NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 30, 2021

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, D.C. 20426

Re: CIP-003-8 Electronic Access Controls Study
Docket No. RM17-11-000

Dear Secretary Bose:

The North American Electric Reliability Corporation ("NERC") hereby submits the report titled *CIP-003-8 Electronic Access Controls Study*. NERC submits this report to the Federal Energy Regulatory Commission (the "Commission") in accordance with the Commission's directive in paragraph 30 of Order No. 843.[1]

In Order No. 843, the Commission approved Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls.[2] The Commission also directed NERC to:

(1) develop modifications to CIP-003-7 to address mitigation of the risk of malicious code posed by third-party transient devices;[3] and

(2) conduct a study of the implementation of electronic access controls at assets containing low impact BES Cyber Systems, concluding in a report filed at the Commission within 18 months of the effective date of CIP-003-7.[4]

[1] *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, Order No. 843, 163 FERC ¶ 61,032 (2018).

[2] *Id.* at P 17.

[3] *Id.* at P 37.

[4] *Id.* at P 30.

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

For the first directive, NERC developed Reliability Standard CIP-003-8, which the Commission approved on July 31, 2019.[5] For the second directive, NERC and the Regional Entities,[6] collectively the Electric Reliability Organization ("ERO") Enterprise, conducted a study of approximately 200 registered entities with assets containing low impact BES Cyber Systems regarding: (1) what electronic access controls entities chose to implement and under what circumstances at these assets; (2) whether the electronic access controls adopted by entities provide adequate security; and (3) other relevant information found by the ERO Enterprise as a result of the study.

The enclosed report provides the results of the study of electronic access controls at assets containing low impact BES Cyber Systems. As more fully described therein, the ERO Enterprise found registered entities' electronic access controls applied to assets containing low impact BES Cyber Systems were generally effective in providing adequate security.

NERC respectfully requests that the Commission accept the attached report submitted in accordance with the Commission's directive in Order No. 843.

Respectfully submitted,

/s/ Marisa Hecht
Lauren Perotti
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, D.C. 20005
202-400-3000
lauren.perotti@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Enclosure:

CIP-003-8 Electronic Access Controls Study (June 2021)

[5] Federal Energy Regulatory Commission, Letter Order, *Approval of Reliability Standard CIP-003-8 (Cyber Security – Security Management Controls)*, Docket No. RD19-5-000 (July 31, 2019). On April 1, 2020, CIP-003-8 became effective; however, there were no changes to Section 3 regarding electronic access controls from CIP-003-7 Requirement R2 Attachment 1.

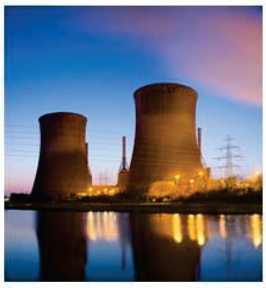
[6] The six Regional Entities include the following: Midwest Reliability Organization, Northeast Power Coordinating Council, Inc., ReliabilityFirst Corporation, SERC Reliability Corporation, Texas Reliability Entity, Inc., and Western Electricity Coordinating Council.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-003-8 Electronic Access Controls Study

June 30, 2021

RELIABILITY | RESILIENCE | SECURITY

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

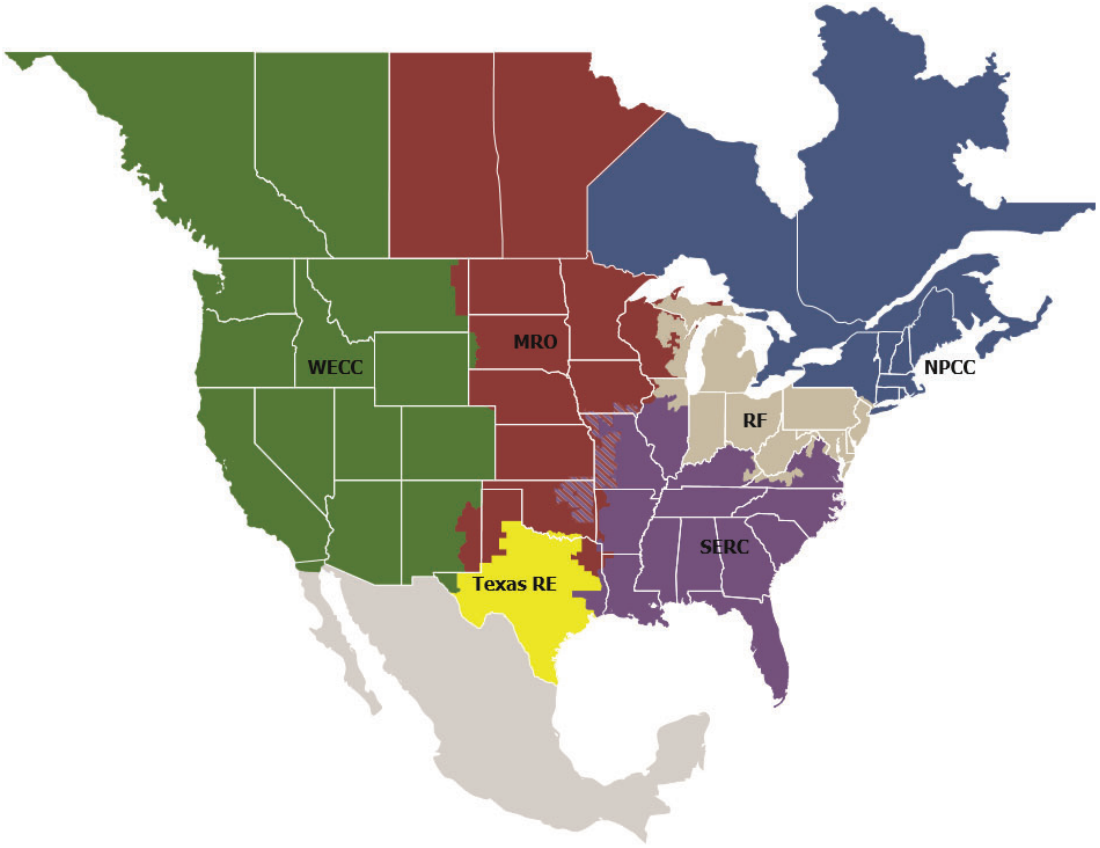
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities, is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entity boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners /Transmission Operators participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

This report provides the results of the ERO Enterprise's study to assess industry's implementation of electronic access controls required by Reliability Standard CIP-003-8 (Electronic Access Controls Study or Study).[1] The ERO Enterprise completed the Study consistent with FERC's directive in Order No. 843 to perform a study to assess: (1) what electronic access controls entities chose to implement and under what circumstances; (2) whether the electronic access controls adopted by responsible entities provide adequate security; and (3) as well as other relevant information found by NERC as a result of the study.[2]

In conducting the Study, the ERO Enterprise found registered entities' electronic access controls applied to assets containing low impact Bulk Electric System (BES) Cyber Systems were generally effective in providing adequate security. In addition, the ERO Enterprise found registered entities reported various facts or conditions surrounding the deployment of electronic access controls to assets containing BES Cyber Systems. These facts or conditions equated to defense in depth measures or controls implemented by registered entities. The ERO Enterprise also identified opportunities to strengthen registered entities' implementation of electronic access controls.

This report is organized as follows:

- *Section 1* discusses electronic access controls chosen by registered entities and the circumstances associated with implementation.
- *Section 2* examines the level of security of the electronic access controls chosen by the registered entities.
- *Section 3* identifies other relevant information related to the compliance or security posture of the low impact BES Cyber Systems observed during the Study.
- *Section 4* provides a conclusion.

[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.

[2] Order No. 843, *Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, 163 FERC ¶ 61,032, at P 30 (2018) (approving Reliability Standard CIP-003-7).

Background

Reliability Standard CIP-003-7 became effective on January 1, 2020, and required registered entities to implement physical security controls (CIP-003-7 Requirement R2 Attachment 1 Section 2) and electronic access controls (CIP-003-7 Requirement R2 Attachment 1 Section 3) for assets containing low impact BES Cyber Systems. On April 1, 2020, CIP-003-8 became effective; however, there were no changes to CIP-003-7 Requirement R2 Attachment 1 Sections 2 and 3.

Reliability Standard CIP-003-8 Requirement R2 Attachment 1 Section 3 requires registered entities to implement electronic access controls. Specifically, for each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the responsible entity shall implement electronic access controls to:

- Permit only necessary inbound and outbound electronic access as determined by the responsible entity for any communications that are:
  - between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s);
  - using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and
  - not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).
- Authenticate all Dial-up Connectivity, if any, that provides access to low impact BES Cyber System(s), per Cyber Asset capability.

Section 1: Assessment of Electronic Access Controls

To help assess the implementation of electronic access controls at assets containing low impact BES Cyber Systems, NERC relied on the expertise of the Regional Entities' Compliance Monitoring and Enforcement Program (CMEP) staff. Regional Entities collected data for the Study using the electronic access controls implementation form (see Appendix A) during CMEP activities such as compliance audits and self-certifications. The ERO Enterprise gathered data from approximately 200 registered entities between January 1, 2020 and March 1, 2021. Approximately 24 registered entities surveyed did not have applicable communications to assets containing low impact BES Cyber Systems or did not have assets containing low impact BES Cyber Systems. Therefore, these registered entities were not included in the Study.

The ERO Enterprise examined responses to the electronics access controls implementation form and reviewed various artifacts such as network diagrams, firewall/router configurations, and electronic access controls plans. In addition, the ERO Enterprise conducted interviews with registered entities as necessary. Due to COVID-19 pandemic travel restrictions, there were no onsite verifications conducted for the Study.

Electronic Access Controls Implementation Observations

The following section provides the ERO Enterprise's observation of registered entities' implementation of electronic access controls based on the data gathered.

Firewalls

While registered entities use various methods of electronic access controls, a majority of registered entities use firewalls to meet the CIP-003-8 electronic access controls requirement. Approximately 89 percent of studied registered entities reported using firewalls as the primary electronic access control to assets containing low impact BES Cyber Systems. Firewalls filter or prevent specific types of communications from moving between two different network zones (e.g., untrusted network and trusted network). One common approach of registered entities using firewalls includes the use of an access control list (ACL) coupled with deny by default strategy.

Routers

Another form of electronic access control reported was the use of routers with ACLs as opposed to firewalls. Routers can function in a manner similar to firewalls by filtering communication between trusted and untrusted networks. Approximately four percent of studied registered entities relied on routers to provide electronic access control to assets containing low impact BES Cyber Systems.

Uni-directional Gateways

Another form of electronic access control reported by approximately one percent of registered entities was the use of uni-directional gateways. Uni-directional gateways incorporate a one-way communication path and do not allow communication using a routable protocol entering the asset containing low impact BES Cyber Systems. The uni-directional gateway is implemented to permit only the necessary outbound communications using the routable protocol communication leaving the asset containing low impact BES Cyber Systems.

Physical Isolation

Approximately five percent of studied registered entities used physical isolation of the low impact BES Cyber System(s) from the routable protocol communication entering or leaving the asset containing the low impact BES Cyber System(s), commonly referred to as an air gap.

Dial-up Connectivity

Approximately one percent of studied registered entities allow Dial-up Connectivity to assets containing low impact BES Cyber Systems. Registered entities that communicated using Dial-up Connectivity implemented authentication

controls to access low impact BES Cyber Systems. For example, one registered entity requires dial back to a pre-defined phone number for the device performing Dial-up Connectivity. In addition, the device performing Dial-up Connectivity is enabled only as needed and disconnected when not in use.

Figure 1 below displays the observed electronic access controls.

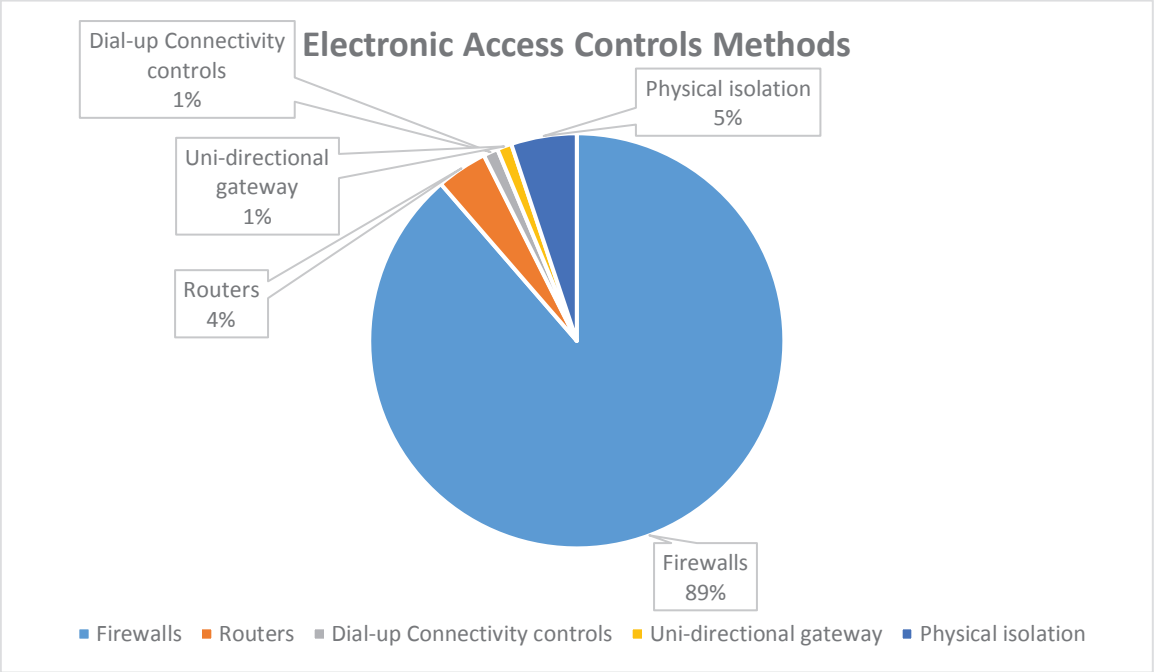


Figure 1: Observed Electronic Access Controls

Facts or Conditions of Electronic Access Controls Deployment

As noted earlier, in Order No. 843 FERC directed NERC to perform a study to assess what electronic access controls entities chose to implement and under what circumstances. The ERO Enterprise inquired about the circumstances (i.e., facts or conditions) associated with each responsible entity's implementation of electronic access controls to assets containing low impact BES Cyber Systems. Registered entities reported various facts or conditions associated with electronic access controls implementation for assets containing low impact BES Cyber Systems. The facts or conditions reported equated to defense in depth measures or controls implemented by registered entities. In some cases, these controls are equivalent to controls found in CIP Standards associated with high and medium impact BES Cyber Systems (e.g., CIP-005-6, CIP-007-6, and CIP-010-3). These facts or conditions include network architecture, physical conditions, training and awareness, vendor access, provisioning access, monitoring, and other controls.

Network Architecture

The majority of the registered entities implemented some form of network segmentation (logical and/or physical) for electronic access controls. As noted earlier, registered entities primarily used network firewalls to segment the low impact BES Cyber Systems from external networks. In addition, many registered entities implemented a defense in depth model to add extra layers of protection to the assets containing low impact BES Cyber Systems. Defense in depth measures observed included some of the following items: demilitarized zones, jump hosts, multi-factor authentication, and virtual private networks.

In some cases, registered entities implemented demilitarized zone architectures to add further protection from untrusted outside networks. In addition, to further protect low impact BES Cyber Systems, some entities utilized jump host technology. The jump host acts as a proxy to facilitate communications from the remote user to the low impact BES Cyber Systems. Some registered entities implemented multi-factor authentication to further protect access to low impact BES Cyber Systems. Common authentication factors observed by the ERO Enterprise included passwords, PINs, and tokens. Finally, many entities required the use of a virtual private network to communicate with low impact BES Cyber Systems. The use of virtual private networks enhanced the confidentiality and integrity of communications between a low impact BES Cyber System and a Cyber Asset outside the asset containing low impact BES Cyber Systems by utilizing encryption, authentication, and encapsulation technologies.

Physical Controls

Registered entities reported various physical controls associated with the implementation of electronic access controls to assets containing low impact BES Cyber Systems. However, the physical controls observed primarily aligned with the physical security controls required in CIP-003-8 Requirement R2 Attachment 1 Section 2. Some of the physical controls noticed during the Study are as follows:

- Badge/card readers
- Monitoring and alarming
- Secured doors
- Visitor control programs
- Keyed doors
- Fences with locking gates
- Key management program
- Video surveillance
- Physical port management on devices providing electronic access controls

Training
Many registered entities required training as a control associated with the implementation of electronic access controls to assets containing low impact BES Cyber Systems. In addition, several registered entities reported the incorporation of awareness materials as a requirement for gaining access to low impact BES Cyber Systems. Some examples of training observed are the following:

- Employees are trained for initial access with an annual retraining requirement frequency
- Awareness materials are sent out on a monthly basis
- Training must be completed prior to gaining access
- Awareness topics are discussed during monthly meeting
- Training covered certain items such as proper Cyber Asset usage and social engineering.

Vendor Access
Registered entities continue to rely on vendor access to BES Cyber Systems to ensure reliable operations. In many cases, the use of vendor products and/or services often requires vendors to access registered entities' environments remotely. In some instances, the registered entities' environment also contains third-party software. With the increasing compromise of third-party vendor products and potential vendor remote access to those products, it is essential to mitigate cyber security risk associated with supply chain. As a result, proper implementation of electronic access controls such as firewalls is essential.

In the ERO Enterprise's review of electronic access controls, commonly used remote access protocols were configured in network firewall ACLs specifically for vendor remote access. However, it was also noted some registered entities did not allow vendor remote access while some registered entities limited vendor access to only on site. Registered entities implemented various controls that allowed vendors remote access to low impact BES Cyber Systems. Below are some controls noted for vendor remote access to low impact BES Cyber Systems:

- Vendor remote access sessions could be disconnected at any time
- Vendor remote access was monitored by registered entity personnel
- Vendors had to contact registered entity before gaining access
- Vendor remote access was controlled with a manual on/off switch
- Vendor remote access sessions were monitored verbally

Provisioning Access
As a condition to gaining access to low impact BES Cyber Systems, entities implemented various provisioning methods. Most registered entities implemented the principle of least privilege when providing access to low impact BES Cyber Systems. Some entities utilized a ticketing system to track authorized access to low impact BES Cyber Systems. In addition, some registered entities granted access to low impact BES Cyber Systems based on roles (role-based access). Finally, some registered entities required completed background checks prior to accessing low impact BES Cyber Systems.

Monitoring
Registered entities implemented various monitoring controls as a condition of electronic access controls to assets containing low impact BES Cyber Systems. Monitoring consisted of items such as the use of a security operations center, log reviews, and configuration change management. For entities that implemented an intrusion prevention system, some reported the use of a security operations center to monitor for malicious or abnormal activity. Other entities implemented reviews such as vulnerability assessments and documentation reviews to monitor the effectiveness of the electronic access controls to assets containing low impact BES Cyber Systems. Some entities utilize change management processes in managing electronic access controls to assets containing low impact BES

Cyber Systems. These change management processes include monitoring the electronic access controls for configuration changes.

Other Controls

Other controls noted during the Study implemented by registered entities included the following:

- Web filtering
- Patching
- High availability firewall configurations
- Gap analysis/vulnerability assessment
- Firewall configuration reviews
- USB port locked or disabled
- DVD/CD Rom drive locked or disabled
- Baseline configuration monitoring
- Whitelisting
- Tamper tape
- Ethernet port locks
- Password management software
- Anti-virus software
- Encryption
- Access log reviews
- Identity access management system
- Penetration tests

Section 2: Security of Electronic Access Controls

Overall, the electronic access controls observed generally provided adequate security to assets containing low impact BES Cyber Systems. As noted earlier, firewalls, routers, uni-directional gateways, and air gapping were among the primary methods of electronic access controls implemented by entities with assets containing low impact BES Cyber Systems. Regional Entities noted that registered entities implemented robust processes for maintaining electronic access controls including ACL management. In many cases, communication through firewalls was limited to specific IP addresses, protocols, and services. Some registered entities incorporated protections equal to high impact BES Cyber Systems and medium impact BES Cyber Systems for their low impact BES Cyber Systems. Some examples noted are the implementation of intrusion prevention systems, security patching programs, and password management programs for low impact BES Cyber Systems.

In some cases, however, ERO Enterprise staff identified opportunities for improvement such as improved controls for vendor remote access. For example, some registered entities allowed vendor remote access continuously without monitoring electronic access logs or implementing other technical controls. Some registered entities only used non-technical controls, such as non-disclosure agreements, for vendor remote access. In other instances, registered entities allowed communications to low impact BES Cyber Systems using vulnerable protocols such as telnet and file transfer protocol. These protocols are commonly used in industrial control system environments for Cyber Assets such as relays, communication processors, and remote terminal units and may be necessary to communicate with vendors. In another case, a registered entity implemented overly permissive access permission on firewalls performing electronic access controls to assets containing low impact BES Cyber Systems.

The ERO Enterprise also observed a registered entity that incorporated adequate electronic access control perimeter defenses as required by Reliability Standard CIP-003-8; however, the registered entity deployed an anti-virus solution that provided broad access to files and elevated privileges on the Cyber Assets on which the software is installed, which could be exploited by malicious cyber actors to compromise those information systems. In addition, the registered entity used end of life operating systems on applicable Cyber Assets. As a result, the ERO Enterprise determined the registered entity did not provide adequate security.

In all cases, the implementation of registered entities' electronic access controls were assessed against the Reliability Standard CIP-003-8 security objective for appropriate determinations.

Section 3: Additional Observations

As noted earlier, in Order No. 843 FERC directed NERC to perform a study to assess: (1) what electronic access controls entities chose to implement and under what circumstances; (2) whether the electronic access controls adopted by responsible entities provide adequate security; and (3) as well as other relevant information found by NERC as a result of the study. The following section discusses other relevant information related to the compliance or security posture of the low impact BES Cyber Systems observed during the Study. These additional observations may not directly relate to electronic access controls required in Reliability Standard CIP-003-8, however highlight items of interest related to the registered entities' compliance or security posture. The additional observations are listed below.

- A registered entity indicated they do not implement additional controls beyond those required in Reliability Standard CIP-003-8 due to staff limitations.
- For registered entities allowing continuous vendor remote access, projects are ongoing to implement more restrictive firewall rules and controls to limit remote connections.
- A registered entity used manual keys to control physical access to low impact BES Cyber Systems and the Cyber Asset providing electronic access control to the asset containing low impact BES Cyber Systems. As a result, the Regional Entity recommended implementing a card access solution.
- Some registered entities are running end of life operating systems on low impact BES Cyber Systems. These end of life operating systems are not supported by vendors, and increase registered entities' attack surfaces.
- A Regional Entity discovered a low impact BES Cyber System spanned multiple physical locations. In this instance, the registered entity has different teams that handle physical controls; however, the electronic access controls did not limit the logical access between the physical locations.
- A Regional Entity identified concerns specific to wireless access utilization in regard to Transient Cyber Assets and Removable Media.
- A Regional Entity found some registered entities used outdated network diagrams to represent the low impact BES Cyber System environment. The outdated network diagrams reflected initial deployments of low impact BES Cyber Systems and were not updated when changes to the environment occurred.
- A Regional Entity discovered a registered entity allowed communications using a routable protocol; however the registered entity converted the routable communications to serial communications prior to reaching the asset containing low impact BES Cyber Systems. As a result, the registered entity excluded the asset containing low impact BES Cyber System(s) from the applicability of Reliability Standard CIP-003-8.
- A Regional Entity noted there are no clear guidelines for shared access to low impact BES Cyber Systems.
- Regional Entities noted there are no patching requirements for low impact BES Cyber Systems or Cyber Assets used for electronic access controls to assets containing low impact BES Cyber Systems. In some cases, registered entities are utilizing legacy Cyber Assets that are no longer supported due to product end of life, and the registered entity is not patching the equipment.
- A Regional Entity noted that Reliability Standard CIP-003-8 Requirement R2 Attachment 1 Section 3 does not explicitly mention achieving a security objective to control electronic access whereas Reliability Standard CIP-003-8 Requirement R2 Attachment 1 Section 5 includes language requiring registered entities "to achieve the objective of mitigating the risk."
- Regional Entities noted that creating a new CIP Reliability Standard specific to low impact BES Cyber System requirements may accommodate for the depth of controls currently required and future growth. In addition, further separation of the protections into specific Requirements may facilitate more effective monitoring and reporting of where deficiencies exist in registered entities' implementations of low impact protections.

- A Regional Entity noted the language used to scope CIP-003, “Each asset containing low impact BES Cyber Systems,” is a physical boundary that may be problematic when implementing logical controls specific to a physical boundary and identifying the electronic boundary to ensure the security objective(s) are met.

Section 4: Conclusion

The ERO Enterprise has concluded that, generally, the electronic access controls chosen by the studied registered entities generally provided adequate security under Reliability Standard CIP-003-8. However, the ERO Enterprise identified some opportunities for improvement among the studied registered entities where additional or improved controls would enhance their security posture, such as improved controls for vendor remote access. In conducting the Study, the ERO Enterprise noted the majority of the studied registered entities implemented firewalls with ACLs as the primary electronic access control method to assets containing low impact BES Cyber Systems. As noted earlier, firewalls filter or prevent communications between untrusted networks and trusted networks. The ERO Enterprise also identified additional observations related to the compliance or security posture of the low impact BES Cyber Systems observed during the Study, such as registered entities' use of legacy Cyber Assets.

The ERO Enterprise will continue to evaluate electronic access controls to assets containing low impact BES Cyber Systems for effectiveness. In addition, the ERO Enterprise will continue to perform outreach activities focusing on controls and best practices during compliance monitoring engagements and ERO Enterprise outreach engagements.

Finally, the ERO Enterprise recognizes the Project 2020-03 standards drafting team's ongoing efforts. The project will address the NERC Board resolution adopted at its February 2020 meeting to modify Reliability Standard CIP-003-8 to include policies for low impact BES Cyber Systems to: (1) detect known or suspected malicious communications for both inbound and outbound communications; (2) determine when active vendor remote access sessions are initiated; and (3) disable active vendor remote access when necessary. The efforts of the Project 2020-03 standards drafting team may address items noted in the Study.

Appendix A: Electronic Access Controls Implementation Form

The ERO Enterprise gathered specific information about registered entities' implementation of electronic access controls to assets containing low BES Cyber Systems using the CIP-003-8 electronic controls implementation study form below. The form is listed in the CIP-003 Reliability Standard Audit Worksheet, and was utilized during compliance monitoring engagements to obtain relevant information for the Study. As noted earlier, the ERO Enterprise gathered data from approximately 200 registered entities between January 1, 2020 and March 1, 2021.

NERC Reliability Standard Audit Worksheet

CIP-003-8 Electronic Controls Implementation Study

This section to be completed by the Compliance Enforcement Authority

For compliance engagements between January 1, 2020, and June 30, 2021, compliance monitoring teams shall capture the following information:

1. Describe the electronic access controls for low impact BES Cyber Systems the Responsible Entity has chosen to implement.

2. Describe the circumstances associated with the Responsible Entity's implementation of electronic access controls for low impact BES Cyber Systems. This information may include aspects of the environment of the controls used, such as physical conditions, network topologies, how the need for access is determined and documented, or other items that are necessary to understand the effectiveness of the electronic controls.

3. In the professional judgement of the compliance monitoring team, do the electronic access controls adopted by the Responsible Entity for low impact BES Cyber Systems provide adequate security? If not, please describe how the security is inadequate and how an entity might approach improving this security.

4. Provide any additional information regarding electronic access to low impact BES Cyber Systems that may be relevant to this study.

5. In the professional judgement of the compliance monitoring team, are any changes necessary to the language of CIP-003-8 in order to improve the effectiveness of this Standard? If so, please describe the suggested changes.

Provide the above information to NERC in the manner prescribed by NERC.