NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 12, 2017

VIA OVERNIGHT MAIL

Sheri Young, Secretary of the Board
National Energy Board
517 – 10th Avenue SW
Calgary, Alberta
T2R 0A8

Re: Remote Access Study Report

Dear Ms. Young:

On June 30, 2017, pursuant to Order No. 822 of the Federal Energy Regulatory Commission ("FERC"),[1] the North American Electric Reliability Corporation ("NERC") submitted to FERC a report providing the results of a study on the remote access protections required by NERC's Critical Infrastructure Protection ("CIP") Reliability Standards ("Remote Access Study Report"). Remote access refers to the ability to access a system, application, or data from a remote location. Remote access technology allows logging into a system as an authorized user without being physically present at its keyboard. NERC completed the Remote Access Study consistent with the FERC directive in Order No. 822 to perform a study to assess: (1) the effectiveness of the controls in the CIP Reliability Standards to mitigate known remote access vulnerabilities; (2) the risks posed by remote access-related threats and vulnerabilities; and (3) appropriate mitigating controls for any identified risks.[2]

NERC submitted to FERC a public and non-public version of the Remote Access Study Report. In the public version, NERC redacted sensitive data regarding Critical Electric Infrastructure. NERC requested that FERC designate the redacted portions of the Remote Access Study Report as Critical Energy/Electric Infrastructure Information ("CEII"), consistent with Section 388.113 of FERC's regulations.[3] The redacted portions of the Remote Access Study Report provide sensitive information on the manner in which entities subject to NERC's CIP Reliability Standards have implemented security controls to protect against the risks associated with remote access to cyber assets used to control and monitor bulk-power system facilities. Among other things, the redacted portions of the Remote Access Study Report describe the type of security controls used by entities to address remote access-related threats and vulnerabilities and assesses the

[1] *Order No. 822, Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,037, at P 64 (2016).

[2] *Id*.

[3] 18 C.F.R. § 388.113 (2016).

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

effectiveness of those controls, noting areas requiring further enhancement. As a result, the details provided in the redacted portions of Remote Access Study Report could be useful to a person planning an attack on Critical Electric infrastructure. NERC requested that FERC designate the redacted portions of the Remote Access Study Report as CEII for the full period allowed under FERC's regulations.[4]

Attached to this letter is the public version of the Remote Access Study. Should you wish to receive the non-public version of the Report, please contact the undersigned.

Respectfully submitted,

/s/ Shamai Elstein
Shamai Elstein
North American Electric Reliability Corporation
Counsel
1325 G Street, NW, Suite 600
Washington, D.C. 20005
202-400-3009
shamai.elstein@nerc.net

Counsel to the North American Electric Reliability Corporation

[4] 18 C.F.R. § 388.113(e)(1).

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Remote Access Study Report

June 30, 2017

RELIABILITY | ACCOUNTABILITY



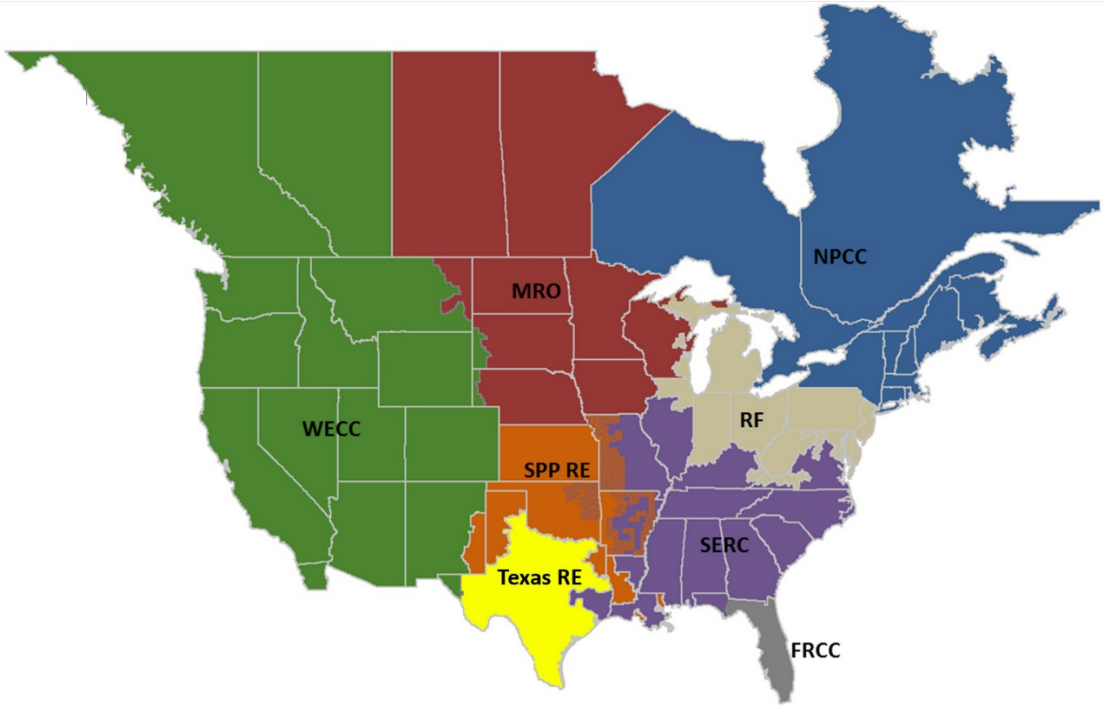

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system (BPS) in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the BPS through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the Electric Reliability Organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the BPS, which serves more than 334 million people.

The North American BPS is divided into eight Regional Entity (RE) boundaries as shown in the map and corresponding table below.



The North American BPS is divided into eight RE boundaries. The highlighted areas denote overlap as some load-serving entities participate in one Region while associated transmission owners/operators participate in another.

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP RE	Southwest Power Pool Regional Entity
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Executive Summary

This report provides the results of NERC's study on the remote access protections in NERC's Critical Infrastructure Protection (CIP) Reliability Standards (Remote Access Study or Study).[1] Remote access refers to the ability to access a system, application, or data from a remote location. Remote access technology allows logging into a system as an authorized user without being physically present at its keyboard. NERC completed the Remote Access Study consistent with the FERC's directive in Order No. 822 to perform a study to assess: (1) the effectiveness of the controls in the CIP Reliability Standards to mitigate known remote access vulnerabilities; (2) the risks posed by remote access-related threats and vulnerabilities; and (3) appropriate mitigating controls for any identified risks.[2]

In conducting the Remote Access Study, NERC found that the existing protections required by the CIP Reliability Standards and the manner in which registered entities have implemented those protections are largely effective in mitigating many of the risks associated with remote access. NERC observed that registered entities have implemented effective security controls in compliance with the remote access protections in the CIP Reliability Standards, with few exceptions identified during compliance monitoring activities, and, in many cases, implemented additional remote access controls beyond those required by the CIP Reliability Standards to further strengthen their security posture. NERC also identified certain areas that may require additional focus to ensure that risks related to remote access are effectively mitigated.

This report summarizes NERC's findings from the Remote Access Study. As discussed below, NERC identified 19 areas for continued focus. These areas are categorized in the following manner in this report:

- **Effective Mitigating Practices** – This category refers to security and operational practices implemented by registered entities that were particularly effective at mitigating risks and represent opportunities for outreach and information sharing to further their use throughout the industry.
- **Areas for Further Analysis** – This category refers to areas for additional research, potential standards modifications, or technical guidance to more accurately address remote access-related threats and vulnerabilities.
- **Enhancement Opportunities** – This category refers to areas where NERC and the Regional Entities, (collectively, the ERO Enterprise) can help facilitate the use of industry best practices within the confines of the CIP Reliability Standards.
- **Training and Awareness** – This category refers to those security controls, best practices, and other methods to demonstrate compliance that may not be well understood by registered entities and may require training, outreach, or guidance to improve industry awareness on controls that can be used to mitigate the risks associated with remote access.

This report is organized as follows:

- *Section 1* discusses the risks posed to the Bulk Electric System (BES) by remote access-related threats and vulnerabilities.

[1] Unless otherwise designated, all capitalized terms used herein shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards* (NERC Glossary), http://www.nerc.com/files/Glossary_of_Terms.pdf. For ease of reference, Appendix B hereto includes a glossary of terms used in this report.

[2] Order No. 822, *Revised Critical Infrastructure Protection Reliability Standards*, 154 FERC ¶ 61,037, at P 64 (2016) (approving Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, CIP-007-6, CIP-009-6, CIP-010-2 and CIP-011-2).

- *Section 2* explains the manner in which the currently-effective CIP Reliability Standards address those risks.
- *Section 3* provides the ERO Enterprise's observations on the manner in which registered entities have implemented controls to address the risks associated with remote access.
- *Section 4* examines the effectiveness of the CIP Reliability Standards and registered entities implementation of those standards in mitigating the risks posed by remote access, and describes areas that may require additional consideration to ensure that remote access risks are effectively mitigated.
- *Section 5* discusses next steps to address the areas identified for further consideration.

Section 1. Remote Access Related Threats and Vulnerabilities

Remote access refers to the ability to access a system, application, or data from a remote location. Remote access can take one of two forms: (1) human or user-initiated remote access, referred to as Interactive Remote Access in NERC's CIP Reliability Standards; or (2) automated system-to-system access. Registered entities frequently use Interactive Remote Access technologies to enable remote users to operate, support, and maintain control systems networks and other BES Cyber Systems. Among other things, providing for remote access enables users to efficiently access Cyber Assets to troubleshoot application software issues and repair data and modeling problems that cause application errors.

In addition, registered entities frequently use system-to-system (or machine-to-machine) remote access for, among other things, data exchange. For instance, Inter-Control Center Communications Protocol (ICCP) is the most common form of data-sharing communications between control centers and often relies on system-to-system remote access. Using a network connection, ICCP enables one energy management system (EMS) to exchange real-time operational data with another EMS at a remote electric power entity.

These remote access technologies, while important for efficiently operating, supporting, and maintaining Cyber Assets, including those for control systems, could open up attack vectors. If not properly secured, remote access could result in unauthorized access to a registered entity's network and control systems, with potentially serious consequences. An attacker, for instance, could breach an environment via remote access by deliberately compromising security controls to obtain privileged access to critical systems. Although registered entities generally do not rely on Internet facing systems to operate and monitor the BES, malicious actors have demonstrated capabilities to infiltrate systems that are not Internet facing, such as systems designed to run autonomously with minimal human interaction and other mission critical applications that are used to perform supervisory control that, if misused, could result in serious reliability issues. Additionally, a compromised device that is allowed to remotely access a Cyber Asset can serve as a gateway for cyber-criminals to attack networks.

Once the attacker gains remote access to the system, the attacker could then upload malware, copy sensitive data, compromise other computer systems, and even operate BES elements to undermine the reliability of the BES. As evidenced by the cyber-attacks on Ukrainian power companies in December 2015 that resulted in power outages impacting a large number of customers, unauthorized access could be used to operate transmission and generation assets in a malicious manner by a remote user.[3] Additionally, as evidenced by the December 2016 cyber-attack in Kiev, Ukraine which adversely affected electric grid operations, malware can be preconfigured to scan and evaluate networks to target susceptible systems and force them to misoperate or operate in a manner counter to their intended use.[4] Malware does not require a malicious actor or direct human intervention in order for it to compromise target systems, and in turn present real threats to the autonomous systems used in substations and generators where user intervention is not expected. Malicious actors and malware programs can also target BES Cyber Systems with denial of service attacks, which could render operational networks and systems inoperable or result in outages.

Cyber security threats continue to evolve. The electric industry's reliance on systems and technologies that are commonly available could enable adversaries to develop tools and mechanisms to compromise the most ubiquitous systems. Registered entities must therefore continue to implement and reinforce sound security

[3] *See* DHS, ICS-Cert, Cyber-Attack Against Ukrainian Critical Infrastrucutre (Feb. 25, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[4] *See* CRASHOVERRIDE, Analysis of the Threat to Electric Grid Operations, https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

measures within their organizations to mitigate the risks associated with remote access. Training, security policies, and documented processes help ensure that security is not compromised through the introduction of unsecured computers or unsecured access. Properly configuring software on devices used to remotely access BES Cyber Systems, and implementing securely designed network architectures are crucial for continued security of the BES Cyber Systems. Also essential are secure methods to authenticate users. As discussed in the following section, the CIP Reliability Standards require applicable registered entities to implement a number of fundamental security controls when permitting remote access to networks containing BES Cyber Systems.

Section 2. CIP Reliability Standards Addressing Remote Access

The currently-effective CIP Reliability Standards require registered entities to implement a number of security controls for remote access. Specifically, the CIP Reliability Standards include the following requirements for remote access protection:

- *CIP-003-6, Requirement R1*: Entities must have cyber security policies governing remote access to BES Cyber Systems. Senior management must approve these policies to help ensure that secure practices are implemented.
- *CIP-004-6, Requirement R1*: Responsible entities must implement a cybersecurity awareness program that, at least once a calendar quarter, reinforces cyber security practices, which may include practices related to remote access.
- *CIP-004-6, Requirement R2*: All personnel who have remote access capability must periodically receive training that reinforces cyber security practices.
- *CIP-004-6, Requirement R4, Part 4.1-4.3*: All personnel who have remote access must be explicitly authorized and periodically reviewed to ensure such access is limited and controlled.
- *CIP-004-6, Requirement R5, Parts 5.1 and 5.1*: To ensure that terminated or transferred personnel do not retain the ability to access BES Cyber Systems remotely, entities must revoke the access rights of terminated or transferred personnel.
- *CIP-005-5, Requirement R1, Part 1.1*: Entities must protect all BES Cyber Systems with routable connectivity by including them in an Electronic Security Perimeter (ESP) to control access. An ESP is defined as the logical border surrounding a network to which BES Cyber Systems are connected using routable protocol.
- *CIP-005-5, Requirement R1, Part 1.2*: All connections to BES Cyber Systems originating from outside the ESP must be through an identified access point (through a firewall) so that all connections are known and controlled.
- *CIP-005-5, Requirement R1, Part 1.3*: For all connections to BES Cyber Systems inside the ESP there must be a documented reason for such access, both inbound and outbound, and a denial to all other access.
- *CIP-005-5, Requirement R1, Part 1.4*: Remote access via dial-up connectivity must be authenticated.
- *CIP-005-5, Requirement R1, Part 1.5*: All inbound and outbound communications must be examined to detect malicious communication.
- *CIP-005-5, Requirement R2, Part 2.1*: Interactive Remote Access to BES Cyber Systems must go through an Intermediate System (limiting the entry points to the ESP and controlling the types of access allowed to BES Cyber Systems).
- *CIP-005-5, Requirement R2, Part 2.2*: Interactive Remote Access sessions must be encrypted to the Intermediate System to protect the confidentiality and integrity of the communications.
- *CIP-005-5, Requirement R2, Part 2.3*: Interactive Remote Access sessions must have multi-factor authentication to ensure only appropriate personnel have access.
- *CIP-007-6, Requirement R1, Part 1.1*: BES Cyber Systems are further protected from potential remote access attacks by limiting their network exposed ports and services to only those required for operation of the system.
- *CIP-007-6, Requirement R4*: In the event of unauthorized or suspicious remote access, entities must keep event logs and periodically review them for intervention or after-the-fact analysis.

- *CIP-007-6, Requirement R5, Part 5.1*: Remote access users of BES Cyber Systems must also authenticate their interactive use access session to the BES Cyber System.

The primary focus of the remote access protections in the CIP Reliability Standards is to address user-initiated remote access, referred to as Interactive Remote Access. Interactive Remote Access is defined in the NERC Glossary as:

> *User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.*

CIP Reliability Standard CIP-005-5, Requirements R1 and R2 provide the core controls for mitigating the risks associated with network connectivity and Interactive Remote Access. The following is a more in-depth discussion of those requirements and the manner in which they address remote access-related threats and vulnerabilities.

Pursuant to CIP-005-5, Requirement R1, registered entities must establish the following network connectivity protections:

- All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.
- All External Routable Connectivity[5] must be through an identified Electronic Access Point (EAP).
- Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.
- Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.
- Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.

The ESP-related requirements in CIP-005-5, Requirement R1 essentially create a "trust-zone" to segment BES Cyber Systems from non-trusted environments. The ESP serves to control traffic at the external electronic boundary of the BES Cyber System and provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks.

[5] External Routable Connectivity is defined in the NERC Glossary as "[t]he ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection."

Under CIP-005-5, Requirement R2, registered entities allowing Interactive Remote Access into an ESP must implement the following security controls to mitigate the risk from unauthorized users accessing high and medium impact BES Cyber Systems and their associated Protected Cyber Assets:

- Use an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.
- For all Interactive Remote Access sessions, use encryption that terminates at an Intermediate System.
- Require multi-factor authentication for all Interactive Remote Access sessions.

The term Intermediate System is defined in the NERC Glossary as:

> *A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.*

The use of an Intermediate System prohibits remote users from directly accessing Cyber Assets inside an ESP and potentially exposing these Cyber Assets to vulnerabilities that may exist on the remote user's device. A jump host, which is part of the Intermediate System, acts as a proxy to facilitate communications from the remote user to Cyber Assets within the ESP. Forcing all Interactive Remote Access through the jump host allows the registered entities to limit the permitted ESP firewall access control list rules to only those required to facilitate communications with the jump host. Additionally, external facing firewalls can also limit access control list rules to only those rules required to facilitate communications between the remote user and the jump host.

The use of encryption provides additional protections. Encryption is used to protect the confidentiality and integrity of data that is sent between the remote computer and the Intermediate System. Data encryption is important for anyone who wants or needs secure data transfer. Encryption is needed when there is a risk of unauthorized interception of transmissions on the communications link. It is especially important when using the Internet as the communication means.

The use of multi-factor authentication provides an added layer of security. Passwords can be guessed, stolen, hijacked, found, or given away. They are subject to automated attacks including brute force attacks, in which possible passwords are tried until the password is found, or dictionary attacks, where words and word combinations are tested as possible passwords. But if a password or PIN must be supplied along with a one-time password supplied by a token, a fingerprint, or some other factor, the password is of no value unless the other factors required for authentication are also acquired.

In conducting the Remote Access Study, NERC focused on the specific network connectivity and Interactive Remote Access protections in CIP-005-5, Requirements R1 and R2 as these requirements are the focal point of the remote access protections in the CIP Reliability Standards. As explained in the following section, NERC staff reviewed the manner in which entities implemented Reliability Standards CIP-005-5 and found that the required protections are helping to effectively mitigate many of the risks associated with Interactive Remote Access.

Section 3. Assessment of Remote Access Control Implementation

To help assess the effectiveness of the remote access controls required by the CIP Reliability Standards and determine if the appropriate mitigating controls are in place, NERC, working with the Regional Entities, reviewed the manner in which registered entities implementated remote access controls, including those required by the CIP Reliability Standards as well as any additional security controls. The ERO Enterprise used information gathered from over 30 completed audits of registered entities between July 1, 2016 and May 15, 2017. The 30 audits covered registered entities representing the following functional registrations: Balancing Authority (BA); Distribution Provider (DP); Generator Owner (GO); Generator Operator (GOP); Planning Coordinator (PC); Reliability Coordinator (RC); Resource Planner (RP); Transmission Owner (TO); Transmission Operator (TOP); Transmission Planner (TP); and Transmission Service Provider (TSP).

NERC examined the Regional Entities' assessment of each audited registered entity, along with supporting information such as work papers and related compliance evidence. The ERO Enterprise also developed a questionnaire for use during audits and spot checks, referred to as the "Remote Access Form", which can be found in Appendix A, to gather specific data on the implementation of remote access controls. Among other things, NERC reviewed registered entities' network and firewall device configurations, Interactive Remote Access procedures, network management procedures, Electronic Access Control or Monitoring Systems (EACMS) configuration files, and participant interview notes. NERC also reviewed audit reports and self-reports to identify areas of noncompliance related to remote access protections for trends and areas of focus to improve remote access control implementation.

Using this information, NERC assessed the relative strengths and weaknesses of registered entities' remote access and network access controls. As discussed in greater detail below, NERC found that the registered entities' remote access architectures are generally compliant with the CIP-005-5 requirements and the security controls are generally effective at mitigating vulnerabilities.

Observations of Remote Access Control Implementation

The following section provides NERC's observations of registered entities implementation of remote access controls based on the data gathered on each of the items included in the Remote Access Form.

Item 1 – Network Architecture

Item 1 of the Remote Access Form requested the following information to be evaluated by the Regional Auditor:

> *Review a sample of the registered entity's Electronic Security Perimeters (ESPs). Evaluate applicable access controls, intrusion detection capabilities, malware prevention capabilities, etc. Document for the study any notable strengths or weaknesses in these areas.*

The focal point of this item was to evaluate the architectural components associated with the registered entity's ESP infrastructure used to support remote access. In accordance with CIP-005-5, Requirement R1, Part 1.1, registered entities segmented their operational technology routable networks that contained their BES Cyber Systems from other networks, such as their corporate networks. Most of the registered entities from which NERC

collected data implemented multiple ESPs for their primary Control Centers, backup Control Centers, and substations, as applicable.[6]

[redacted]

Item 2 – Interactive Remote Access

Item 2 of the Remote Access Form requested the following information to be evaluated by the Regional Auditor:

> *Review and evaluate the entity's architecture for Interactive Remote Access. Document for the study any notable strengths or weaknesses in the entity's approach, including session encryption, identification and protection of Intermediate Systems, use and appropriateness of authentication services (Active Directory, Lightweight Directory Access Protocol (LDAP), RSA, etc.), strength of multi-factor user authentication, etc.*

The focal point of this item was to understand and evaluate the controls associated with the registered entity's remote access architecture.

Interactive Remote Access and Intermediate Systems Architecture

[redacted]

[6] None of the entities observed during the Remote Access Study had generation facilities with high or medium impact BES Cyber Systems subject to Reliability Standard CIP-005-5.

[redacted]

Intermediate Systems

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Remote User Systems

[redacted]

7 [redacted]

[redacted]

[redacted]

[redacted]

Item 3 – Additional Interactive Remote Access Protections

Item 3 of the Remote Access Form requested the following information to be evaluated by the Regional Auditor:

> *Review and evaluate the registered entity's architecture for Interactive Remote Access. Document for the study any notable strengths or weaknesses in the entity's approach, including session encryption, identification and protection of Intermediate Systems, use and appropriateness of authentication services (Active Directory, Lightweight Directory Access Protocol (LDAP), RSA, etc.), strength of multi-factor user authentication, etc. Evaluate the controls applicable to Interactive Remote Access. Document for the study any notable strengths or weaknesses in the entity's controls:*
>
> *a. Assess the monitoring of actions that may be taken by the remote user who has successfully authenticated to the Intermediate System, if any:*
>
> *i. Session logging,*
>
> *ii. Key stroke logging,*
>
> *iii. Screen captures,*
>
> *iv. Automated session terminations, and*
>
> *v. Audit logging of all actions taken.*
>
> *b. Assess controls for the required encryption that terminates at the Intermediate System:*
>
> *i. Encryption strength, and*
>
> *ii. Encryption key updates.*
>
> *c. Evaluate the mitigation of risks posed by corporate networks to Intermediate Systems:*
>
> *i. E.g., DMZs used to protect jump hosts and authentication services.*

Remote User Session Monitoring

[redacted]

[redacted]

Encryption

[redacted]

Demilitarized Zone (DMZ)

[redacted]

8 [redacted]

[redacted]

[redacted]

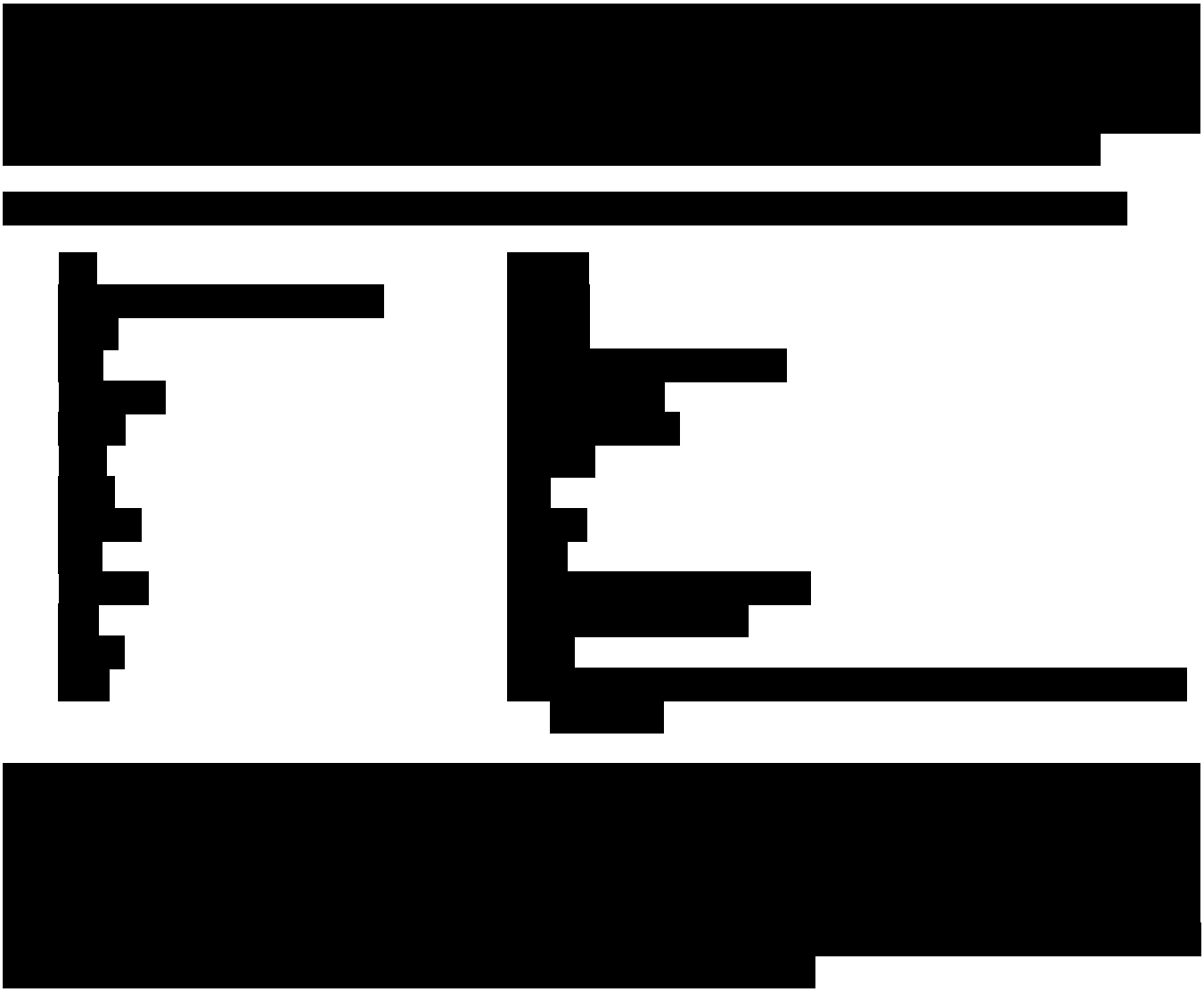
Item 4 – System-to-System Remote Access

Item 4 of the Remote Access Form requested the following information to be evaluated by the Regional Auditor:

> *Evaluate the protections provided for system-to-system communications crossing the ESP boundary. Document for the study the protocols used and any notable strengths or weaknesses in these protections. Systems-to-system communications may include:*
>
> *a. ICCP (Inter-Control Center Communications Protocol),*
>
> *b. Management console communications,*
>
> *c. DNP/IP (Distributed Network Protocol over Internet Protocol),*
>
> *d. Modbus/IP (Modbus over Internet Protocol),*
>
> *e. SQL*Net (Oracle client/server middleware),*
>
> *f. Replication,*
>
> *g. Failover, and/or Other protocols*

The focal point of this item was to evaluate the controls associated with system-to-system remote access. [redacted]

[redacted]



Item 5 – Lessons Learned from Cyber Incident in the Ukraine

Item 5 of the Remote Access Form requested the following information to be evaluated by the Regional Auditor:

Evaluate and document for the study the entity's controls to address the Ukraine's specific Remote Access Vulnerabilities:

- *Spear phishing and malware detection capabilities on Corporate Networks*
- *Application whitelisting*[9]
- *Disabling of macros at email servers and in Windows-based applications*
- *Application of Lessons Learned on Mixed-Trust EACMS to ensure that credentials from corporate enterprise cannot be exploited by escalation tactics*

[9] Application whitelisting is a cyber security control that requires applications to be predefined and permitted to execute on a Cyber Asset. Any application that does not have an explicit permission to execute will be prevented from executing. This differs from traditional cyber security controls where applications are permitted to execute unless an anti-malware software identifies an application as malware and prevents it from executing. If a malware manages to get onto a Cyber Asset with whitelisting protection, the malware could not execute since it does not have permission to do so.

- *Protection for IP to serial converters*
- *Other protections implemented*

The focal point of this item was to understand and evaluate the steps registered entities took to address vulnerabilities that led to the cyber incident in the Ukraine. A cyber-attack was perpetrated against electric utilities in the Ukraine in December 2015, resulting in power outages that affected at least 225,000 customers. The attackers initially compromised the business networks of the utilities and used credentials obtained on those networks to gain access to the industrial control system networks including the networks that housed SCADA systems. The attackers used credentials to access SCADA systems at multiple control centers and opened breakers at substations. The attackers also used their access to change the firmware on substation communications infrastructure, rendering the devices useless. More details of the cyber-attack may be found in the ICS-CERT report Cyber-Attack Against Ukrainian Critical Infrastructure.

To better understand the manner in which registered entities are addressing remote access risk, NERC requested information from registered entities on actions taken to prevent potential cyber hackers from gaining access to corporate networks and escalating privileges to gain access to Cyber Assets inside the ESP. The following are NERC's findings on this matter:

[redacted]

[redacted]

[redacted]

[redacted]

10 [redacted]

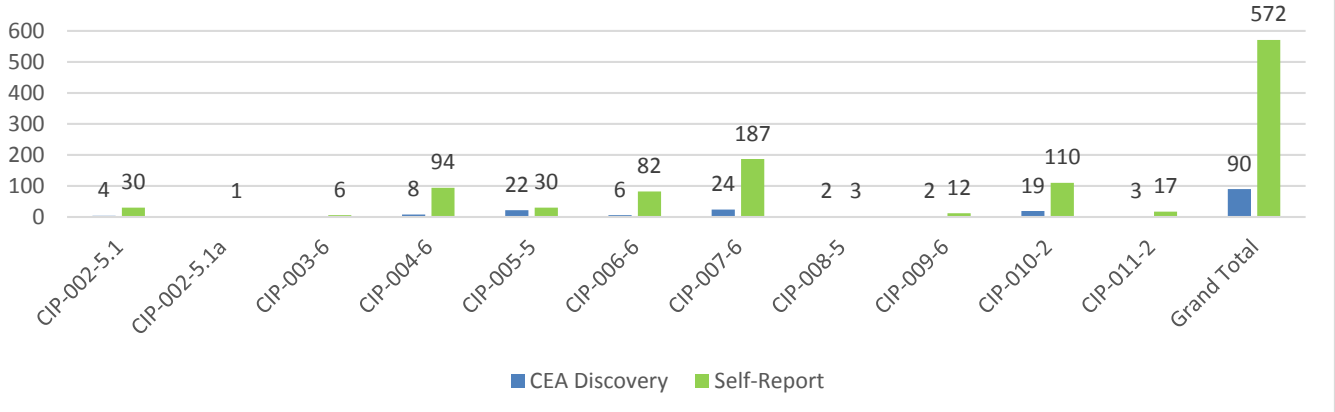
[redacted]

[redacted]

Compliance Monitoring Observations

As noted above, NERC also reviewed audit reports to identify areas of noncompliance related to remote access protections to identify trends and areas of focus to improve implementation of remote access controls. Table 1 below summarizes the number of instances of noncompliance of the CIP Reliability Standards the ERO Enterprise identified from July 1, 2016 through May 15, 2017. As shown in Table 1, there were 662 instances of noncompliance. Of the total number of noncompliance, however, only 52 or eight percent (22 instances of discovered by the ERO Enterprise and 30 instances of self-reports) of those instances were related to remote access or otherwise associated with CIP-005-5, which includes the primary requirements application to remote access.

Table 1
Total New CIP V5 Standards by Self-Report/CEA Discovery
Discovered- July 1, 2016 - May 15, 2017



[redacted]

Section 4. Effectiveness of Remote Access Protections

In conducting the Remote Access Study, NERC staff found that the existing protections required by the CIP Reliability Standards and the manner in which registered entities have implemented those protections are effective in mitigating many of the risks associated with remote access. The requirements outlined in Section 2 above – from the training requirements, to the electronic access requirements, and the core requirements in CIP-005-5 applicable to Interactive Remote Access – address many of the risks associated with remote access, establishing barriers to unauthorized access to BES Cyber Systems, and their associated Protected Cyber Assets. Similarly, as described in Section 3, NERC observed that, with a few exceptions, registered entities have implemented effective security controls in compliance with the remote access protections in the CIP Reliability Standards and, in many cases, implemented remote access controls beyond those required by the CIP Reliability Standards to further strengthen their security posture. NERC also identified certain areas that may require additional consideration to ensure that risks related to remote access are effectively mitigated.

This section summarizes NERC's findings from the Remote Access Study. As noted above, NERC identified 19 areas for continued focus. These areas are categorized in the following manner:

- **Effective Mitigating Practices** – This category refers to security and operational practices implemented by registered entities that were particularly effective at mitigating risks and represent opportunities for outreach and information sharing to further their use throughout the industry.
- **Areas for Further Analysis** – This category refers to areas for additional research, potential standards modifications, or technical guidance to more accurately address remote access-related threats and vulnerabilities.
- **Enhancement Opportunities** – This category refers to areas where the ERO Enterprise can help facilitate the use of industry best practices within the confines of the CIP Reliability Standards.
- **Training and Awareness** – This category refers to those security controls, best practices, and other methods to demonstrate compliance that may not be well understood by registered entities and may require training, outreach, or guidance to improve industry awareness on controls that can be used to mitigate the risks associated with remote access.

Effective Mitigating Practices

[redacted]

[redacted]

11 [redacted]

12 [redacted]

Areas for Further Analysis

[redacted]

Enhancement Opportunities

[13]

Training and Awareness

14

15

[redacted]

Section 5. Next Steps

As discussed in Section 4, NERC identified a number of areas for consideration to further enhance the security posture of the electric industry. NERC will use its various reliability tools, including training and outreach, the issuance of security guidelines, or modifications to the CIP Reliability Standards, as appropriate, to address the issues identified in this report and enhance remote access protections. Appendix C hereto provides NERC's action plan for addressing the issues identified in this report.

The ERO Enterprise will also continue to emphasize the evaluation of remote access controls during compliance monitoring engagements. As described in Section 3, there are opportunities to improve the consistent and effective implementation of the remote access protections required by the CIP Reliability Standards. NERC will continue reviewing audit reports and self-reports to identify trends indicating areas for future focus. NERC will continue to help ensure that registered entities apply the appropriate Interactive Remote Access controls as defined by the CIP Standards, providing periodic updates to industry on remote access compliance performance issues and opportunities, and additional focus on effective controls and the use of best practices for securing remote access connections.

The threat landscape is constantly changing and requires adaptation and information sharing on how best to address these issues in an effective and efficient manner. The results from this effort show very positive steps have been taken to address remote access protections. The ERO Enterprise will continue monitoring the implementation of remote access controls and work with industry and FERC to address the areas identified in this report as a further step toward our shared commitment of assuring the reliability and security of the North American bulk power system.

Appendix A: Remote Access Form

The ERO Enterprise gathered specific information about registered entities implementation of remote access controls through the use of the Remote Access Form. The form directed Regional Entity auditors to obtain the following information:

- **Item 1** – Review a sample of the registered entity's ESPs. Evaluate applicable access controls, intrusion detection capabilities, malware prevention capabilities, etc. Document any notable strengths or weaknesses in these areas.
  - *Applicable CIP Reliability Standards: CIP-005-5, Requirement R1, Parts 1.1, 1.2, 1.3, 1.4, and 1.5*
- **Item 2** – Review and evaluate the registered entity's architecture for Interactive Remote Access. Document any notable strengths or weaknesses in the entity's approach, including session encryption, identification and protection of Intermediate Systems, use and appropriateness of authentication services (Active Directory, Lightweight Directory Access Protocol (LDAP), RSA, etc.), strength of multi-factor user authentication, etc.
  - *Applicable CIP Reliability Standards: CIP-005-5, Requirement R2, Parts 2.1, 2.2, 2.3*
- **Item 3** – Evaluate the controls applicable to Interactive Remote Access. Document any notable strengths or weaknesses in the registered entity's controls:
  - Assess the monitoring of actions that may be taken by the remote user who has successfully authenticated to the Intermediate System, if any:
    - Session logging,
    - Key stroke logging,
    - Screen captures,
    - Automated session terminations, and/or
    - Audit logging of all actions taken.
  - Assess controls for the required encryption that terminates at the Intermediate System:
    - Encryption strength, and
    - Encryption key updates.
  - Evaluate the mitigation of risks posed by corporate networks to Intermediate Systems:
    - E.g., DMZs used to protect jump hosts and authentication services.
    - Evaluate the mitigation of risks posed by multi-use systems (corporate AD servers, RSA services also use for Internet-based access to corporate networks, etc.) when used by Intermediate Systems.
      - *Applicable CIP Reliability Standards: CIP-005-5, Requirement R1, Part 1.5*
- **Item 4** – Evaluate the protections provided for system-to-system communications crossing the ESP boundary. Document for the study the protocols used and any notable strengths or weaknesses in these protections. Systems-to-system communications may include:
  - ICCP
  - Management console communications
  - DNP/IP (Distributed Network Protocol over Internet Protocol)
  - Modbus/IP

- SQL*Net (Oracle client/server middleware)
- Replication
- Failover, and/or
- Other protocols
- *Applicable CIP Reliability Standards: CIP-005-5, Requirement R1, Part 1.3*

- **Item 5** – Evaluate and document the registered entity's controls to address specific remote access vulnerabilities related to the cyber-attack against Ukrainian critical infrastructure:
  - Spear phishing and malware detection capabilities on Corporate Networks
  - Application whitelisting
  - Disabling of macros at email servers and in Windows-based applications
  - Application of Lessons Learned on mixed-trust EACMS to ensure that credentials from corporate enterprise cannot be exploited by escalation tactics
  - Protection for IP to serial converters, if any, and/or
  - Other protections implemented

Appendix B: Definitions

Glossary Term	Glossary Definition
BES Cyber Asset	A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems.
BES Cyber System	One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity.
Control Center	One or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in realtime to perform the reliability tasks, including their associated data centers, of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generator Operator for generation Facilities at two or more locations.
Cyber Assets	Programmable electronic devices, including the hardware, software, and data in those devices.
Dial-up Connectivity	A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.
Electronic Access Control or Monitoring Systems	Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.
Electronic Access Point	A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
Electronic Security Perimeter	The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.
External Routable Connectivity	The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection.
Interactive Remote Access	User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of the Responsible Entity's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1. Cyber Assets used or owned by the Responsible Entity 2. Cyber Assets used or owned by employees, and 3. Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

Glossary Term	Glossary Definition
Intermediate System	A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.
Protected Cyber Assets	One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter. The impact rating of Protected Cyber Assets is equal to the highest rated BES Cyber System in the same ESP.

Appendix C: NERC Outreach and Coordination Activities

No.	Topic	Target Date	NERC Outreach & Coordination Activities
1	[redacted]	Q4 2018	NERC Webinar, Critical Infrastucture Protection Committee (CIPC) coordination,[16] ERO Training
2	[redacted]	Q4 2018	NERC Webinar, CIPC coordination, ERO Training
3	[redacted]	Q2 2018	NERC Webinar, CIPC coordination
4	[redacted]	Q4 2017	NERC Webinar, CIPC coordination
5	[redacted]	Q4 2018	NERC Webinar, CIPC coordination
6	[redacted]	Q4 2017	NERC Webinar, CIPC coordination, ISAC Advisory
7	[redacted]	Q4 2017	CMEP Area of Focus, NERC Webinar, CIPC coordination
8	[redacted]	Q2 2018	NERC Webinar, Present issue to CIP standard drafting team (SDT), CIPC coordination
9	[redacted]	Q4 2018	NERC Webinar, CIPC coordination, ERO Training, ISAC Advisory
10	[redacted]	Q4 2017	NERC Webinar, Present issue to CIP SDT, CIPC coordination
11	[redacted]	Q4 2017	NERC Webinar Present issue to CIP SDT, CIPC coordination
12	[redacted]	Q2 2018	NERC Webinar, Present issue to CIP SDT, CIPC coordination
13	[redacted]	Q2 2018	NERC Webinar, CIPC coordination, ISAC Advisory
14	[redacted]	Q4 2018	NERC Webinar, Present issue to CIP SDT, CIPC coordination
15	[redacted]	Q2 2018	NERC Webinar, CIPC coordination
16	[redacted]	Q4 2017	NERC Webinar, Present issue to CIP SDT, CIPC coordination

[16] The CIPC consists of cyber and physical security subject matters experts and helps NERC advance the physical security and cybersecurity of the critical electricity infrastructure of North America by, among other things, working closely with NERC operating and planning committees to identify needs for new or revised CIP standards and developing security guidelines to enhance industry protctions. NERC will consult with CIPC subject matter experts to help address the issues identified in the Remote Access Study.

No.	Topic	Target Date	NERC Outreach & Coordination Activities
17	[redacted]	Q4 2018	NERC Webinar, CIPC coordination
18	[redacted]	Q2 2018	NERC Webinar, Present issue to CIP SDT, CIPC coordination
19	[redacted]	Q2 2018	NERC Webinar, CMEP Area of Focus

Appendix D: CIP Reliability Standards That Impact EACMS

CIP Reliability Standards Requirements and Parts	
CIP-003-6, Requirement R1	CIP-007-6, Requirement R4, Part 4.1
CIP-004-6, Requirement R2, Part 2.1	CIP-007-6, Requirement R4, Part 4.2
CIP-004-6, Requirement R2, Part 2.2	CIP-007-6, Requirement R4, Part 4.3
CIP-004-6, Requirement R2, Part 2.3	CIP-007-6, Requirement R4, Part 4.4
CIP-004-6, Requirement R3, Part 3.1	CIP-007-6, Requirement R5, Part 5.1
CIP-004-6, Requirement R3, Part 3.2	CIP-007-6, Requirement R5, Part 5.2
CIP-004-6, Requirement R3, Part 3.3	CIP-007-6, Requirement R5, Part 5.3
CIP-004-6, Requirement R3, Part 3.4	CIP-007-6, Requirement R5, Part 5.4
CIP-004-6, Requirement R3, Part 3.5	CIP-007-6, Requirement R5, Part 5.5
CIP-004-6, Requirement R4, Part 4.1	CIP-007-6, Requirement R5, Part 5.6
CIP-004-6, Requirement R4, Part 4.2	CIP-007-6, Requirement R5, Part 5.7
CIP-004-6, Requirement R4, Part 4.3	CIP-009-6, Requirement R1, Part 1.1
CIP-004-6, Requirement R4, Part 4.4	CIP-009-6, Requirement R1, Part 1.2
CIP-004-6, Requirement R5, Part 5.1	CIP-009-6, Requirement R1, Part 1.3
CIP-004-6, Requirement R5, Part 5.2	CIP-009-6, Requirement R1, Part 1.4
CIP-004-6, Requirement R5, Part 5.3	CIP-009-6, Requirement R1, Part 1.5
CIP-004-6, Requirement R5, Part 5.4	CIP-009-6, Requirement R2, Part 2.1
CIP-004-6, Requirement R5, Part 5.5	CIP-009-6, Requirement R2, Part 2.2
CIP-005-5, Requirement R1, Part 1.5	CIP-009-6, Requirement R3, Part 3.1
CIP-006-6, Requirement R1, Part 1.2	CIP-009-6, Requirement R3, Part 3.2
CIP-006-6, Requirement R1, Part 1.3	CIP-010-2, Requirement R1, Part 1.1
CIP-006-6, Requirement R1, Part 1.4	CIP-010-2, Requirement R1, Part 1.2
CIP-006-6, Requirement R1, Part 1.5	CIP-010-2, Requirement R1, Part 1.3
CIP-006-6, Requirement R1, Part 1.8	CIP-010-2, Requirement R1, Part 1.4
CIP-006-6, Requirement R1, Part 1.9	CIP-010-2, Requirement R2, Part 2.1
CIP-007-6, Requirement R1, Part 1.1	CIP-010-2, Requirement R3, Part 3.1

CIP Reliability Standards Requirements and Parts	
CIP-007-6, Requirement R2, Part 2.1	CIP-010-2, Requirement R3, Part 3.3
CIP-007-6, Requirement R2, Part 2.2	CIP-010-2, Requirement R3, Part 3.4
CIP-007-6, Requirement R2, Part 2.3	CIP-011-2, Requirement R1, Part 1.1
CIP-007-6, Requirement R2, Part 2.4	CIP-011-2, Requirement R1, Part 1.2
CIP-007-6, Requirement R3, Part 3.1	CIP-011-2, Requirement R2, Part 2.1
CIP-007-6, Requirement R3, Part 3.2	CIP-011-2, Requirement R2, Part 2.2
CIP-007-6, Requirement R3, Part 3.3	