NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 2, 2017

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

Re: CIP-014 Report – Physical Security Protection for High Impact Control Centers
Docket No. RM15-14-__

Dear Secretary Bose:

Pursuant to Order No. 802 of the Federal Energy Regulatory Commission ("FERC" or "Commission),[1] the North American Electric Reliability Corporation hereby submits a report as **Attachment 1** hereto, assessing whether all Control Centers with High Impact BES Cyber Systems, as identified and categorized pursuant to Reliability Standard CIP-002-5.1a, should be protected under the CIP-014 Reliability Standard. Should you have any questions, please do not hesitate to 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

cc: Official service list in Docket No. RM15-14-000

[1] Order No. 802, *Physical Security Reliability Standard*, 149 FERC ¶ 61,140 (2014).

CERTIFICATE OF SERVICE

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

Dated at Washington, D.C. this 2nd day of October, 2017.

/s/ Shamai Elstein

Shamai Elstein
Counsel for the North American Electric Reliability Corporation

ATTACHMENT 1

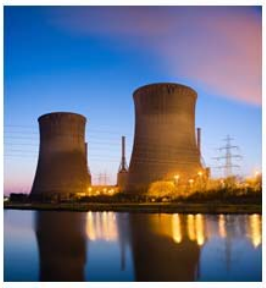
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-014 Report

Physical Security Protection for High Impact Control Centers

October 2, 2017

RELIABILITY | ACCOUNTABILITY

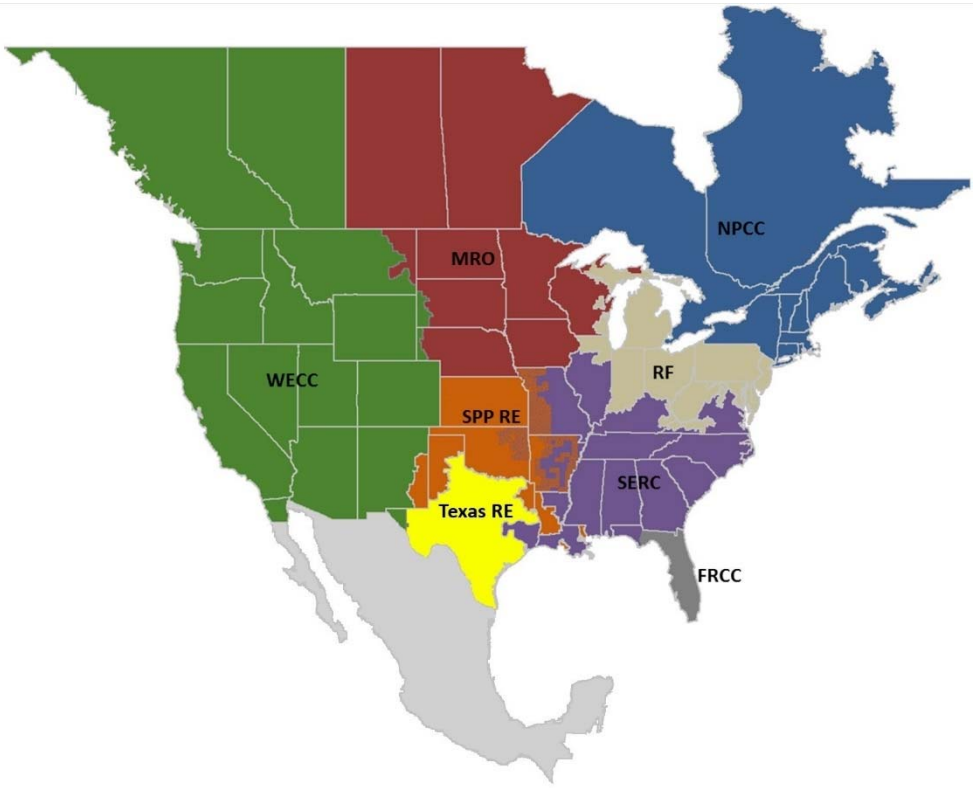
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

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 and security 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 or Commission) 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 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

Introduction

The reliability and security of the BPS is fundamental to national security, economic development, and public health and safety. A major disruption in electric service due to extreme weather, equipment failure, a cyber security incident, or a physical attack could have far-reaching effects. Owners and operators of the BPS must therefore institute measures to protect against and mitigate the impact from both conventional risks (e.g., extreme weather and equipment failures) and emerging security risks, such as physical attacks intended to damage or disable critical elements of the BPS.[1]

To that end, NERC's Critical Infrastructure Protection (CIP) Reliability Standards require registered entities to implement physical security controls to protect critical Bulk Electric System (BES) assets. Pursuant to the CIP cyber security Reliability Standards, registered entities must (i) identify and categorize their BES Cyber Systems as High, Medium, or Low Impact, (ii) implement protections to control physical access to Low Impact BES Cyber Systems (CIP-003-6, Requirement R2), (iii) provide cyber security training to and perform background checks on any individuals granted unescorted physical access to High and Medium Impact BES Cyber Systems (CIP-004-6, Requirements R2 and R3), (iv) implement an access management program (CIP-004-6, Requirement R4) for High and Medium Impact BES Cyber Systems, and (v) implement protections to monitor and control physical access to High and Medium Impact BES Cyber Systems (CIP-006-6, Requirements R1 and R2).

Additionally, in Order No. 802, FERC approved Reliability Standard CIP-014-1, which requires Transmission Owners (TOs) and Transmission Operators (TOPs) to protect certain "critical" Transmission stations and substations and their associated primary Control Centers from physical attack that could damage or render such facilities inoperable.[2] The CIP-014 Reliability Standard requires TOs to take the following steps to address the risks that physical attacks pose to the reliable operation of the BPS:

- Perform a risk assessment of their systems to identify (1) their "critical" Transmission stations and Transmission substations (i.e., those that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection), and (2) the primary Control Centers that operationally (i.e., physically) control the identified Transmission stations and Transmission substations.
- Evaluate the potential threats and vulnerabilities of a physical attack to the facilities identified in the risk assessment.
- Develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of the identified facilities.

Further, TOPs that operate primary Control Centers that operationally control any of the Transmission stations or substations identified by the TO must also:

- Evaluate the potential threats and vulnerabilities of a physical attack to such primary control centers; and

[1] Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, http://www.nerc.com/files/Glossary_of_Terms.pdf.

[2] Order No. 802, *Physical Security Reliability Standard*, 149 FERC ¶ 61,140 (2014). Subsequently, the Commission approved a second version of the standard, CIP-014-2, to remove the term "widespread" from the requirements, consistent with the Commission's directive in Order No. 802. *N. Am. Elec. Reliability Corp.*, Letter Order, Docket No. RD15-4-000 (Jul. 14, 2015).

- Develop and implement a security plan, based on the evaluation of threats and vulnerabilities, designed to protect against and mitigate the impact of physical attacks that may compromise the operability or recovery of such primary Control Centers.

When approving the CIP-014 Reliability Standard, FERC also directed NERC to make an informational filing assessing whether all Control Centers with High Impact BES Cyber Systems (referred to herein as High Impact Control Centers) should be protected under the CIP-014 Reliability Standard.[3] As described in Section 1 of Attachment 1 to Reliability Standard CIP-002-5.1a, High Impact Control Centers include certain primary and backup control centers that perform the functions of a Reliability Coordinator (RC), Balancing Authority (BA), Generator Operator (GOP), and TOP. BES Cyber Systems that are used by and located at such Control Centers receive heightened scrutiny under the CIP cyber security Reliability Standards CIP-003 through CIP-011 and are subject to the most controls. FERC sought to understand "whether there is a need for consistent treatment of 'High Impact' Control Centers for cyber security and physical security purposes through the development of Reliability Standards that afford physical protection to all 'High Impact' Control Centers."[4] FERC directed NERC to submit the informational filing within two years of the effective date of CIP-014-1 (i.e., October 1, 2017) as NERC would be "in a better position to provide this assessment after implementation of Reliability Standard CIP-014-1 and Reliability Standard CIP-006-5, the latter of which provides some physical protection to 'High Impact' control centers."[5]

Consistent with FERC's directive, this report provides NERC's assessment of whether the CIP-014 Reliability Standard should apply to all High Impact Control Centers, not just those primary Control Centers that operationally control the identified "critical" Transmission stations and substations. As explained in this report, based on further analysis of security risks and BPS impact, NERC found that if a High Impact Control Center with operational control of BES Facilities, whether a primary or backup, is subject to a physical attack, it could have a direct and significant impact on Real-time operations and may result in instability, uncontrolled separation, or Cascading within an Interconnection. Due to this concern, NERC will initiate its stakeholder processes to further evaluate and consider applying the controls required in the CIP-014 Reliability Standard (specifically Requirements R4, R5, and R6) to other High Impact primary and backup Control Centers with operational control over BES Transmission or generation Facilities.

This report is organized as follows:

- Section 1 discusses the development, scope, and requirements of the CIP-014 Reliability Standard, and FERC's directive to submit an informational report on physical security for High Impact Control Centers.
- Section 2 describes High Impact Control Centers and their BES reliability-related functions.
- Section 3 provides data on the number and type of High Impact Control Centers currently identified as subject to the CIP-014 Reliability Standard.
- Section 4 discusses the various physical security threats associated with Control Centers and the manner in which the currently-effective CIP Reliability Standards address those threats.
- Section 5 explains NERC's assessment that, given the physical security threats to and importance of High Impact Control Centers to BES reliability, NERC, working with stakeholders, will further evaluate and consider applying the controls required in the CIP-014 Reliability Standard to other High Impact primary and backup Control Centers with operational control over BES Transmission or generation assets.

[3] *Id*. at P 58.

[4] *Id*. at P 57.

[5] *Id*. at P 58.

- Section 6 discusses next steps to address the issues through NERC's stakeholder processes.

Section 1: CIP-014 Requirements and High Impact Control Center Directive

FERC Order Directing Development of CIP-014

On April 16, 2013, unknown assailants attacked the Metcalf substation in Coyote, California. The assailants cut fiber-optic phone lines, shutting off service to nearby neighborhoods, and fired more than 100 rounds of .30-caliber rifle ammunition into the radiators of 17 electricity transformers at the substations. The assault lasted only 19 minutes, but it caused $15 million in damage. Although this incident did not adversely impact reliable BES operations, the attack underscored the importance of physical security for BES infrastructure. Physical attacks on BES infrastructure have the potential to adversely impact the reliable operation of the BES and, if critical infrastructure is damaged or rendered inoperable as a result of a physical attack, could result in instability, uncontrolled separation, or Cascading in an Interconnection.

The Metcalf incident initiated renewed focus on the threat of physical attacks on BES infrastructure, and on March 7, 2014, FERC issued an order directing NERC to submit for approval, within 90 days, "one or more Reliability Standards that [would] require certain registered entities to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation of the [BPS]."[6] FERC stated that the Reliability Standard should require owners and operators of the BPS to take at least three steps: (1) registered entities should be required to "perform a risk assessment of their systems to identify their 'critical facilities'"; (2) registered entities should be required to "evaluate the potential threats and vulnerabilities to those identified critical facilities"; and (3) registered entities should be required to "develop and implement a security plan designed to protect against attacks to [their critical facilities] based on the assessment of the potential threats and vulnerabilities to their physical security."[7]

Among other things, FERC also stated that the proposed Reliability Standard(s) should include procedures for a third party to (1) verify the list of identified facilities, (2) review the evaluation of threats and vulnerabilities, and (3) review the security plan. FERC also stated that "[a] critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the [BPS]," noting that "[FERC] expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers."[8]

Requirements in CIP-014

In response to FERC's March 7 Order, NERC developed Reliability Standard CIP-014-1, which contains six requirements designed to protect against and mitigate the impact of physical attacks on certain Transmission stations and Transmission substations, and their associated primary control centers, as follows:

- *Requirement R1* requires applicable TOs to perform risk assessments on a periodic basis to identify their Transmission stations and substations (existing and planned to be in service within 24 months) that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.[9] The TO must then identify the primary control center that operationally controls each of the identified Transmission stations or Transmission substations.

---

6 *Reliability Standards for Physical Security Measures*, 146 FERC ¶ 61,166, at P 1 (2014) (March 7 Order).

7 *Id*. at PP 6-9.

8 *Id*. at P 6, FN 6.

9 A TO that identified a "critical" Transmission station/substation in its previous risk assessment under Requirement R1, must perform another risk assessment within 30 calendar months. A TO that did not identify a "critical" Transmission station/substation in its previous risk assessment under Requirement R1, must perform another risk assessment within 60 calendar months.

- *Requirement R2* provides that each applicable TO shall have an unaffiliated third party with appropriate experience verify the risk assessment performed under Requirement R1. The TO must either modify its identification of facilities consistent with the verifier's recommendation or document the technical basis for not doing so.
- *Requirement R3* requires the TO to notify a TOP that operationally controls a Transmission station or substation identified under Requirement R1 of such identification. This requirement helps ensure that the TOP has notice of the identification so that it may timely fulfill its resulting obligations under Requirements R4 and R5 to protect that primary Control Center.
- *Requirement R4* requires each applicable TO and TOP to conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of its respective Transmission station(s), Transmission substation(s), and primary Control Center(s) identified in Requirement R1, as verified under Requirement R2. The evaluation shall consider the following: (1) the unique characteristics of the identified critical facilities; (2) prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and (3) intelligence or threat warnings received from sources such as law enforcement, the ERO, the Electricity Information Sharing and Analysis Center (E-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.
- *Requirement R5* requires each TO and TOP to develop and implement a documented physical security plan that covers each of its respective Transmission stations, Transmission substations, and primary Control Centers identified in Requirement R1, as verified under Requirement R2. The physical security plans shall include the following attributes: (1) resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4; (2) law enforcement contact and coordination information; (3) a timeline for executing the physical security enhancements and modifications specified in the physical security plan; and (4) provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).
- *Requirement R6* provides that each TO and TOP subject to Requirements R4 and R5 have an unaffiliated third party with appropriate experience review its Requirement R4 evaluation and Requirement R5 security plan. Each TO or TOP must either modify its evaluation and security plan consistent with the recommendation of the reviewer or document its reasons for not doing so.

As relevant to this report, NERC explained in its petition that the primary focus of the Reliability Standard is Transmission stations and substations, which are uniquely essential elements of the BPS as they make it possible for electricity to move long distances, connect generation to the grid, serve as critical links or hubs for intersecting power lines, and are vital to the delivery of power to major load centers.[10] The petition also explained that the standard drafting team for CIP-014-1 recognized that it was also necessary to identify and protect the primary control centers that operationally control any critical Transmission stations or Transmission substations.[11] The petition explained:

> A primary control center is a control center that the TO or TOP uses as the principal, permanently-manned site to operate a [BPS] facility. A primary control center operationally controls a Transmission station or Transmission substation when the electronic actions from the control center can cause direct physical action at the identified Transmission station or Transmission substation, such as opening a breaker. If a physical attack damages or otherwise renders such a primary control center inoperable, it could jeopardize the reliable operation of the critical

[10] *Petition of NERC for Approval of Proposed Reliability Standard CIP-014-1* at 18, Docket No. RM14-15-000 (May 23, 2014).

[11] *Id*. at 19.

> Transmission station and Transmission substation in Real-time because it could remove or severely limit the ability to operate that critical facility remotely to respond to events on the system or otherwise ensure the reliable operation of a critical [BPS] facility. Similarly, if perpetrators of a physical attack seize a primary control center that operationally controls a critical Transmission station or Transmission substation, the attackers could directly operate the critical Transmission station and Transmission substation to cause significant adverse reliability impacts.[12]

NERC also explained that it did not extend the scope of the CIP-014 Reliability Standard to Control Centers that provide back-up capability and Control Centers that cannot operationally control a critical Transmission station or substation, as they do not present the same risks to Real-time operations if they are the target of a physical attack.[13] As it relates to backup Control Centers, NERC explained that if a physical attack damages or renders inoperable a backup Control Center for a critical Transmission station or Transmission substation, it would be unlikely to have significant adverse reliability impact in Real-time as the registered entity can continue operating the Transmission station or substation from the primary Control Center.[14]

Similarly, NERC explained that a physical attack at a Control Center that only has monitoring or oversight capabilities would likely not have the direct reliability impact in Real-time contemplated in the March 7 Order because operators at such Control Centers do not have the ability to physically operate critical BPS facilities.[15] Although certain monitoring and oversight capabilities might be lost if the Control Center is damaged or rendered inoperable as a result of a physical attack on such controls centers, NERC explained that the TO or TOP that operationally controls the critical Transmission station or substation would be able to continue operating its transmission system to prevent instability, uncontrolled separation, or Cascading within an Interconnection.[16]

NERC also stated that, consistent with FERC's focus in the March 7 Order on Transmission Facilities, the scope the CIP-014 Reliability Standard did not include generation Facilities and any associated Control Centers.[17] NERC noted that the loss of a generation Facility is unlikely to have the uncontrollable impact that FERC was concerned about in the March 7 Order.

NERC also acknowledged that certain Control Centers with High Impact BES Cyber Systems under Reliability Standard CIP-002-5.1 would not be subject to the proposed Reliability Standard.[18] NERC stated that this reflects the different nature of cyber security risks and physical security risks at Control Centers. Specifically, an asset that presents a heightened risk to the BPS from a cyber security perspective may not present the same risk from a physical security perspective and vice versa. A primary cyber security concern for Control Centers is the corruption of data or information and the potential for operators to take action based on corrupted data or information. This concern exists at Control Centers that operationally control BPS facilities and those that do not. As such, there is no distinction in CIP-002-5.1 between these Controls Centers. In contrast, NERC stated that such a distinction is

12 *Id*. at 19.

13 *Id*. at 19-20.

14 *Id*.

15 *Id*. at 20-21.

16 *Id*.

17 *Id*. at 22-24.

18 *Id*. at n. 55.

appropriate in the physical security context and concluded that each type of High Impact Control Center under CIP-002-5.1 does not necessarily need the additional protections provided by the proposed Reliability Standard.[19]

NERC also explained that while the proposed Reliability Standard only covers primary Control Centers that operationally control a critical Transmission station or substation, the physical security protections required under the CIP-006 Reliability Standard are applicable to all High and Medium Impact Control Centers irrespective of their ability to operationally control BPS facilities. Reliability Standard CIP-006-6 requires registered entities to implement physical security measures designed to restrict physical access to locations containing High and Medium Impact BES Cyber Systems. As it does with all of its mandatory Reliability Standards, NERC committed to continue to assess the scope and effectiveness of the CIP-014 Reliability Standard, including whether it should apply to all High Impact Control Centers.[20]

Order No. 802 Directive for Informational Filing on High Impact Control Centers

FERC approved CIP-014-1 in Order No. 802 on November 20, 2014. In a letter order issued July 14, 2015, FERC approved CIP-014-2, which removed the term "widespread" from the Reliability Standard.[21] As noted above, in Order No. 802, FERC also directed NERC to make an informational filing that assesses whether all High Impact Control Centers should be protected under the CIP-014 Reliability Standard, not just those primary Control Centers that physically operate a "critical" Transmission station or substation. The Commission expressed concern that a successful attack on a High Impact Control Center not already covered by the CIP-014 Reliability Standard could prevent or impair situational awareness, especially from a wide-area perspective, or could allow attackers to distribute misleading and potentially harmful data and operating instructions that could result in instability, uncontrolled separation, or cascading failures.[22]

19 *Id*.

20 *Id*. at 14-15; *Comments of the North American Electric Reliability Corporation in Response to Notice of Proposed Rulemaking*, Docket No. RM14-15-000 (Sept. 8 2014).

21 *N. Am. Elec. Reliability Corp.*, Letter Order, Docket No. RD15-4-000 (Jul. 14, 2015).

22 Order No. 802 at P 51.

Section 2: Types of High Impact Control Centers

This section of the report discusses the types of High Impact Control Centers in greater detail, explaining the functions performed at those Control Centers and why they were deemed High Impact for purposes of cyber security protection. The purpose of NERC's CIP cyber security Reliability Standards, CIP-002-5.1a through CIP-010-2, is to mitigate cyber security risks to BES Facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable as a result of a cyber attack would affect the reliable operation of the BES. The CIP cyber security Reliability Standards apply a risk-based construct, requiring Responsible Entities[23] to identify and categorize BES Cyber Systems as High, Medium, or Low Impact consistent with the criteria set forth in Attachment 1 to CIP-002-5.1a, and then protect those BES Cyber Systems commensurate with the risks they present to the reliable operation of the BES, in accordance with the requirements in CIP-003 through CIP-011.[24]

According to Section 1 of Attachment 1 to CIP-002-5.1a, BES Cyber Systems used by and located at the following Control Centers must be identified as "High Impact":

1.1 Each Control Center or backup Control Center used to perform the functional obligations of the RC.

1.2 Each Control Center or backup Control Center used to perform the functional obligations of the BA for: (1) generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or (2) one or more of the assets:

- Each generation Facility that its Planning Coordinator (PC) or Transmission Planner (TP) designates, and informs the Generator Owner (GO) or GOP, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year (Criterion 2.3).
- Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its RC, PC, or TP as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies (Criterion 2.6).
- Each Special Protection System (SPS), Remedial Action Scheme (RAS), or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROLs violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable (Criterion 2.9).

1.3 Each Control Center or backup Control Center used to perform the functional obligations of the TOP for one or more of the following assets:

- Each BES reactive resource or group of resources at a single location (excluding generation Facilities) with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (excluding those at generation Facilities) (Criterion 2.2).
- Transmission Facilities operated at 500 kV or higher (Criterion 2.4).
- Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation, where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations and has an "aggregate weighted value"

[23] As used in the CIP Reliability Standards, a Responsible Entity refers to the registered entity responsible for the implementation of and compliance with a particular requirement.

[24] Order No. 791, *Version 5 Critical Infrastructure Protection Reliability Standards*, 145 FERC ¶ 61,160, 78 Fed. Reg. 72,755 (2013), *order on clarification and reh'g*, Order No. 791-A, 146 FERC ¶ 61,188 (2014).

exceeding 3000. The “aggregate weighted value” for a single station or substation is determined by summing the "weight value per line" for each incoming and each outgoing BES Transmission Line that is connected to another Transmission station or substation (Criterion 2.5).

- Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements (Criterion 2.7).
- Transmission Facilities, including generation interconnection Facilities, providing the generation interconnection required to connect generator output to the Transmission Systems that, if destroyed, degraded, misused, or otherwise rendered unavailable, would result in the loss of generation Facilities exceeding 1500 MW in a single Interconnection or a reactive resource or group of resources at a single location with an aggregate maximum Reactive Power nameplate rating of 1000 MVAR or greater (Criterion 2.8).
- Each SPS, RAS, or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROLs violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable (Criterion 2.9).
- Each system or group of Elements that performs automatic load shedding under a common control system, without human operator initiation, of 300 MW or more implementing under voltage load shedding (UVLS) or under frequency load shedding (UFLS) under a load shedding program that is subject to one or more requirements in a NERC or regional Reliability Standard (Criterion 2.10).

1.4 Each Control Center or backup Control Center used to perform the functional obligations of the GOP for one or more of the following assets:

- Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. (Criterion 2.1).
- Each generation Facility that its PC or TP designates, and informs the GO or GOP, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year (Criterion 2.3).
- Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its RC, PC, or TP as critical to the derivation of IROLs and their associated contingencies (Criterion 2.6).
- Each SPS, RAS, or automated switching System that operates BES Elements, that, if destroyed, degraded, misused or otherwise rendered unavailable, would cause one or more IROLs violations for failure to operate as designed or cause a reduction in one or more IROLs if destroyed, degraded, misused, or otherwise rendered unavailable (Criterion 2.9).

The Control Centers described in Criteria 1.1-1.4 are referred to in this report as High impact Control Centers.[25] From a cyber security perspective, each of these Control Center types were designated as High Impact because of the Real-time operational impact to the grid if compromised by a cyber attack. The following is a discussion of the functions supported by each type of High Impact Control Center.

[25] As defined in the NERC Glossary, a Control Center includes any associated data center.

Control Centers Performing the Function of the Reliability Coordinator

As described in NERC's Functional Model,[26] the RC maintains the Real-time operating reliability of its RC Area and in coordination with its neighboring RC's wide-area view. The wide-area view includes situational awareness of its neighboring RC Areas. Its scope includes both transmission and balancing operations, and it has the authority to direct other functional entities to take certain actions to ensure that its RC Area operates reliably. An RC, however, does not have direct operational control (i.e., physical control) of any Transmission or generation Facilities.

Under CIP-002-5.1a, all Control Centers performing the functions of the RC are deemed High Impact Control Centers because of the functions that the RC performs. From a cyber security perspective, if the BES Cyber Systems used by and located at such Control Centers were compromised such that the data used and communicated by the RC was corrupted, there could be a significant adverse impact on Real-time reliability as operators could take action based on corrupted data.

Control Centers Performing the Functions of the Balancing Authority

The BA, as described in the Functional Model, integrates resource plans ahead of time, maintains generation-load-interchange-balance within a BA Area, and contributes to Interconnection frequency in Real-time. Similar to the RC, BAs have a coordination role and may not have direct operational control of any BES Facilities.

Under CIP-002-5.1a, Control Centers performing the function of a BA for over 3000 MW in a single interconnection or for certain other types of assets are designated as High Impact. From a cyber security perspective, if the BES Cyber Systems used by and located at such Control Centers were subject to a cyber attack, such that the data used and communicated by the BA was corrupted, there could be a significant adverse impact on Real-time reliability as operators could take action based on corrupted data.

Control Centers Performing the Functions of the Transmission Operator

As described in the Functional Model, TOPs are responsible for the Real-time operating reliability of the Transmission assets within its TOP Area. The TOP is responsible for the Real-time operating reliability of the transmission assets under its purview. The TOP has the authority to take certain actions to ensure that its TOP Area operates reliably. An entity performing the functions of the TOP is frequently the entity with direct operation control over Transmission Facilities.

Under CIP-002-5.1a, Control Centers performing the function of a TOP for certain types of significant Transmission Facilities are designated as High Impact. From a cyber security perspective, if the BES Cyber Systems used by and located at such Control Centers were subject to a cyber attack, such that the data used and communicated by the TOP was corrupted or results in a threat actor gaining remote control over Transmission assets, there is the potential for significant adverse impact in a single Interconnection.

Control Centers Performing the Functions of the Generator Operator

As described in the NERC Functional Model, the GOP directly operates, or directs the operation of, generation Facilities and performs the functions of supplying energy and reliability-related services. An entity performing the functions of the GOP is frequently the entity with direct operation control over generation Facilities.

Under CIP-002-5.1a, Control Centers performing the function of a GOP for over 1500 MW in a single interconnection or for certain other types of generation assets are designated as High Impact. From a cyber security perspective, if the BES Cyber Systems used by and located at such Control Centers were subject to a cyber

[26] NERC's Functional Model is available at http://www.nerc.com/pa/Stand/Functional%20Model%20Archive%201/Functional_Model_V5_Final_2009Dec1.pdf.

attack, such that the data used and communicated by the GOP was corrupted or results in a threat actor gaining remote control over generation assets, there is the potential for significant adverse impact in a single Interconnection.

Section 3: Analysis of High Impact Control Centers Subject to CIP-014

As discussed above, a Control Center is within the scope of the CIP-014 Reliability Standard if it operationally controls a "critical" Transmission station or substation. To help assess whether the controls in the CIP-014 Reliability Standard should apply to other High Impact Control Centers, NERC collected data on the High Impact Control Centers that registered entities identified as subject to CIP-014-2. The following section provides a summary of that data.

Control Center Population Subject to CIP-014

To determine the total population of High Impact Control Centers, NERC reviewed data collected through registered entities' self-certifications of CIP-002-5.1a and CIP-014-2. The following discusses the self-certifications used to collect the necessary information.

Self-Certification for CIP-002-5.1a

To help assess compliance with Reliability Standard CIP-005-2.1a, in the third quarter of 2016, NERC and the Regional Entities (collectively, the ERO Enterprise) directed applicable registered entities to complete a self-certification for CIP-002-5.1a. Entities were required to report the number and type of BES assets (e.g., Control Centers (primary and backup), Transmission stations or substation, generation plants, etc.) with High, Medium, or Low Impact BES Cyber Systems. Through these self-certifications, NERC identified a total of 143 registered entities with High Impact Control Centers. Collectively, these 143 entities have a total of 432 High Impact Control Centers (primary and backup Control Centers). There are 32 registered entities with multiple primary High Impact Control Centers, and 47 registered entities have multiple backup High Impact Control Centers.

Self-Certification for CIP-014-2

To help assess compliance with Reliability Standard CIP-014-2, in the second quarter of 2016, NERC and the Regional Entities directed registered TOs to complete a self-certification related to compliance with Requirements R1-R3 of CIP-014-2.[27] Specifically, the TOs were asked to provide answers to the following requests:

- Identify the number of Transmission stations and substations that meet the criteria under Applicability Section 4.1.1.
- Indicate whether an initial risk assessment has been performed for these assets pursuant to Requirement R1.
- Identify the number of primary Control Centers associated with the assets identified under Requirement R1.
- Indicate whether a third party verified the risk assessment pursuant to Requirement R2.
- Provide the number of Transmission stations, substations, and associated primary Control Centers that resulted after the third-party verification.
- Indicate whether any TOPs were notified pursuant to Requirement R3, and list their names.

Through these self-certifications, NERC identified that there were 65 TOs or TOPs with a Control Center subject to CIP-014-2. These 65 entities collectively identified a total of 105 primary Control Centers subject to the standard. All 105 primary Control Centers are High Impact Control Centers, as described in Section 1 of Attachment 1 to CIP-002-5.1a.[28] Given the total number of High Impact Control Centers (432), the percentage of

[27] There were 315 entities registered as TOs as of May 13, 2016.

[28] These 65 registered entities also have 118 High Impact Control Centers that they did not identify as subject to CIP-014-2.

High Impact Control Centers that registered entities identified subject to CIP-014-2 is approximately 24 percent of the total number of High Impact Control Centers (See Figure 3.1).

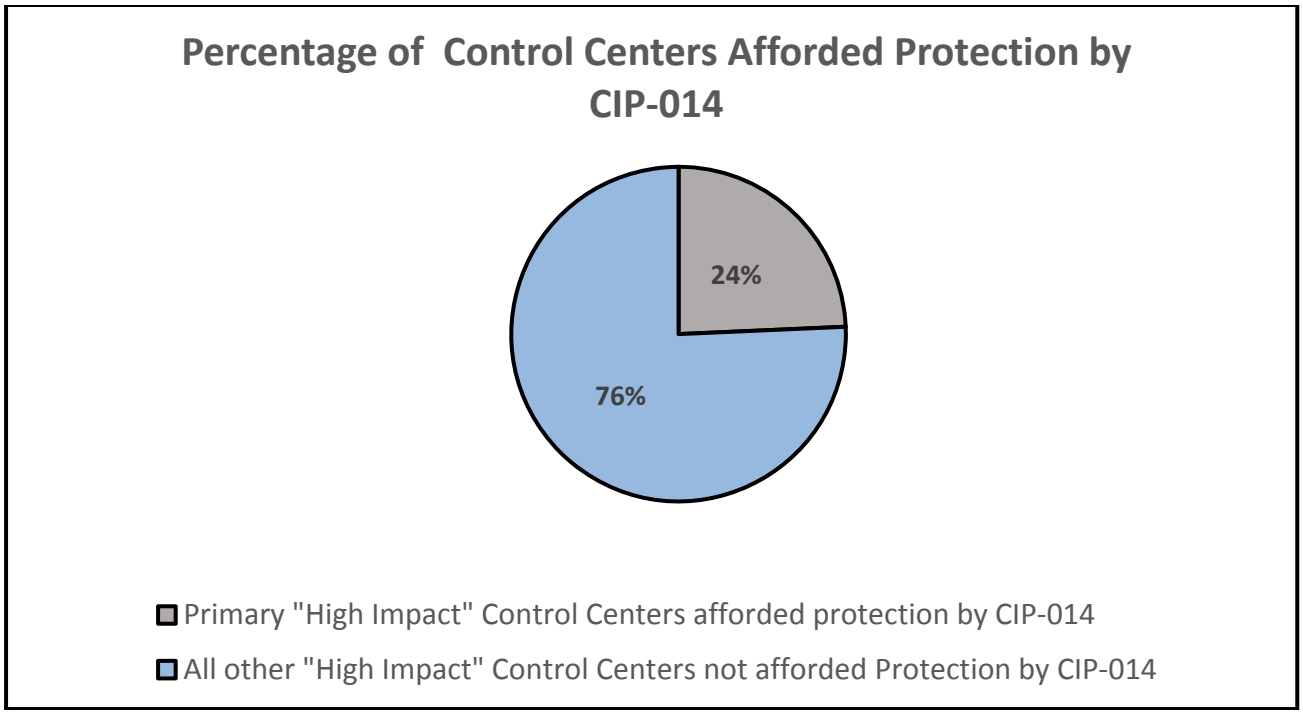


Figure 3.1: Percentage of Control Centers Afforded Protection by CIP-014

Analysis of Self-Certification Data

The data provided by the self-certifications indicate that 143 registered entities had High Impact Control Centers and that 65 (or 45 percent) of those registered entities had a primary High Impact Control Center subject to CIP-014-2. As such, 78 (or 55 percent) of registered entities with a High Impact Control Center did not have a Control Center subject to CIP-014-2. See Figure 3.2.

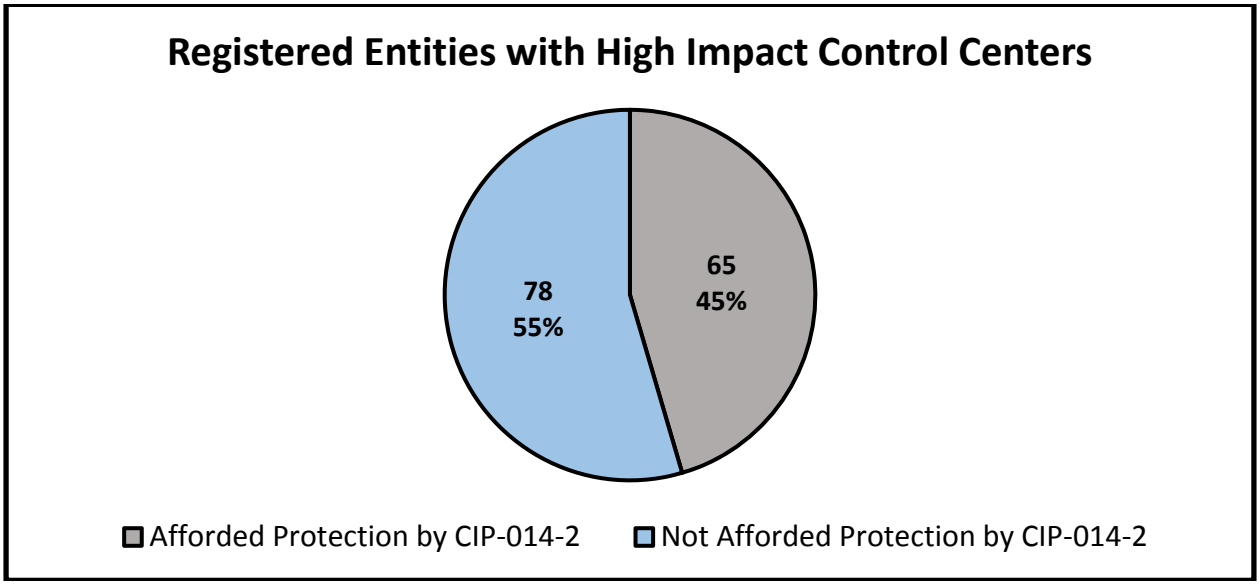


Figure 3.2: Registered Entities with High Impact Control Centers

A further analysis of the self-certification data indicates that of the 65 registered entities with Control Centers subject to the CIP-014 Reliability Standard, there are 27 registered TOs with 20 or more Transmission stations or substations that meet the criteria in Section 4.1.1 of CIP-014-2. Of these 27 registered entities, 25 have identified at least one "critical" Transmission station or substation and at least one High Impact Control Center subject to the requirements of the CIP-014 Reliability Standard.

Of the 78 registered entities with High Impact Control Centers that did not identify as having a Control Center subject to CIP-014-2, 16 of those registered entities are not registered as TOs or TOPs (i.e., they are RCs, BAs, or GOPs). Six of these 16 registered entities do not have operational control of any Transmission stations or substations or generation resources. These six registered entities account for 11 High Impact primary Control Centers and 11 High Impact backup Control Centers. The remaining 10 of the 16 registered entities have operational control of generation assets which account for 13 High Impact primary Control Centers and 13 High Impact backup Control Centers. Collectively, these 10 registered entities control seven Medium Impact generation resources, as defined in Section 2 of Attachment 1 to CIP-002-5.1a, and 220 Low Impact generation resources, as defined in Section 3 to Attachment 1 to CIP-002-5.1a. See Table 3.1.

Table 3.1: GO/GOP/BA Registered Entities Not Subject to CIP-014 and Span of Control

GO/GOP/BA with High Impact Control Centers Not Subject to CIP-014	GO/GOP/BA Registration with Operational Control Over Generation Resources	Number of Primary High Impact Control Centers	Number of Backup High Impact Control Centers	Medium Impact Generation Resources	Low Impact Generation Resources
16	10	13	13	7	220

The remaining 62 of the 78 entities with High Impact Control Centers that did not identify as having a Control Center subject to CIP-014-2 are registered as TOs or TOPs. These TOs and TOPs did not identify a primary Control Center with operational control of a "critical" Transmission station or substation per CIP-014-2 R1. Collectively, they have a total of 161 High Impact primary and backup Control Centers, and have operational control of 369 Medium Impact substations, as defined in Section 2 of Attachment 1 to CIP-002-5.1a, and 3,791 Low Impact substations, as defined in Section 3 of Attachment 1 to CIP-002-5.1a. See Table 3.2.

Table 3.2: Registered Entities Not Subject to CIP-014 and Operational Control

TO/TOP Registration Not Subject to CIP-014	Number of Primary High Impact Control Centers	Number of Backup High Impact Control Centers	Medium Impact Substations Operated	Low Impact Substations Operated
62	79	82	369	3,791

Section 4: Control Center Physical Security Threats

There are two basic threats to consider relating to the physical security of Control Centers: (1) a physical attack designed to damage, destroy, or otherwise render the Control Center inoperable; or (2) a physical attack designed to gain physical access to the Control Center to operate BES assets in a manner that would adversely affect reliable BES operations.

In the first type of threat, the assailant's objective is to affect the availability or operability of the Control Center. For instance, threat actors could approach the facility housing the Control Center in a vehicle filled with explosives and detonate it close enough to the facility to destroy or damage the facility to render the Control Center inoperable. Similarly, a threat actor could seek to render a Control Center inoperable by cutting off its power sources, including its backup power supplies. Additionally, this type of threat scenario also includes threat actors seeking to gain entry into the facility housing the Control Center to damage or destroy the equipment and systems in the Control Center used to operate the grid.

The second type of threat involves threat actors that seek to gain physical access to the Control Center with the intent to operate the grid in an unreliable manner, by directly operating or directing others to operate the system in a manner that would adversely affect reliable operations, including damaging BES equipment. This type of physical attack may require the threat actors to have a sophisticated knowledge of grid operations and the BES Cyber Systems that control BES Facilities. This type of attack *could* have a greater impact on BES operations as compared to the first type of attack.

The CIP Reliability Standards seek to address these physical security threats through the physical security controls required in Reliability Standards CIP-003-6, CIP-004-6, CIP-006-6, and CIP-014-2. First, under currently effective Reliability Standard CIP-003-6, Requirement R2, entities must control physical access to Low Impact BES Cyber Systems.[29] If an entity has a Control Center with Low Impact BES Cyber Systems, it must implement controls to prevent unauthorized physical access to such systems.

Pursuant to CIP-004-6, the registered entity must take the following actions for any individual granted unescorted physical access to High Impact BES Cyber Systems and associated Electronic Access Control and Monitoring Systems (EACMS) and Protected Cyber Assets (PCAs), and Medium Impact BES Cyber Systems with External Routable Connectivity (ERC) and associated EACMS and PCAs:

- Provide the individual training on physical access controls, among other things (Requirement R2).
- Perform a personnel risk assessment (or background check) of the individual (Requirement R3).
- Implement an access management program to authorize, based on need, individuals that may have unescorted physical access into a Physical Security Perimeter (PSP), which houses BES Cyber Systems (Requirement R4).
- Implement an access revocation program to revoke an individual's access authorization (Requirement R5).

The requirements in CIP-004-6 are designed to reduce the risk of physical security events at Control Centers and other types of facilities by training individuals on physical access controls (i.e., how they work, what to look for, etc.) and taking steps to eliminate insider threats by ensuring that only individuals with a need for unauthorized physical access have and can be trusted with such access.

[29] A modified version of the standard, CIP-003-7, is currently pending before the Commission in Docket No. RM17-11-000. The affirmative obligation to implement physical access controls remains in the pending version.

Further, pursuant to Reliability Standard CIP-006-6, registered entities must implement protections to monitor and control unauthorized physical access to High Impact and Medium Impact BES Cyber Systems, further mitigating the threat of a physical attack. More specifically, CIP-006-6 Requirement R1 mandates that registered entities implement one or more documented physical security plans that include the following:

- For Medium Impact BES Cyber Systems and Physical Access Control Systems (PACS) associated with High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with ERC, registered entities must define operational or procedural controls to restrict physical access (Part 1.1).
- For Medium Impact BES Cyber Systems with ERC and associated EACMS and PCAs, registered entities must utilize at least one physical access control to allow unescorted physical access into each PSP to only those individuals who have authorized unescorted physical access (Part 1.2).
- For High Impact BES Cyber Systems and associated EACMS and PCAs, registered entities must utilize two or more different physical access controls to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access (Part 1.3).
- For High Impact BES Cyber Systems and associated EACMS and PCAs, and for Medium Impact BES Cyber Systems with ERC and associated EACMS and PCAs, registered entities must: (1) monitor for unauthorized access through a physical access point into a PSP (Part 1.4); (2) issue an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection (Part 1.5); (3) log entry of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry (Part 1.8); and (4) retain the physical access logs for 90 days.
- For PACS associated with High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with ERC, registered entities must (1) monitor each PACS for unauthorized physical access to a PACS (Part 1.6), and (2) issue an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection (Part 1.7).
- For High Impact BES Cyber Systems and associated PCAs, and for Medium Impact BES Cyber Systems at Control Centers and associated PCAs, registered entities must restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a PSP.

Further, under CIP-006-6 Requirement R2, registered entities must implement a visitor control program that requires: (1) continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each PSP; and (2) manual or automated logging of visitor entry into and exit from the PSP that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor. Lastly, under CIP-006-6 Requirement R3, registered entities must implement a PACS maintenance and testing program to help ensure that the PACS are functioning properly.

In addition to the requirements of Reliability Standards CIP-004-6, and CIP-006-6, the CIP-014 Reliability Standard requires additional physical security protections for certain critical facilities, as discussed in Section 1 of this report. Whereas Reliability Standards CIP-004-6 and CIP-006-6 focus specifically on physical access controls, which may be implemented for the entire Control Center or only the areas in which BES Cyber Systems are located, the CIP-014 Reliability Standard focuses on physical attacks designed to damage or otherwise render the Control Center inoperable, and well as those designed to or to compromise operations through gaining physical access to the Control Center with the intent to operate the grid in an unreliable manner. Further, the CIP-014 Reliability Standard takes a more holistic, objective-based approach, requiring entities to identify site-specific threats

vulnerabilities, and the implementation of site-specific physical security plans designed to mitigate those threats and vulnerabilities.

In performing the threat and vulnerability assessment required by the CIP-014 Reliability Standard for Control Centers, registered entities would consider the risks related to the two types of threat scenarios discussed above: damage/destruction and takeover of operational control. The following are items that registered entities may consider when conducting a threat and vulnerability assessment:

- Terrain/elevation of surrounding ground or structures providing line of sight.
- Line-of-sight distance from approach avenues (distance and direction that armament can be utilized).
- Proximity to and speed of adjacent vehicular traffic for vehicle-induced damage.
- Proximity to traffic for easy vehicular access and egress (e.g., "drive-by" access).
- Proximity to other targets of interest or critical load (e.g., number of customers affected, densely populated area, high-profile commercial or governmental entities served, etc.)
- Number of operational targets, electrical component assets, etc. at a single site.
- Proximity to company or other response personnel may impact target selection and restoration response.
- Proximity to law enforcement or emergency personnel may impact target selection and restoration response.
- The risk resulting from historical events that have occurred at this location as well as similar facilities nationwide and the proximity of these events to the facility being assessed.
- Location of the Control Center (collocated in a company headquarters, standalone secured facility, collocated in company headquarters with other tenants, located in a multi-tenant facility owned by someone else, etc.).

The following are examples of security measures one could expect to see at a site protected under the CIP-014 Reliability Standard:

- Perimeter fencing: At a minimum, registered entities will employ a chain-link fence around the site. The fence will be at least seven feet high with a one-foot barbed wire top guard extending out at a 45-degree angle. Many registered entities will provide additional security by increasing the height of the perimeter fence and using no cut/no climb chain-link fence or expanded metal fencing panels to deter and delay intruders.
- Vehicle and pedestrian access gates: At a minimum, registered entities will secure vehicle and pedestrian access gates with high-strength metal chains and padlocks. Many registered entities will provide additional security by employing automated access control systems with alarm notification on all main access gates and require additional gates be secured in a manner that will only allow them to be opened from inside the facility. Registered entities may also employ high security gates that have been designed and rated to stop vehicles based on vehicle size, weight, and speed of approach. Some registered entities will also employ a vehicle inspection system at vehicle gates, especially if these gates allow access to delivery vehicles.
- On-site or Roving Security Officers/Other Trained Personnel: Some registered entities may employ armed or unarmed contract or proprietary uniformed security officers at either fixed, permanent sites or conducting frequent, irregular vehicle and/or foot patrols.
- Intrusion Detection Systems: Physical intrusion detection is typically accomplished by physical controls put in place to detect entry into a defined security perimeter. Examples of physical intrusion detections

may be security guards, access control systems, mantraps, vehicle traps, motion/vibration sensors, video surveillance, and other motion-detection devices.

The following section analyzes whether, given the types of physical security threats to and risks associated with the inoperability or compromise of High Impact Control Centers, the additional controls required by the CIP-014 Reliability Standard should be applied to categories of High Impact Control Centers beyond those that have operational control of Transmission stations and substations identified by the risks assessments required by Requirement R1

Section 5: Assessment of Application of CIP-014 to High Impact Control Centers

Consistent with FERC's directive in CIP-014, NERC reassessed the scope of the CIP-014 Reliability Standard based on the data described in Section 3 of this report, an evaluation of the physical security threats particular to Control Centers, and the potential impact to BES reliability if a High Impact Control Center were subject to a physical security attack. For the reasons discussed below, NERC found that, from a risk and impact perspective, the distinction between High Impact Control Centers with operational control as compared to those without operational control remains appropriate. NERC also found, however, that, given the thresholds for High Impact Control Centers outlined in Attachment 1 to CIP-00205.1a, if High Impact Control Centers with operational control of BES Transmission or generation Facilities were damaged, otherwise rendered inoperable, or seized as a result of a physical attack, there could be significant adverse reliability impact, including instability, uncontrolled separation, and Cascading in an Interconnection. NERC plans to work with stakeholders to further evaluate and consider applying the controls required in the CIP-014 Reliability Standard (specifically Requirements R4, R5, and R6) to other High Impact primary and backup Control Centers with operational control over BES Transmission or generation Facilities, not just those primary Control Centers that operationally control critical Transmission stations or substations. The following discusses NERC's findings.

Operational Control of BES Facilities

As discussed in Section 1 of this report, the primary focus of the CIP-014 Reliability Standard is to protect Transmission stations and substations given their uniquely essential role in BES operations. Control Centers are only covered by the CIP-014 Reliability Standard insofar as they operationally control a critical Transmission station or substation. NERC initially limited the scope of Control Centers subject to the CIP-014 Reliability Standard to those with operational control of critical Transmission stations and substations because it was those Control Centers that, if subject to a physical attack, could have the types of adverse impacts contemplated in the March 7 Order (i.e., instability, uncontrolled separation, and Cascading within an Interconnection). More specifically, if a Control Center has the capability to remotely cause physical actions at critical Transmission stations or substations (such as opening or closing breakers), a physical attack that damages or otherwise renders such a Control Center inoperable could jeopardize the reliable operation of the Transmission station or substation in Real-time because it could remove or severely limit the ability to operate that critical facility remotely to respond to events on the system, or otherwise ensure the reliable operation of a critical facility. Similarly, if threat actors seize such a Control Center, they could directly operate (or force the registered entity's system operators to operate) the critical Transmission stations and substations to cause significant adverse reliability impacts.

In contrast, Control Centers that do not have operational control of a critical Transmission station or substation, such as a Control Center that performs the functions of an RC or BA, would not have the same direct, Real-time impact if subject to a physical attack. Specifically, if such a Control Center were damaged or rendered inoperable due to a physical attack, the primary impact is the loss of situational awareness and certain wide-area view monitoring or oversight capabilities. The functional entities that operationally control BES Transmission or generation assets, however, would be able to continue operating their assets and communicate with neighboring registered entities to prevent instability, uncontrolled separation, or Cascading within an Interconnection. While the loss of a Control Center that does not have operational control of a "critical" Transmission station or substation would be significant, an attack designed to damage or otherwise render such a Control Center inoperable would likely not have the direct reliability impact on Real-time operations contemplated in the March 7 Order.

Similarly, if threat actors were to gain entry into a Control Center that does not operationally control BES assets, they would not have the ability to directly operate (or force the registered entity's system operator to operate) any BES Facility from that Control Center. The primary risk associated with a physical attack at such a Control Center is that the threat actors would seize control of the facility with the intent to: (1) access the BES Cyber

Systems at the Control Center to corrupt the data and information that system operators with operational control of BES Facilities use to reliably operate the BPS; or (2) force the personnel at the Control Center to direct system operators at other Control Centers with operational control of BES Facilities to take actions contrary to reliable operations. While applying the requirements in Reliability Standard CIP-014-2 to these Controls Centers would help mitigate these risks, extending these mandatory requirements to such Control Centers does not appear necessary at this time. While an attack of this nature could have significant impact, there are already significant barriers to successfully carrying out such an attack. First, the threat actors would have to have a sophisticated knowledge of BES operations specific to that area and the systems within that Control Center. Additionally, such an attack relies on system operators at functional entities with operational control of BES assets to act on the corrupted data/information or on the direction to act contrary to reliability. While these system operators may not have the wide-area view of the RC or BA, it is unlikely that they would take action that would damage their equipment or that they know or suspect could cause significant adverse impact, including instability, uncontrolled separation, or Cascading without communicating with personnel at the compromised Control Center and possibly other impacted functional entities.

More importantly, the requirements in Reliability Standards CIP-004-6 and CIP-006-6, discussed in Section 4, were specifically designed to deter, detect, delay, assess, communicate, and respond to these types of attacks. As discussed above, these Reliability Standards, among other things, help reduce the potential for an insider threat, raise awareness of physical security issues, train personnel on physical access controls, require the implementation of physical security controls to prevent unauthorized access, require registered entities to monitor for unauthorized access, and require the use of alarms or alerts to help response to any detected unauthorized access. During its compliance monitoring activities, the ERO Enterprise has observed that, pursuant to these Reliability Standards, most registered entities with High Impact Control Centers have implemented robust physical access protections to mitigate risks associated with unauthorized access to their Control Centers.

For these reasons, when reassessing the scope of the CIP-014 Reliability Standard consistent with the Commission's directive, NERC did not identify the security need to mandate that entities apply the controls in the CIP-014 Reliability Standard to Control Centers that do not operationally control BES assets. Nevertheless, NERC will, in conjunction with its stakeholders, continue to evaluate physical security issues for these Control Centers to determine whether any additional security protections should be mandated. Furthermore, NERC will continue to encourage entities to conduct threat and vulnerability assessments for these Control Center to enhance their security awareness and protections.

High Impact Control Centers Not Already Subject to CIP-014-2 with Operational Control of BES Assets

While NERC's assessment that operational control of BES assets is a well-founded basis for whether to mandate that registered entities apply the controls required in the CIP-014 Reliability Standard to High Impact Control Centers, NERC found that the application of those controls should not necessarily be restricted to those High Impact Control Centers that have operational control over a critical Transmission station or substation. As set forth in the criteria in Attachment 1 to Reliability Standard CIP-002-5.1a and as described in Section 2 of this report, High Impact Control Centers with operational control over Transmission or generation assets have significant spans of control or operate facilities central to reliable operations, whether due to their size (e.g., operational control of Transmission Facilities operated at 500 kV or 1500 MW of generation in a single Interconnection) or function (e.g., operational control of SPS, RAS, or automated switching Systems that operate certain BES Elements critical to operating within IROLs).

Given the size and types of BES assets operated from High Impact Control Centers, NERC's assessment of the potential impact of a physical attack on a High Impact Control Center with operational control over BES assets indicates that if such Control Centers were damaged, otherwise rendered inoperable, or seized by threat actors, there could be significant impacts to reliability, in some cases greater than the impact that could result if a critical

Transmission station or substation were attacked. For instance, if a High Impact Control Center performing the functions of a TOP has operational control of more than one Transmission station or substation, none of which are critical under Reliability Standard CIP-014-2, and is compromised as a result of a physical attack such that the TOP loses remote operational control of those substations, the adverse reliability impact may be at least as impactful as the loss of any single critical Transmission substation identified pursuant to CIP-014-2. Similarly, if a Control Center with operational control of 1500 MW of generation or more in a single Interconnection is damaged or destroyed as a result of a physical attack, it could remove or severely limit the ability to operate remotely those generation units and to respond to events on the system or otherwise ensure reliable operations.

Based on these findings, NERC will initiate its stakeholder processes to further evaluate and consider applying the controls required by the CIP-014 Reliability Standard to High Impact Control Centers that: (1) have operational control of BES Transmission or generation assets; and (2) if damaged, otherwise rendered inoperable or seized as a result of a physical attack, could result in instability, uncontrolled separation, or Cascading in an Interconnection. Depending on the nature of the BES assets operated by the High Impact Control Center, damage, inoperability, or seizing of that Control Center may not result in instability, uncontrolled separation, or Cascading in an Interconnection. For instance, if a Control Center performing the functions of a TOP is deemed High Impact only due to its operation of Transmission Facilities identified as essential to meeting Nuclear Plant Interface Requirements, damage to or the inoperability of that Control Center due to a physical attack may not cause such BES reliability impact. The controls required by CIP-004-6 and CIP-006-6 may be sufficient to protect against any such risks. NERC's stakeholder processes would help address these issues and ensure the CIP-014 Reliability Standard is properly scoped to focus resources on those facilities that require the additional protections afforded by that standard.

Backup Control Centers

As described above, in its petition for approval of CIP-014-1, NERC explained that it did not extend the scope of the CIP-014 Reliability Standard to Control Centers that provide back-up capability because if a physical attack damages or renders the backup Control Center inoperable, it would be unlikely to have significant adverse reliability impact in Real-time as the registered entity can continue operating its critical Transmission station or substation from the primary Control Center. In reassessing the scope of the CIP-014 Reliability Standard, however, NERC recommends that stakeholders further consider the need to apply the controls required by the CIP-014 Reliability Standard (specifically Requirements R4, R5, and R6) to High Impact Control Centers that provide backup capabilities to any primary Control Center subject to the standard. That is because many backup Control Centers mirror the operations of the primary Control Center and are kept operationally ready to assume operations at all times. If a backup Control Center is subject to a physical attack, it could have similar adverse reliability impact to that of the primary Control Center. If, for instance, the primary Control Center cannot be used whether due to a physical attack or otherwise, the backup Control Center becomes important for Real-time operations and, as such, may warrant the increased physical security required under CIP-014-2. Additionally, if the primary Control Center is destroyed and the backup Control Center assumes operational control over Transmission or generation assets, it is now the primary Control Center and should be subject to the physical security protections required by the CIP-014 Reliability Standard.

Section 6: Next Steps

NERC will initiate its stakeholder processes, including the Critical Infrastructure Protection Committee, to address the findings and recommendations in this report. Among other issues, NERC, through its stakeholder process, will seek to further identify those High Impact Control Centers that: (1) have operational control of BES assets; and (2) if damaged, rendered inoperable or seized as a result of a physical attack, could result in instability, uncontrolled separation, or Cascading in an Interconnection.

In addition, the ERO Enterprise will continue to emphasize the evaluation of physical security controls during compliance monitoring engagements, both under CIP-014-2 and CIP-006-6. Furthermore, the ERO Enterprise will conduct monitoring activities of registered entities with CIP-014 applicability to determine adequacy and appropriateness of resulting risk assessment methodologies and security controls. There are opportunities to improve the consistent and effective implementation of physical security controls considered by the CIP Reliability Standards for all High Impact Control Centers with operational control over BES Transmission or generation Facilities.

The security 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 ERO Enterprise will continue working with industry, both through the development of Reliability Standards, increased information sharing through the Electricity Information Sharing and Analysis Center, the development of security guidelines, and training exercises, among others, to enhance the security of the BES.