NATF Practices Document for NERC Reliability Standard CIP-014-2 Requirement R4

This document was submitted to NERC for consideration as compliance "Implementation Guidance" on 9/26/17. NERC will review and post a decision on its website.

Disclaimer

Open Distribution

Contents

Revisions

Date	Version	Notes
June 24, 2015	1.0	Original Version
September 20, 2017	2.0	Updated references to current standard (CIP-014-2). No technical content changes.

Section 1 Purpose

The purpose of this document is to provide a NERC Reliability Standard CIP-014-2 Requirement R4 practices guide containing an approach, common practices, and understanding for conducting evaluations of the potential threats and vulnerabilities of a physical security attack against a *Transmission station, Transmission substation, and/or a primary control center*.

Problem Statement

NERC CIP 014-2: Requirement R4 states:

Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following: [VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]

4.1. *Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);*

4.2. *Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and*

4.3. *Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.*

Scope

The purpose of this project was to develop approaches and/or common terminology and understandings that are defensible (but not prescriptive) for evaluation of potential threats and vulnerabilities as specified in CIP-014 Requirement R4. The final Requirement R4 Practices Guide includes a list of threats and tactics for consideration in determination of potential vulnerabilities when assessing a Transmission station(s), Transmission substation(s), and/or primary control center(s) identified under Requirement R1 and verified according to Requirement R2. The intent of the Requirement R4 Practices Guide is to assist NATF members in developing a best practices document to assist in the evaluation of the potential threats and vulnerabilities of a physical attack on a Transmission station(s), Transmission substation(s), and/or primary control center(s).

Section 2 Definitions

Glossary of NERC-Defined Terminology

Cascading – The uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption that cannot be restrained from sequentially spreading beyond an area predetermined by studies.

Electric Reliability Organization (ERO) – NERC is the electric reliability organization for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.

North American Electric Reliability Corporation (NERC) – A not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system 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's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people.

Team-Recommended Terminology

Aggressor – Any internal or external person or group intending to, planning on, or committing an attack on a Transmission station(s), Transmission substation(s), and/or primary control center(s).

Assessment – Evaluation, judgment, measurement, review, consideration, opinion.

Design Basis Threat (DBT) – The design basis threat for purposes of this document should include aggressor tactics and capabilities with consideration of "Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. Federal and/or Canadian governmental agencies, or their successors."

Risk – Danger, threat, hazard. For purposes of this document a risk is the probability of peril to a Transmission station, Transmission substation, or a primary control center.

Risk Assessment – The systematic process of evaluating the potential risk that may be involved in a projected activity.

Risk Assessment of Facilities – The systematic process of evaluating potential threats and vulnerabilities of a location or facility.

Tactic (the "how") – Action or strategy planned to achieve a specific end. For purposes of this document, the tactic is the "how" action(s) of the attack.

Threat – The intent to conduct harm or capitalize on an actual or perceived vulnerability that could result in damage, destruction, or loss of life or property.

Threat and Vulnerability Assessment (Physical Attack) – The systematic process of evaluating, identifying, quantifying and prioritizing threats, vulnerabilities or security weaknesses to determine the potential or projected risk to identified assets such as Transmission station(s), Transmission substation(s), and primary control center(s).

Vulnerabilities – A weakness, or a gap, that can potentially be exploited by a threat.

Section 3 Guide

Requirement and Threat

Requirement R4 - *"Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission* Owner *according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2." The threat and vulnerability evaluations shall include the following attributes:*

The primary focus of the threat and vulnerability evaluation under Requirement R4 is the potential tactics, rather than the motivation of the aggressor. An aggressor's likely motivation may be to impact the reliability of the Bulk Electric System by rendering a Transmission station(s), Transmission substation(s), and/or primary control center(s) inoperable or damaged as a result of a physical attack which could result in uncontrolled separation, or Cascading within an Interconnection. However, a simple act of copper theft may also have unintended consequences to the reliability of the Bulk Electric System.

Tools and Methods

T**here are numerous evaluation and assessment tools** that can identify site strengths and weaknesses of the Transmission station(s), Transmission substation(s), and primary control center(s) identified under Requirement R1.

Most of these evaluation and assessment tools assign a numerical value that is placed in a decision matrix to identify the likelihood of a target or component being chosen. These tools can be used to readily identify specific components that may warrant additional protection and thus lower risk to the substations and primary control centers. Assuming an entity owns/operates more than one facility that is deemed critical under CIP-014-2, the decision matrix may also provide insight as to which facilities may be at greater risk due to the identified vulnerabilities and thus can be used to prioritize the order in which the facilities are addressed.

The first steps toward satisfying Requirement R4 will be to characterize/identify:

> **4.1.** Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s)"

An evaluation of the site-specific characteristics, combined with potential threats and tactics, allows the owner/operator to consider and apply mitigations to better protect assets. The threat and vulnerability evaluation should be a risk-based, decision-making process. Using the results of the asset, threat, and vulnerability assessment, risk can be determined. The physical security evaluation checklist in Appendix 2 will assist in identification of site-specific characteristics.

The goal of a physical attack threat and vulnerability evaluation is to identify weaknesses to which mitigations can be applied in an attempt to harden and protect specific targets from the aggressor's hostile attacks. Mitigations include physical security, risk-management, redundancy, resiliency, and/or response.

The evaluation should first identify the site components or assets that are considered critical and essential to the facility being evaluated and determine the criticality of each component or asset. Identified critical components or assets should be prioritized based on the vulnerabilities or weaknesses they pose to the facility to determine which component or asset may warrant additional mitigation or protection. This systematic process requires assessment of each component or asset with regard to human resources and infrastructure needs.

It may be beneficial for the Requirement R4 threat and vulnerability evaluation findings to be shared with the Requirement R1 evaluation assessment team for consideration in future threat and vulnerability assessments. Requirement R1 assessors should have a clear understanding of the potential operational state that a substation or primary control center would likely be in after an attack. The nature of the failure mode, method of attack, or tactic utilized may impact the control center's ability to take equipment offline in a controlled manner, which in some cases may avoid a total loss of the asset.

If the risk is to be addressed, mechanisms such as spare components, operational-response plans, physical-response plans, and/or the capability to rebuild the lost asset within a reasonable amount of time could be considered acceptable mitigations to the risk. Response and resiliency measures to offset threats and vulnerabilities should be considered in the Security Plan.

Threats and vulnerabilities should be viewed as potential occurrences with adverse intent that will affect the operability of the targeted location. The evaluation results should be derived from a systematic survey approach that considers physical, informational, operational features/assets and include threats to the building or structure. The evaluation should identify and prioritize potential threats and vulnerabilities.

When prioritizing critical stations or primary control centers that require mitigation measures, consideration should be given to the following:

- Preservation of life
- Cascading, uncontrolled, or successive loss of system elements triggered by an incident at any location
- Cascading resulting in widespread electric service interruption that cannot be restrained from spreading beyond an area predetermined by studies
- Time and cost to repair the would-be target
- Long lead-time equipment

Additionally, various levels of risk impact should be considered; for example:

- Damage to critical components or assets within the owner’s/operator’s system resulting in unscheduled downtime affecting the operation of a facility for a manageable, temporary period of time.
- Damage to critical components or assets within the owner’s/operator’s system that is more extensive, with both temporary and permanent impact to components or assets and reliability.
- Damage to critical components or assets within the owner’s/operator’s system that could potentially result in unscheduled downtime that has a cascading effect with potentially devastating consequences felt well beyond the owner’s/operator’s system. The resulting damage and losses may have far-reaching implications. Unscheduled downtime may potentially threaten public

safety, financial stability, and regulatory compliance, and/or reliability to interconnected transmission systems.

Appendix 1 – Site Specific Vulnerability Considerations

SITE-RELATED VULNERABILITY CONSIDERATIONS
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
Historical events that have occurred at similar facilities nationwide and the proximity of these events to the facility being assessed
PROCEDURAL AND PERSONNEL VULNERABILITIY CONSIDERATIONS
Lack of significant/high-value replacement components necessary for facility functionality may be impactful financially, resulting in an extended facility outage and a reduction in BES reliability
Lack of secured off-site storage for significant/high-value spare components
Gaps in or lack of security mitigations (physical and human)
Gaps in or lack of physical security policies and procedures, or failure to enforce them. This would include visitor and tour restrictions (prohibited areas, who can authorize, hours permitted, key / access management, security device testing, etc.)
Gaps in or lack of "use of" policies or procedural controls for vehicles, identification badges, keys, uniforms, personal protective equipment (PPE) that could be used to gain access or "blend in"
Staffing (or lack of) / hours
FACILITY VULNERABILITIY CONSIDERATIONS
No locks on switchgear and breaker cabinets, or other access-restricting hardware
No protection of facility service (monitoring of primary, secondary station service, and lock on facility main breaker)
Existing methods to deter, detect, delay, analyze, and respond to aggressor attacks
Terrain
Distances from features such as trees, hills, tall buildings with windows, etc.

Physical barriers and other natural means to inhibit or control access. Fences, vehicle barrier systems, large rock, etc. (Be aware of local restrictions on fences and other barriers. If present, note ways to defeat barriers.)
Document the stand-off distance between the perimeter fence and critical components, such as transformers and control houses
Identify what access is authorized, and how it is granted. If access is shared with outside entities, consider this process as well. (Also note ways to defeat authorization.)
Overall culture of security
Vehicle and pedestrian pathways
On-site personnel

Aggressor and Tactic Considerations

For purposes of this document, risk-based target identification is the process of considering the probability of an aggressor attack, and the potential impact of loss to thus identify and prioritize assets and components as potential targets. Using this methodology, mitigations may be considered or utilized on a scale to the probability of the threat, and the consequence of loss or destruction of the asset.

As with vulnerabilities to facilities, aggressors and their motivations may vary from site to site. Consideration should be given to aggressor propensity on a site-by-site basis. The tables below may be of assistance in considering what may be applicable at certain locations and adapted for others.

When assessing the path and methods of entry or access to a Transmission station, Transmission substation, or a primary control center, consideration should be given to the overall area surrounding the facility and the approach paths.

POTENTIAL AGGRESSORS - Scale of likelihood (Low/Med/High, which will change over time) for consideration
Criminal (gangs, drug groups, organized crime)
Domestic terrorist
Rogue/lone wolf
Insider
International terrorist
Environmental extremist
POTENTIAL AGGRESSORS - Wider-scale consideration
Consideration of events of national interest
Concerning industry trends, construction, developing threats, etc. that modify the threat and/or vulnerability
Proximity to groups suspected of disruption event plans or history
POTENTIAL METHODS OF ACCESS

Forced
Duress
Surreptitious
Deceit - feigning a legitimate function to blend in to gain access or information
Granted access - internal, valid access, social engineering
Vehicle/ATV
Waterway
Air - throwing items/devices, drone, plane, helicopter
Subterranean - cable path, manhole, sewer, service tunnel
TACTICS & OTHER ISSUES FOR CONSIDERATION
Insider threat / misuse of knowledge
Misuse of / failure to protect information from compromise
Active shooter / intentional direct fire, sniper intentional fire; direct or arc trajectory - line of sight ballistics
Indirect fire / or collateral damage ballistics resulting in unintended damage (e.g., hunting)
RPG, mortars, propelled IEDs
Physical attack and/or incident that would require an emergency response by law enforcement or facility personnel at an alternate location that could divert responders and result in a delay to an emergency response to a primary site
Staged incident that would delay an emergency response to a facility (e.g., protestors or other types of aggressors blocking access routes)
Sabotage
Equipment vandalism
Tannerite
VBIED
IED: backpack, pipe bomb, package, etc.
Electrical fault
Arson
Drones / airplanes (as a tactic with or without an IED)
Simultaneous attacks at multiple locations to impact the bulk electric system
IP and wireless security devices can be hacked and blocked

Render primary control centers and/or critical substation control houses inoperable or uninhabitable by impacting facility: • Station service (primary, secondary, & breakers) • HVAC systems • Fire • Communications • Water • Sewer
Power supplies and head-end panels for security devices should be protected (primary and secondary power).
Any other incident that would require an emergency response by law enforcement or facility personnel not covered above

Consideration of Environmental Concerns

Although random and unpredictable, factoring in environmental concerns may be beneficial when considering risks and potential mitigations. Certain mitigations may actually cause risk when coupled with environmental concerns, such as floods, hurricanes, tornado, and ice. For example, a formidable ballistics wall that is constructed in a tornado prone area may be more likely to result in an outage than a ballistics threat.

Appendix 2 - Physical Security Evaluation Checklist

PHYSICAL SECURITY EVALUATION CHECKLIST	
Section	Title
1.0	Facility Information
2.0	Personnel Information
3.0	Facility Maintenance Contact
4.0	Operations / Primary Contact
5.0	Facility Executive / Director Contact
6.0	Utility Information
7.0	First Responders
8.0	First Responders Interaction
9.0	Emergency Operations
10.0	Security Management
11.0	Response
12.0	Security Force
13.0	Natural Hazards
14.0	Fence / Perimeter
15.0	Site / Perimeter
16.0	Building Envelope
17.0	Utility Systems
18.0	Mechanical Systems
19.0	Electrical Systems
20.0	Fire Alarm Systems
21.0	Security Systems
22.0	Communication Systems
23.0	Information Technology Systems
24.0	Sensitive Material/Equipment
25.0	Security Plan & Historical Site Occurrences

1.0 Facility Information	
Facility Name	
Other facility names or aliases	
Facility Type (if substation list kV)	
Is this a shared facility with another utility company? If so, who? (Add contact for each)	
Address of facility (nearest intersection and landmarks if no physical address) If this address is NOT the 911 address (if applicable), list the 911 address here:	Site address _____ Driving directions from intersection, or site address if needed (e.g. ¼ mile east of gate at this address): _____ _____ _____ 911 address: _____
Latitude/Longitude *(Decimal format preferred)*	Latitude: ____ Longitude: ____
Facility Phone Number	
General Facility Description	Describe: _____ _____

What are the operating hours of this facility?	☐ No personnel assigned / on site as needed ☐24 / 7 / 365 ☐24 / 7 / closed for some days during the year ☐24 / less than 7 days a week ☐Less than 24 hours a day, 7 days per week ☐Less than 24 hours a day, less than 7 days per week
What is the estimated occupancy of the facility during normal working hours?	
2.0 Personnel Information	
How many people have unescorted access to the facility?	
Are employees and contractors required to possess appropriate security clearances and approval for accessing critical areas?	
Are reviews of access authorization requests and revocation of access authorization conducted for restricted areas?	
Are all employees and contractors required to sign in and sign out on a building register, or through electronic means?	
Is all personal electronic access disabled in accordance with policy and procedure when access credentials are lost, stolen, or when terminated etc.?	

How frequently is the list of individuals with unescorted physical access audited?	
Are employees encouraged and/or instructed to challenge strangers in their work area?	
Are security posters and signage displayed at the facility?	
Are all employees provided with annual security awareness training?	
Are identification badges issued to all employees and contractors entering the site/facility?	
Is the facility open to the public, including for meetings, tours, etc.?	
Does the site provide separate entrances for employees & visitors so visitors may be properly logged in? Describe process.	
Are visitors required to present identification prior to gaining access to the facility?	
Do employees and visitors wear visibly displayed company-issued identification badges at all times when on site?	
Are site visitors escorted by authorized personnel with unescorted access?	

Are visitors required to manually or electronically log in and be escorted into critical or restricted areas?	
Are the electronic logging devices (card readers) and/or manual logs located outside the critical or restricted areas?	
3.0 Facility Maintenance Contact	
First Name	
Last Name	
Title	
Company	
Phone	Office: _____ Other: _____
Email	
Same as Primary Facility Contact ☐Yes ☐No	
4.0 Operations / Primary Contact (may be different than Primary Facility Contact)	
First Name	
Last Name	
Title	
Phone	Office: _____ Other: _____
Email	
5.0 Facility Executive / Director Contact	
First Name	
Last Name	
Title	
Company	
Phone	Office: _____ Other: _____
24 Hour Contact	
Email	
6.0 Utility Information	

Gas / Propane if applicable (replicate as needed)	
First Name	
Last Name	
Title	
Company	
Phone	Office: _____ Cell: _____ Other: _____
24 Hour Contact	
Email	
Communication (replicate as needed)	
First Name	
Last Name	
Title	
Company	
Phone	Office: _____ Cell: _____ Other: _____
24 Hour Contact	
Email	
Electric (replicate as needed)	
First Name	
Last Name	
Title	
Company	
Phone	Office: _____ Cell: _____ Other: _____
24 Hour Contact	
Email	

Utility Information Continued	
Water (replicate as needed)	
First Name	
Last Name	
Title	
Company	
Phone	Office: _____ Other: _____
24 Hour Contact	
Email	
Other Utility Contact - (replicate as needed)	
First Name	
Last Name	
Title	
Company	
Phone	Office: _____ Other: _____
24 Hour Contact	
Email	
7.0 First Responders	
First Responders – Law Enforcement (replicate as needed)	
First Name	
Last Name	
Company / Agency	
Title / Position	
Phone	Office: _____ Other: _____
Email	
First Responders – Fire Department (replicate as needed)	
First Name	
Last Name	
Company / Agency	
Title / Position	
Phone	Office: _____ Other: _____
Email	
First Responders – Emergency Medical (replicate as needed)	

First Name	
Last Name	
Company / Agency	
Title / Position	
Phone	Office: _____ Other: _____
Email	
8.0 First Responders Interaction	
Law Enforcement Agency Name	
Have there been onsite visit(s) with this first responder?	☐No ☐Yes (note date / purpose here)_____
Fire Response Agency Name	
Have there been onsite visit(s) with this first responder?	☐No ☐Yes (note date / purpose here)_____
Emergency Medical Agency Name	
Have there been onsite visit(s) with this first responder?	☐No ☐Yes (note date / purpose here)_____

9.0 Emergency Operations	
Does the facility have a written Emergency Operations Plan?	☐No ☐Yes If yes, the plan is developed at the: ☐Corporate-level ☐Facility-level Has the plan been approved by senior management? ☐No ☐Yes Has the plan been coordinated with local law enforcement? ☐No ☐Yes If yes, is it reviewed annually with local law enforcement? ☐No ☐Yes Are key personnel aware of and do they have access to a copy of the plan? ☐No ☐Yes Are personnel trained on the plan? ☐No ☐Yes

Emergency Operations Continued	
Does the facility have a written Emergency Operations Plan?	Is the plan exercised at least once a year? ☐No ☐Yes If yes, these exercises are: ☐Tabletop (practical or simulated exercise) ☐Functional (walk-through or specialized exercise) ☐Full scale (simulated or actual event) Are exercise results documented, approved, and reported to executive management? ☐No ☐Yes Does the plan address situations such as evacuation or shelter in place procedures, fire, facility under attack, weather event, etc.? ☐No ☐Yes *If applicable, consider attaching a copy of the Emergency Operations Plan(s) – or indicate file path or SharePoint location of the document.

10.0 Security Management	
Does the facility have a written security plan?	☐No ☐Yes *If yes,* The plan is developed at the: ☐Corporate-level ☐Facility-level Has the plan been approved by senior management? ☐No ☐Yes Has the plan been coordinated with emergency responders? ☐No ☐Yes If yes, Is it reviewed annually with emergency responders? ☐No ☐Yes Are key personnel aware of and do they have access to a copy of the plan? ☐No ☐Yes ☐Full scale (simulated or actual event)

Security Management Continued	
	Are personnel trained on the plan? ☐No ☐Yes Is the plan exercised at least once a year? ☐No ☐Yes If yes, these exercises are: ☐Tabletop (practical or documentation exercise) ☐Functional (walk-through or specialized exercise) Are exercise results documented, approved and reported to executive management? ☐No ☐Yes
11.0 Response	
Does the Security Operations Center receive calls and determine appropriate response measures for this site?	
Has the asset owner identified a designated official(s) responsible to take specific actions for an emergency response to the facility?	Officials may include: outside emergency responders, onsite/corporate security, employees/contractors. Actions may include: notifications, physical response, operational actions

Have plans been developed for response to alarms and incidents?	

12.0 Security Force	
Does the facility have a security force?	☐No ☐Yes If yes, Onsite security force ☐No☐Yes Roving patrol (interior / exterior)? (Describe.) ☐No☐Yes _____ _____ Offsite security force **only** (no onsite force) ☐No☐Yes If yes to either onsite or offsite security force: Is there a Supplemental Capacity Plan? ☐No☐Yes *If yes,* Supplemental Capacity Plan has the following Personnel: ☐None ☐Law Enforcement (Contract/Off-duty) ☐Contracted Security ☐Other organization/corporate Arrest Authority ☐No☐Yes Detain Authority (define) ☐No☐Yes

Standard operating procedures / post orders? Describe post locations and hours of operation. Indicate the date that the post orders were last reviewed or updated and the sufficiency of the post orders.	☐Yes ☐No	
Are employee entrances to physical security perimeters controlled by security officers during business hours?	☐Yes ☐No	
Are employee entrances to physical security perimeters controlled by security officers after business hours?	☐Yes ☐No	
During what hours (if any) are fixed security officers posted at the <u>perimeter</u> to challenge and identify persons prior to accessing the site?	Define:	
Specify the equipment available to the security force	Uniformed ☐No ☐Yes Armed (i.e., gun) ☐No ☐Yes	Restraints ☐No ☐Yes

	Less than Lethal Weapons ☐No ☐Yes *If yes, complete the following* ☐Taser ☐Chemical Repellant ☐Collapsible ☐Baton/Baton Stun Gun	Communications: ☐No ☐Yes *If yes, complete the following* ☐ Radio - secure and continuously monitored ☐Cell Phone ☐Duress Alarms / "Panic" Buttons
	Body Armor ☐No ☐Yes	Canine Patrols ☐No ☐Yes
13.0 Natural Hazards		
Is the facility located in an area that experiences any of the following natural hazards? Check all that apply	☐ **Earthquake** Does the facility have deployable mitigation measures for this specific hazard? ☐No ☐Yes Describe:	
Is the facility located in an area that experiences any of the following natural hazards?		

Is the facility located in an area that experiences any of the following natural hazards? Check all that apply	☐ **Flood** Does the facility have deployable mitigation measures for this specific hazard? ☐No ☐Yes Describe: ☐ **Hurricane** Does the facility have deployable mitigation measures for this specific hazard? ☐No ☐Yes Describe: ☐ **Lightning strikes** Does the facility have deployable mitigation measures for this specific hazard? ☐No ☐Yes Describe: ☐ **Severe winter storms (ice/snow)** Does the facility have deployable mitigation measures for this specific hazard? ☐No ☐Yes Describe: ☐ **Tornado** Does the facility have deployable mitigation measures for this specific hazard? ☐No ☐Yes Describe: ☐ **Wildfire** Does the facility have deployable mitigation measures for this specific hazard? ☐No ☐Yes Describe: ☐ **Other natural hazards:** Does the facility have deployable mitigation measures for this specific hazard? ☐No ☐Yes Describe:

14.0 Fence / Perimeter	
Does the facility have fencing?	☐No ☐Yes *If yes, score the rest of this section for the weakest section of fence.*
Percentage Enclosed	☐100% of the facility enclosed AND 100% Significant asset(s) are enclosed ☐Less than 100% of the facility enclosed, BUT 100% Significant asset(s) are enclosed ☐100% of the facility enclosed, BUT less than 100% Significant asset(s) are enclosed ☐Less than 100% of the facility enclosed AND less than 100% Significant asset(s) are enclosed

Other fence characteristics	
Is the area free of objects / structures that would aid in traversing the fence (trees, sheds, barrels, etc.?)	☐Yes ☐No
Is there a clear zone? (*An area inside or outside the perimeter that allows for clear sight of fence perimeter, e.g., no vegetation or objects, no privacy slats).*	☐Yes ☐No
Fence is clearly marked with visible, well-placed "warning" signs.	☐Yes ☐No
Is there signage in place on or near the perimeter of the facility that defines: Ownership boundaries?	☐Yes ☐No Describe:

Fence / Perimeter Continued

Private property		☐Yes ☐No	
No trespassing		☐Yes ☐No	
Emergency response address		☐Yes ☐No	
Fence Characterization *(Check all that apply)* *(Identify the weakest portion of fence, if type varies)*	**Type** ☐Chain link ☐Anti-Climb Aluminum or steel ☐Standard Aluminum or steel ☐Other – not chain link ☐Concrete ☐Brick and Mortar ☐Steel ☐ Wrought Iron ☐ Wood ☐Plastic	**Height** ☐Less than or equal to 5 ft. ☐5+ ft. – 6 ft. ☐6+ ft. – 7 ft. ☐7+ ft. – 15 ft. ☐Greater than 15 ft. **Base of fence** ☐Anchored ☐Not anchored ☐N/A (e.g., concrete or brick/mortar wall)	**Enhancements** ☐K-rated for vehicle penetration ☐Second Fence ☐Electric Fence ☐Aircraft Cable/Vehicle restraint cable with reinforced anchor points ☐Coiled razor wire ☐Coiled barbed wire ☐Spikes ☐Privacy screening ☐None
Other / Specify: _____ _____			

15.0 **Site / Perimeter**

Are any projects currently scheduled for the facility? (Security enhancement projects, outages, capital improvement, etc...) Describe the nature and scope of the project.	
Does the facility have site identified hazardous material stored on site?	

Where is HAZMAT storage located and how is it controlled?	
Is HAZMAT storage located in an area away from loading docks, entrances, uncontrolled parking, transformers, control houses, and other critical assets?	
What major structures surround the facility?	
How many vehicle access points are at the site?	
Describe the locations of the vehicle access points.	
Are there a sufficient number of readily available vehicle barriers to deploy if/when needed at vehicle entry points to facility?	
Does the site have designated/ assigned parking areas? Describe. Are there designated/approved visitor parking areas? Are there designated/approved contractor parking areas? Describe. Are there designated/approved employee parking areas? Describe.	

Is unauthorized access to contractor parking areas restricted? Is unauthorized access to employee parking areas restricted?	
Are there sufficient fences, walls, gates, or other barriers to prevent unauthorized access to restricted areas? If yes, describe the condition. If no, identify the vulnerabilities to the perimeter barriers and or fencing.	
What are the existing types of anti-ram devices for the facility?	
Indicate and identify the location and number of all access controlled gates at the facility.	
Indicate the minimum number of gates that would be required to meet operational needs.	
Identify the location of any gates that could be eliminated.	

Does the facility or significant asset(s) have a high-speed avenue(s) of approach?	
What is the anti-ram / buffer zone / standoff distance from vehicle traffic or parking areas to the asset?	
Are perimeter barriers capable of stopping vehicles? Describe and include the rating in known:	
Does site circulation prevent high-speed approaches by vehicles?	
Are there offsetting vehicle entrances from the direction of a vehicle's approach to force a reduction of speed?	
Is there space for inspection at the curb line or outside the protected perimeter? What is the minimum distance from the inspection location to the building?	
In dense, urban areas, does curb lane parking place uncontrolled parked vehicles unacceptably close to a facility in public rights- of-way?	
Is there a minimum setback distance between the building and parked vehicles?	

Does the site implement stand-off, hardening, and/or blast venting methods to protect critical areas at entrances, personnel locations, and uncontrolled parking? If so, describe.	
Do standalone, above ground parking facilities provide adequate visibility across as well as into and out of the parking facility?	
Is landscaping maintained to prevent obstructing views of first responders and employees?	
Does site landscaping provide hiding places?	
Is the site lighting (where utilized) sufficient to identify threats, and ambient enough to eliminate bright and dark areas?	
Is landscaping maintained to prevent obstructing views of the CCTV cameras, or interfering with lighting, intrusion detection, or vehicle and human observation?	
Do signs provide control of vehicles and people?	
Are trash containers, mailboxes, vending machines, or other fixtures that could conceal explosive devices positioned away from the building?	
Is there an auxiliary lighting system?	

Is there a procedure/policy to identify and act on unauthorized extended-stay vehicles (e.g., reporting to security, LLE, or tow company)?	
Consideration should be given if the facility is publicly visible and identifiable as to its purpose and/or other critical infrastructure, or provides service to U.S. government facilities.	
3. Identify unique characteristics of the site that may increase the likelihood of a physical attack. Provide specific details: ☐ Urban Area ☐ Extreme Rural Area ☐ Location – Lack of timely response by Law Enforcement Personnel ☐ Geography - Limits ability to implement ballistic protections throughout ☐ Surrounding Properties - Limited Set back and/or Buffer Zone - Urban ☐ Surrounding Properties - Limited Set back and/or Buffer Zone - Rural ☐ Other	

Do any known security issues not previously addressed exist at the facility? Describe the issue(s) in detail.	
16.0 Building Envelope	
How many buildings of operational significance are located on the facility?	
Identify each building and its operational function.	
What type of construction? What type of concrete? What type of steel? What type of foundation?	
Is it a mixed-tenant facility?	

Are public toilets, service spaces located in any non-secure areas, including the queuing area before screening at the public entrance?	
Are facility-critical areas, including electrical, telephone/data, fire and alarm systems, water mains, HVAC systems, located a sufficient distance from loading docks, receiving, shipping areas?	
Are all incoming mail and packages screened using X-ray located in isolated, external, or off-site mail receiving facility? Adequate training on detection of suspicious packages?	
Does the site receive mail, parcels, equipment, tool, or construction material deliveries?	
Are mailrooms located away from facility main entrances, areas containing critical services, utilities, distribution systems, and important assets? Does the mailroom have adequate space for explosive disposal containers? Is the mailroom located near the loading dock?	
Is space available for equipment to examine incoming packages and for special containers?	
Are there trash receptacles and mailboxes in close proximity to the facility that can be used to hide explosive devices?	

Is roof access limited to authorized personnel by means of locking mechanisms?	
Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur?	
Have fire exits or escape points been designed and clearly marked?	
Does the facility sit above underground facilities not within the facility's control (e.g., utility tunnel, pedestrian tunnel, subway tunnel)?	
Are there any unsecured penetrations / trenches that lead from outside the fence that lead to the inside of the fence?	
Are there any unsecured penetrations / trenches that lead from outside the fence to the inside of the control house / protected assets (cable vaults and drainage)?	
Are there any unsecured penetrations/paths that lead from outside the primary control center to the inside of the primary control center (interior or exterior access)?	

Penetrations could allow tactics to impact the operability of the transmission substation or primary control center. Describe in detail how the tactics could apply, or how access may be gained. For examples, refer to the tactics list included in the CIP 014-2 Requirement R4.	
To what level are the exterior walls designed to provide less than a high-hazard response? Are the walls capable of withstanding the dynamic reactions from the windows?	
Are the windows systems design (glazing, frames, anchorage to supporting walls, etc.) on the exterior facade balanced to mitigate the hazardous effects of flying glazing following an explosive event? Is the glazing laminated or is it protected with an anti-shatter film?	
Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected? Will the anchorage remain attached to the walls of the facility during an explosive event without failure? Is the façade connected to backup block or to the structural frame? Are non-bearing masonry walls reinforced?	
Consideration should be given to ground level or other permanent fixtures when installing security screening or window glazing treatments to reduce forced entry and/or glass fragmentation on any windows. Describe your methodology.	

Do windows in critical areas prevent visual observation from the exterior into critical areas?	
Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection as the exterior wall?	
Are all accessible exterior windows that do not have some other form of protective measure monitored by an intrusion detection system?	
Indicate the number of exterior windows that do not have some other form of protective measure that would require monitoring by an intrusion detection system.	

Are doors constructed of a sturdy and solid material, functioning optimally?	
Are perimeter doors secured with properly working locks?	
Are all perimeter or critical door hinges installed on the secure side of the door OR do any external hinges have non-removable hinge and/or security pins?	
Are emergency exit doors for occupied buildings (such as primary control centers) secured using an automatic door closer and/or have exit hardware that is compliant with applicable life safety codes and standards?	
Does the site use delayed egress hardware at emergency exits? NOTE: This type of hardware prevents a door from being opened from the egress side, usually for a period of 15 seconds. These exits must have signs posted with instructions, have an audible alarm when the delayed egress is activated, release immediately with a fire alarm or loss of power, meet occupancy requirements, and the building must have a supervised automatic fire detection system.	
Characterize the weakest ceiling / roof for the facility.	

17.0 Utility Systems	
Is potable water required for this facility? If so, what is the source of domestic water?	
Are there multiple entry points for the water supply?	
Is the incoming water supply in a secure location?	
Does the facility have storage capacity for domestic water? How much?	
If the facility has a water extinguishing fire suppression system, what is the source of water?	
Are sewer systems protected? Are they accessible?	
What fuel supplies does the facility rely on for critical operation?	
How much fuel is stored on the facility (list as hazmat)? How is it stored?	
What is the normal source of electrical service for the facility?	
How many service entry points does the facility have for electricity?	
What provisions for emergency power exist?	

If a generator is utilized: Identify diesel / other fuel under the Hazmat section. Has the emergency generator been secured against unauthorized access? How is the emergency generator secured to prevent unauthorized access? Is the generator located at least 25 feet from any vehicle entrance or parking area? Is the standby or emergency equipment tested periodically?	
Is the incoming electric service to the building secured from tampering?	
Does the fire alarm system require communication with external sources?	
By what means does the main telephone and data communications interface the facility?	
Are there multiple or redundant locations for the communication service?	
Is external natural gas required for facility core operations?	
How many natural gas service connections are there for the facility?	

Are natural gas services connections into the facility located above ground or buried?	
Are components of the natural gas supply located inside the building (within control of facility) and protected from vandalism or accidental damage?	
Are components of the natural gas supply located outside of the building (but still within control of facility) protected from vandalism or accidental damage?	
18. Mechanical Systems	
Where are the air intakes and exhaust louvers for the building?	
Are there multiple air intake locations?	
Are there large central air handling units or are there multiple units serving separate zones?	

Is the air supply to critical areas compartmentalized?	
Are the controls for the air handling system in a secure area?	
Does the site use a minimum Efficiency Reporting Value (MERV) 10 particulate filter on all air handling units to include the supply air stream for re-circulation? HVAC isolation switch?	
Is there a one-step shut off for air handlers? If so, where is the shut-off?	
19.0 Electrical Systems	
How are the electrical rooms secured?	
Are critical electrical systems collocated with other building systems?	
Are electrical distribution panels secured or in secure locations?	
What is the extent of the external facility lighting in utility and service areas?	
20. Fire Alarm Systems	
Is the facility fire alarm system centralized or localized?	
Where are the fire alarm panels located?	

Is the fire alarm system standalone or integrated with other functions such as security and environmental systems?	
Does activation of the fire alarm unlock doors permitting free ingress and egress?	

21. Security Systems	
Is there a process to request the installation of new security equipment?	
Does the site have a CCTV system installed?	
Does the site have CCTV coverage viewable on the corporate network and monitored by the security operations center?	
Does the site have CCTV coverage on primary vehicle entrances?	
Indicate the number of vehicle entrances/exits and how many would require CCTV coverage.	
Is there CCTV coverage for the entire facility perimeter? If not, indicate the percentage of perimeter coverage with 1 being 10% and 10 being 100%	
Is there CCTV coverage for parking areas?	

If not, indicate the percentage parking area coverage with 1 being 10% and 10 being 100%.	
Are all access control points into critical areas monitored by CCTV?	
If not, indicate the number of accesses into critical areas that do not have CCTV coverage.	
Are all access points into critical areas from hatches or from the roof or top deck monitored by CCTV? If access points exist, answer "yes." Indicate the number of access points and include additional details.	
If not, indicate the number of hatches or rooftop access points into critical areas that do not have CCTV coverage.	
What is the number of fixed, wireless, and pan-tilt-zoom cameras used? Who are the manufacturers of the CCTV cameras? What is the age of the CCTV cameras in use?	
Is there a process to request service or maintenance for security devices?	
Are records maintained on all security deficiencies?	
Are security deficiencies tracked until they are closed?	

Are the cameras programmed to respond automatically to perimeter / building alarm events? Do they have video motion capabilities?	
Are panic/duress alarm sensors used? If yes, where are they located and are they hardwired or portable?	
Are intercom call-boxes used in parking areas or along the building perimeter?	
Are the perimeter cameras supported by an uninterrupted power supply source: battery or building emergency power?	
What is the quality of video images both during the day and hours of darkness? Are infrared camera illuminators used?	
What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?	
What type of camera housings are used, and are they environmental in design to protect against exposure to heat and cold weather elements?	
Who monitors the CCTV system?	

Does the security operation center receive and assess alarms to determine appropriate response measures as needed?	
Have instructions been developed for responding to intrusion alarms and are they correctly reflected in the alarm instructions within the security operation center(s)? Indicate the last revision date and / or accuracy.	
Are there intrusion detection system alarms on the entire outermost securable perimeter?	
Indicate number of perimeter access portals on the outermost securable perimeter that are not equipped with appropriate alarms for the location/environment. Identify their locations in the comments.	
What type of intrusion detection sensors is used? For example: electromagnetic, fiber optic, active infrared, microwave, seismic, photoelectric, ground, fence, glass, break (vibration/shock), single, double and roll-up door magnetic contacts or switches.	

Is Global Positioning System (GPS) technology used to monitor asset movements?	
Are facility personnel notified of an intrusion alarm? How is the notification made?	
Are the cameras supported by an uninterrupted power supply source: battery or building emergency power?	
Are camera video images of good visual and recording quality?	
Do the camera lenses used have the proper specifications, especially distance viewing and clarity?	
Is there a security photo identification badge processing system in place? Does it work in conjunction with the access control system or is it a standalone system?	
Do all perimeter doors have intrusion detection alarms that are monitored by the security operations center? (If not, document needs)	
What type of interior intrusion detection system sensors is used: electromagnetic, fiber optic, active infrared-motion detector, photoelectric, glass break (vibration/shock), single? Double and roll-up door magnetic contacts or switches?	

Is there a security asset tracking system in place that monitors the movement, control, and accountability of assets within and removal from a facility (e.g. electronic tags, bar codes, wire, infrared/black light markings, etched or chemical embedded id number, etc.)?	
What is the backup power supply source(s) for the access control systems: battery backup or some form(s) of other uninterrupted power sources?	
What access control system equipment is used?	
How old are the systems and what are the related first and maintenance service costs?	
List any cameras, panic alarms, or other devices currently installed and monitored to protect critical internal areas / operations / operations personnel.	
Is the security system designed to be tamper resistant?	
Is access into critical areas from the roof or top deck secured using intrusion detection systems? Describe.	

Are mechanical, electrical, power supply, voice/data telecommunication system nodes, security system panels, elevator, and critical system panels, and other sensitive rooms continuously locked, under electronic security CCTV camera and / or intrusion alarm systems surveillance to prevent unauthorized access?	
Is new security equipment tested prior to activation?	
Who tests the security equipment?	
Is there a preventative maintenance or testing program for all security system components that ensures such equipment is maintained, repaired, or replaced as needed?	
Is there uninterruptible emergency power for essential electronic security systems to allow for continuous operation? If so, describe	
Does the site maintain a formal key management program?	
Who is responsible for key management and the authorized release of them?	
How are keys made, issued, and accounted for?	
Does the key control officer have overall responsibility for issuance and replacement of locks and keys?	

Are keys issued only to authorized personnel?	
Are locks changed upon loss or theft of keys?	
Are current records maintained indicating a clear record of buildings and/or entrances for which keys are issued?	
Are current records maintained indicating a clear record of location and number of master keys?	
Are current records maintained indicating a clear record of location of locks and keys held in reserve?	

Does this facility utilize key boxes that store a site key outside the building or facility (e.g., Knox key safe or simple key box for convenience)? If so, does it have a tamper switch or other monitoring? Explain:	
Are current records maintained indicating a clear record of time of issue and return of keys?	
Are records maintained for the issuance of keys?	
Are key inventories and inspections conducted by the key control officer to ensure accuracy of records?	
Is the removal of essential keys from the premises prohibited?	
Is approval required for reproduction of duplication of keys?	
What types of locking hardware are used throughout the facility? Are manual and electromagnetic cipher, keypad, pushbutton, panic bar, door strikes, and related hardware and software used?	
Are security system as-built drawings being generated and ready for review?	

Have security system design and drawing standards been developed?	
Is security equipment selection criteria defined?	
What contingency plans have been developed or are in place to deal with security control center redundancy and backup operations?	
Are securities systems decentralized, centralized, integrated, and operate over existing IT network or standalone method of operation?	
What security systems manuals are available?	
What maintenance or service agreements exist for security systems?	
22.0. Communication Systems	
How is communications system wiring distributed?	
Are there redundant communications systems available?	
What protective measures are employed for the primary communication service?	
If primary mode of communication service is lost, is there a backup mode of communication?	
Is the communication system, fiber, or cabling accessible from outside the fenced or secured perimeter?	

23.0. Information Technology Systems	
Where are the routers and firewalls located?	
What type, power rating, and location of the UPS? (battery, online, filtered)	
What type and where are the LAN or WAN connections?	
Does the facility perform cyber threat monitoring and/or threat management/remediation?	
Does the organization have a Cybersecurity Plan?	
Is there network segmentation between control networks and business networks?	
Is access to control/computer rooms and remote equipment controlled?	
If information technology service is lost, is there an alternative or backup mode?	
24.0 Sensitive Material/Equipment	
Are there sensitive materials (construction documents, plans, etc.) stored at the site? If so, describe.	
At the site, is access to construction documents (e.g., plans, drawings, etc.) limited to those persons with an established need-to know and appropriate security clearance? Explain.	

Are important files and computer operations secured in an area that prohibits unauthorized entry?	
25.0 Security Plan & Historical Site Occurrences	
Does the facility currently possess a site security plan?	
If yes, when was the last review date?	
If yes, who is the approver?	
List all historical site criminal activity, including trespassing, reported copper and other thefts, etc.	

Appendix 3 – CIP-014 Questionnaire

CIP 014 Questionnaire		
Completion date of the CIP-014 Requirement 2 review		
Completion date of the Physical Security Assessment		
Completion date of the physical security plan documentation. **Within 120 days from** Requirement **R2 completion**		
Does the facility currently possess a Site Security Plan?		
Site Specific Occurrences		
List all site history / incidents of: • Sabotage • Vandalism • Physical attack • Law enforcement response Include the dates for these incidents if possible.	**Date:**	**Occurrence:**

Historical occurrences within the continental U.S.			
List all historical incidents to similar sites within the continental U.S. and the proximity to this location. • Sabotage • Vandalism • Physical attack • Law enforcement response Include the dates for these incidents if possible.	**Date:**	**Occurrence:**	**Proximity:**

Intelligence or Threat Warnings			
Indicated a threat or potential threat to the facility or a similar facility within the continental U.S.	Intel Source	Context of Intelligence or Threat Warning	Date Received
	Local Law Enforcement		
	Joint Terrorism Task Force (JTTF)		
	State Fusion Center		

	State Emergency Management Agency (SEMA)		
	FBI, or Canadian Royal Mounted Police (prior coordination may be required)		
	Industry Peer Group		
	Electric Reliability Organization (ERO)		
	ES-ISAC		
	DHS / HSIN		

Appendix 4 – Resiliency Measures

Resiliency Measures
Describe all site-specific resiliency measures—including operational controls, spare equipment, and/or current and future transmission projects—to prevent the facility from causing instability, uncontrolled separation, or cascading within an interconnection:
Spare Equipment
If spare equipment is stored off-site, has a physical security assessment of the storage facility been completed?

Existing Physical Security Measures to Deter
List below all existing physical security measures designed to deter sabotage, vandalism, physical attack, and/or incidents that would require an emergency response by law enforcement or facility personnel.
Recommended Physical Security Measures to Deter
List below all recommended physical security enhancements, modifications, and mitigations that will deter acts of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel. **(A timeline for implementation of these enhancements must be included in the security plan.)**
Existing Physical Security Measures to Detect
List below all existing physical security measures designed to detect sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel.

Recommended Physical Security Measures to Detect
List below all recommended physical security enhancements, modifications, and mitigations that will detect acts of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel. **(A timeline for implementation of these enhancements must be included in the security plan.)**
Existing Physical Security Measures to Delay
List below all existing physical security measures to delay an act of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel.

Recommended Physical Security Measures to Delay
List below all recommended physical security enhancements, modifications, and mitigations that will delay acts of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel. **(A timeline for implementation of these enhancements must be included in the security plan.)**
Existing Physical Security Measures to Assess
List below all existing physical security measures to assess an act of sabotage, vandalism, physical attack, and/or incidents that would require an emergency response by law enforcement or facility personnel.
Recommended Physical Security Measures to Assess
List below all recommended physical security enhancements, modifications, and mitigations that will assess acts of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel. **(A timeline for implementation of these enhancements must be included in the security plan.)**

Existing Physical Security Measures to Communicate and Respond for an Act of Sabotage
List below all existing physical security measures to communicate and respond to an act of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel.
Recommended Physical Security Measures to Communicate and Respond
List below all *recommended physical security* enhancements, modifications, and mitigations that will respond to acts of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel. **(A timeline for implementation of these enhancements must be included in the security plan.)**

Existing Physical Security Measures to Communicate and Respond to Law Enforcement and Facility Personnel
List below all existing physical security measures to communicate to law enforcement and facility personnel in response to acts of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel.
List below all recommended physical security enhancements, modifications, and mitigations that will communicate to law enforcement and facility personnel in response to acts of sabotage, vandalism, physical attack, and/or incidents that would require emergency response by law enforcement or facility personnel. **(A timeline for implementation of these enhancements must be included in the security plan.)**

Potential Law Enforcement Responder List		
List below all city, county, state, and federal law enforcement departments that may be called upon to provide a response to a real or suspected physical threat at the facility. Please include contact and coordination information.		
Agency	**Contact #**	**Contact #**

Third Party Reviewer	
Name / Company Name	
Describe Qualifications for Meeting CIP-014	
Contact Information	

Non-Disclosure Agreement(s)
Have NDAs and associated documentation been completed? **Remember the NDA is auditable.**
If so, attach to the front of this assessment with cover page indicating **restricted and or business sensitive information**.
Describe any / or absence of unaffiliated third-party recommendations to this assessment and if followed, or documentation justifying as to reason for not following:

Recommendation Summary	**Followed (Y/N)**	**If no, Explain:**

To be completed, signed, and dated by the third-party reviewer:
Reviewed by:
Date Reviewed:
Signature:

Threat Definition:
A Design Basis Threat risk assessment identifies an aggressor developed with a capability list, identifies the target(s), and creates attack scenarios of likely threats and tactics that are external. The Design Basis Threat defines the parameters of the external threat so mitigations can be explored and tested.
An effective DBT should be plausible and include:

- Number of aggressors
- Aggressor knowledge level, competency, and extent of training
- Operational techniques, and method of transport to be utilized as well as means of access to the site
- Tools and equipment readily available for aggressor use (such as ladders, grinders, etc.)
- Tactics deception, forced entry, surreptitiousness, etc.
- Aggressor preparation level
- Aggressor weaponry level

Potential Aggressor Targets:
There is not a clear line of demarcation for CIP-014 Requirement R4. The scope of the threat and vulnerability evaluation may consider areas inside as well as outside the immediate area or fence of Transmission station(s), Transmission substation(s), and primary control center(s). Likely targeted areas would likely include high-impact components such as control houses and primary control center building systems (e.g., power supply, communication systems, HVAC, and other aspects required to keep the location functional / inhabitable). Other likely targets may include long-lead time components such as transformers, communication towers, etc.

Communication systems as a target:
Consideration should be given to this communication risk understanding this (and station service) risk may be present in or outside the fence.
Communication loss may impact the ability:

- for operational transmission monitoring
- for operational transmission control
- for equipment to function appropriately, such as communication to remote ends for relaying purposes
- to monitor physical security devices, thus impacting detection and response capabilities to aggressor attacks

Damage to transformers & associated components

- Cooling systems
  Manufactured from lightweight material for heat shedding, cooling systems are extremely vulnerable. This could be offset by a redundant cooling system that could be external to the transformer. Transformers can also be manufactured with de-rated cooling resulting in the metal being a more resilient thickness. The temperature rating of the transformer can then tolerate a higher heat. The downside is that this de-rating results in lower MVA output. Generally, cooling systems are built for a 30°C average ambient air temperature in a 24-hour period. The de-rating can bring them to 40°C maximum amperage ambient air temperature over a 24-hour period.
- Bushings
  Bushings are particularly vulnerable, and damage may result in catastrophic transformer failure if damaged nearest the bushing turret (mounting plate).
  - Composites (also known as dry or polymeric bushings) that are not spring loaded may mitigate explosive concerns, which could result not only in personnel injury but cause collateral damage to other bushings and insulators.
  - Porcelain bushings are manufactured overseas and therefore have supply-chain issues, including extended lead time. No- or low-replacement bushings pose a resiliency vulnerability.
- Valves

The valves are vulnerable as they can be opened or damaged easily, as valves are not made of as thick of material is the transformer tank walls.
- Circuit breakers
- Remote monitoring equipment
- Transformer tank

Placement of shots or location of damage will impact the rate at which the oil drains to the level that will result in an operational alarm. The shot placement may be such as to cause immediate disabling damage, or such that a delay allows the aggressors time to leave the area without detection.

Although the transformer tank is generally a heavy gauge steel, damage to the tank may result in:
- an oil fire, resulting in equipment damage and/or malfunction
- an extended operational recovery due to long lead time for replacement equipment
- costly environmental recovery and collateral environmental concerns

Other substation components that may be a likely target:
- Cable pits
- Yard relay equipment
- Control houses
- Buss conductor damage
- Circuit breakers
- Facility operational and security communication (copper, fiber, microwave, SCADA etc.).

Transmission station(s), Transmission substation(s), and primary control center(s) are subject to attack at any time.
Aggressors may give consideration to the following:
- Peak load demand periods for greater bulk electric system impact
- Lighting: There are two opposing methodologies regarding facility lighting.
  - One articulates that lighting serves as a valuable deterrent and allows effective observance of potential aggressors thus making the target less attractive.
  - The other articulates that light better allows potential aggressors to see would-be targets. This no-light / low-light target protection methodology may not be practical when consideration is given to the low cost and ready availability of night-vision equipment.
  - Nighttime surveillance and attacks allows better concealment unless installed lighting is such to negate darkness.
  - In no-light arrangements, consideration should be given to fast-acting lighting tied to motion sensing or alarms.

Physical security system response vulnerabilities for consideration:
Three potential concerns of physical security system functionality that should be given consideration are:
1) Equipment performance
2) Security operations center personnel performance
3) Law enforcement response time

Threat and vulnerability evaluations of existing facilities generally show that the primary threats faced by facilities continue to be routine criminal activity; however, the proximity of a facility to high-visibility targets and the ability of the facility itself to affect the Bulk Electric System elevate the risks from both internal and external man-made threats.

Requirement R4.3. states that the threat and vulnerability evaluation shall also consider *"Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the*

Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors."

Local, state, and federal law enforcement agencies, the Electric Reliability Organization, and the Electricity Sector Information Sharing and Analysis Center all serve as valuable resources for threat and information sharing. Additional consideration should be given to industry peer groups who may be able to share incident/event information in an expeditious manner, thus facilitating quicker response plan activation.

Information Protection
Companies should also give consideration to information protection during the facility threats and vulnerabilities analysis. The availability of information pertaining to Transmission station(s), Transmission substation(s), and primary control center(s) may impact the capabilities of the aggressor.

Requirement R4 is not a once and done task. Rather, Requirement R4 should be viewed as an ongoing process for which periodic review considers new tactics, threats, vulnerabilities, and evolving intelligence to improve facility resiliency.

Mitigation, Resiliency, and Response
The evaluation of potential threats and vulnerabilities of a physical attack is only one step in the protection of transmission stations, transmission substations, and primary control centers. Mitigations should consider effectiveness and the benefit provided. It is not possible to eliminate all risk to a facility. Contingency planning and resiliency are very important aspects, as no mitigation can stop every attack.