0	0	0	0	13	12	0	1	8	11	0
Mainframe Computer	0	0	0	0	0	0	0	1	0	0	1	0	0	0
Network Data Communications Device	1	0	0	2	1	4	5	45	5	4	10	8	6	5
PC Laptop	0	0	0	0	0	2	4	0	0	0	2	5	0	0
Peripheral Device	0	0	0	0	0	0	0	9	1	0	0	0	4	2
Physical Access Control System	0	4	0	2	0	2	2	6	1	0	3	0	4	1
Physical Access Monitoring System	0	2	0	2	0	1	1	5	0	0	4	0	3	1
Physical Security Perimeter	0	0	0	0	2	1	0	3	0	0	1	0	1	1
Relay	0	0	0	0	0	0	0	2	1	1	1	1	1	1
RTU	0	0	0	0	0	1	0	3	1	0	1	0	1	1
Server	1	0	0	1	0	4	6	10	2	0	6	6	1	1
Telecommunications Device	0	0	0	0	1	1	1	5	1	1	2	1	1	1
Transmitters	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Valve Controllers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	0	0	0	5	6	0	14	6	2	5	7	6	5

3b(2). TFE Requests, Device Categories (by Region)

NPCC

asset categories	Quantity of TFEs submitted & approved													
	CIP-005				CIP-006	CIP-007								
	R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
Data Storage Device	0	0	0	0	0	0	0	2	0	0	0	0	1	1
Digital Protective Control Device	0	0	0	0	0	0	0	7	1	0	0	0	0	0
Electronic Access Control System	1	1	0	4	0	0	0	32	0	0	1	0	1	0
Electronic Access Monitoring System	1	1	0	0	0	0	0	14	0	2	4	0	1	0
Industrial Process Control System	0	2	0	0	0	10	0	16	8	1	1	1	7	6
Mainframe Computer	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Network Data Communications Device	1	10	0	1	0	3	0	63	3	2	5	0	8	5
PC Laptop	0	1	0	0	0	2	0	5	1	0	2	0	1	1
Peripheral Device	0	1	0	0	0	1	0	16	2	3	3	3	7	4
Physical Access Control System	0	3	0	2	1	0	0	15	2	0	1	1	2	2
Physical Access Monitoring System	0	1	0	1	0	0	0	6	0	0	1	1	0	0
Physical Security Perimeter	0	0	0	0	0	0	0	2	0	0	0	0	0	0
Relay	0	0	0	0	0	2	0	0	1	1	4	0	0	0
RTU	0	1	0	0	0	5	0	12	4	1	2	1	6	5
Server	0	0	0	0	0	3	0	24	4	0	1	0	0	2
Telecommunications Device	0	0	0	0	0	0	0	5	1	0	0	0	1	2
Transmitters	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Valve Controllers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	1	0	0	1	5	0	36	4	1	3	1	10	6

RFC

Quantity of TFEs submitted & approved														
CIP-005				CIP-007										
R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
0	1	0	0	0	0	1	12	6	3	5	2	4	3
0	0	0	0	0	1	0	5	1	0	3	0	2	0
0	6	0	0	0	2	2	41	2	0	11	9	0	0
0	7	5	1	0	0	0	52	4	4	19	19	2	0
0	3	0	0	0	12	2	30	25	8	17	13	19	8
2	0	0	0	0	0	0	0	0	0	0	0	0	0
1	11	3	3	0	7	5	128	48	11	28	21	23	7
2	0	0	0	0	1	3	7	3	0	11	2	3	0
0	0	0	0	0	2	0	13	4	5	5	5	7	6
0	1	3	4	0	0	0	6	3	3	12	3	5	6
0	0	3	3	0	0	0	6	0	3	9	3	4	5
0	0	0	0	15	0	0	1	0	0	0	0	0	0
0	4	0	0	0	3	0	12	4	0	7	6	6	0
0	1	0	0	0	3	0	13	3	0	0	1	11	3
0	0	3	0	0	4	8	43	25	3	34	14	3	1
0	1	0	0	1	0	0	3	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	10	8	3	0	7	2	66	14	21	50	44	27	22

3b(3). TFE Requests, Device Categories (by Region)

SERC

asset categories	Quantity of TFEs submitted & approved													
	CIP-005				CIP-006	CIP-007								
	R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
Data Storage Device	0	10	0	0	0	2	0	74	3	27	44	0	4	4
Digital Protective Control Device	0	0	0	0	0	0	0	0	2	0	0	0	0	0
Electronic Access Control System	1	49	0	8	5	0	0	121	3	3	5	0	0	0
Electronic Access Monitoring System	0	0	0	0	1	0	0	121	3	0	30	0	4	0
Industrial Process Control System	0	0	0	0	0	532	0	571	535	0	32	23	541	541
Mainframe Computer	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Network Data Communications Device	0	5	0	0	4	9	0	1285	377	5	150	0	399	196
PC Laptop	0	0	0	0	3	9	24	0	129	0	64	0	0	0
Peripheral Device	0	0	0	0	0	16	0	36	32	12	12	0	44	26
Physical Access Control System	0	110	0	0	0	0	0	89	74	0	10	2	0	0
Physical Access Monitoring System	0	0	0	0	10	0	0	37	20	0	7	0	0	0
Physical Security Perimeter	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Relay	0	0	0	0	0	0	0	198	8	0	0	0	0	0
RTU	0	0	0	0	0	0	0	199	9	0	0	0	6	6
Server	0	0	0	0	3	12	380	875	210	8	491	6	50	50
Telecommunications Device	0	0	0	0	0	12	0	20	0	12	12	0	12	0
Transmitters	0	0	0	0	0	4	0	4	2	2	2	0	4	0
Valve Controllers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	6	0	0	106	19	0	75	21	33	42	8	51	47

SPP

Quantity of TFEs submitted & approved														
CIP-005				CIP-006	CIP-007									
R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
0	1	0	1	0	0	0	1	0	0	0	0	1	0
0	1	0	0	0	0	0	1	0	0	0	0	1	0
0	8	0	0	0	0	0	6	0	4	5	3	0	0
0	1	0	0	0	0	0	3	0	0	2	1	0	0
0	0	0	0	0	1	0	3	1	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	4	0	2	0	2	2	27	6	1	8	2	5	0
0	0	0	0	0	0	0	4	0	0	3	1	0	7
0	1	0	1	0	0	1	3	0	0	0	0	1	1
0	0	0	2	0	0	0	0	0	0	1	1	0	0
0	0	0	2	0	0	0	0	0	0	2	1	0	0
0	0	0	1	1	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	0	0	1	0	2	1
0	0	0	0	0	0	0	2	0	0	0	0	1	0
0	1	0	0	0	1	0	6	0	3	9	2	0	0
0	1	0	0	0	0	0	4	1	1	3	2	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	2	0	7	3	2	2	2	4	0

3b(4). TFE Requests, Device Categories (by Region)

TRE

asset categories	Quantity of TFEs submitted & approved													
	CIP-005				CIP-006	CIP-007								
	R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
Data Storage Device	0	3	0	2	0	1	0	8	3	3	3	2	2	1
Digital Protective Control Device	0	0	0	0	0	2	0	3	0	0	0	0	2	0
Electronic Access Control System	1	5	0	0	0	0	0	21	0	1	2	1	0	0
Electronic Access Monitoring System	0	1	0	0	0	0	1	9	0	4	6	2	0	0
Industrial Process Control System	0	5	0	6	0	2	0	9	6	7	7	7	8	5
Mainframe Computer	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Network Data Communications Device	1	13	0	16	0	11	0	57	14	9	8	6	26	17
PC Laptop	0	3	0	0	0	2	0	4	1	2	6	5	0	0
Peripheral Device	0	3	0	2	0	6	0	15	11	12	12	12	13	9
Physical Access Control System	3	6	0	4	0	5	0	14	0	8	13	12	5	5
Physical Access Monitoring System	1	5	0	7	0	8	1	17	0	10	10	6	0	0
Physical Security Perimeter	0	0	0	0	2	0	0	0	0	0	0	0	0	0
Relay	0	0	0	0	0	0	0	3	1	0	2	0	2	0
RTU	0	6	0	9	0	8	0	10	4	6	6	5	7	3
Server	0	0	0	0	0	2	2	13	3	2	12	3	2	1
Telecommunications Device	3	18	0	11	0	9	0	14	0	9	9	9	15	13
Transmitters	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Valve Controllers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	0	1	0	0	4	3	1	10	5	4	7	7	6	1

WECC

asset categories	Quantity of TFEs submitted & approved													
	CIP-005				CIP-006	CIP-007								
	R2.4	R2.6	R3.1	R3.2	R1.1	R2.3	R3.2	R4	R5.3	R 5.3.1	R5.3.2	R5.3.3	R6	R6.3
Data Storage Device	0	3	0	0	0	0	0	9	1	0	0	1	1	2
Digital Protective Control Device	0	0	0	0	0	2	0	8	2	1	1	2	7	0
Electronic Access Control System	3	8	0	5	0	1	1	41	2	0	0	0	2	0
Electronic Access Monitoring System	0	1	1	5	0	1	0	14	1	0	0	0	1	0
Industrial Process Control System	0	2	0	0	0	10	1	29	13	7	11	7	25	15
Mainframe Computer	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Network Data Communications Device	1	8	3	7	0	23	0	120	7	8	6	4	24	14
PC Laptop	0	0	0	0	0	6	0	2	1	1	3	2	2	3
Peripheral Device	0	4	0	3	0	4	0	23	7	3	2	0	19	13
Physical Access Control System	0	4	0	1	0	3	0	16	7	4	6	4	1	1
Physical Access Monitoring System	0	0	0	0	0	1	0	2	0	0	0	0	0	0
Physical Security Perimeter	0	1	0	0	2	0	0	3	0	0	1	0	0	0
Relay	0	0	0	1	0	0	0	8	0	3	4	2	4	7
RTU	0	1	1	2	0	6	1	23	3	1	1	0	16	1
Server	0	5	1	2	0	9	1	38	2	2	5	4	1	1
Telecommunications Device	1	1	0	0	0	1	0	12	3	0	0	0	4	3
Transmitters	0	0	0	0	0	0	0	1	0	0	1	0	1	0
Valve Controllers	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	2	8	1	2	1	10	1	51	7	4	14	10	19	11

4. Approved TFE Requests, Basis for Submission (Aggregate)

	Aggregate							
asset categories (per Part A of TFE request)	Aggregate - Approved TFEs - Basis							
	Not technically possible	Operationally infeasible	Precluded by technical limitations	Adverse effect on BES reliability	Cannot achieve by compliance date	Unacceptable safety risks	Conflicts with other statutory or regulatory	Excessive cost that exceeds reliability benefit
Data Storage Device	88	4	8	0	9	0	0	0
Digital Protective Control Device	40	0	1	0	3	0	2	0
Electronic Access Control System	208	9	38	0	4	0	1	5
Electronic Access Monitoring System	127	4	77	2	6	0	0	1
Industrial Process Control System	230	21	85	11	5	0	0	0
Mainframe Computer	3	2	0	0	0	0	0	0
Network Data Communications Device	725	30	113	3	32	0	1	2
PC Laptop	43	33	28	5	2	0	0	2
Peripheral Device	214	1	40	0	2	0	3	0
Physical Access Control System	164	10	37	0	0	0	0	1
Physical Access Monitoring System	112	9	38	0	0	0	0	1
Physical Security Perimeter	19	5	11	0	1	0	2	1
Relay	76	2	5	0	1	0	2	0
RTU	149	8	6	0	0	0	0	0
Server	194	66	88	19	23	3	0	1
Telecommunications Device	153	5	4	0	1	0	0	2
Transmitters	6	0	0	0	0	0	0	0
Valve Controllers	1	0	0	0	0	0	0	0
Other	262	18	195	1	5	0	3	5

5. Approved TFE Requests, Mitigating/Compensating Strategies (Aggregate)

	Aggregate								
Asset categories (per Part A of TFE request)	Aggregate - Approved TFEs - Risk Mitigation/Compensation Strategies								
	ESP	PSP	IDS/IPS	Training	System Status Monitoring	Malware Prevention	Authentication	Encryption	Physical Monitoring
Data Storage Device	64	54	26	8	23	19	22	0	5
Digital Protective Control Device	23	24	12	1	7	5	16	0	5
Electronic Access Control System	140	97	38	30	47	21	62	5	17
Electronic Access Monitoring System	110	105	18	54	38	42	64	2	21
Industrial Process Control System	253	178	42	28	103	42	77	0	32
Mainframe Computer	1	1	1	0	1	1	2	0	1
Network Data Communications Device	536	345	135	77	196	117	163	3	65
PC Laptop	52	34	14	10	28	15	19	1	6
Peripheral Device	194	105	40	27	64	14	28	0	8
Physical Access Control System	124	78	8	20	22	13	35	11	17
Physical Access Monitoring System	92	48	11	21	14	9	33	3	28
Physical Security Perimeter	3	5	0	2	2	2	3	2	18
Relay	60	53	13	1	20	12	36	3	12
RTU	108	83	22	0	35	18	25	1	17
Server	225	125	53	72	54	39	83	1	26
Telecommunications Device	96	81	17	1	31	14	20	1	3
Transmitters	6	7	1	0	0	0	0	0	0
Valve Controllers	1	1	0	0	1	0	0	0	0
Other	298	158	51	97	142	33	107	3	57