

## Project 2014-04 - Physical Security Directives

### Mapping Document

#### Background

In Order No. 802 (final order on CIP-014-1 – Physical Security), issued on November 20, 2014, FERC directed NERC to remove the term “widespread” from Reliability Standard CIP-014-1 or, alternatively, to propose modifications to the Reliability Standard that address the Commission’s concerns. FERC directed that NERC submit a responsive modification within six months from the effective date of this final rule.

#### Standard: CIP-014-2, Physical Security

Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p><b>R1.</b> Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered</p>	<p>Removed the term “widespread” from Requirement R1</p>	<p><b>R1.</b> Each Transmission Owner shall perform an initial risk assessment and subsequent risk assessments of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria specified in Applicability Section 4.1.1. The initial and subsequent risk assessments shall consist of a transmission analysis or transmission analyses designed to identify the Transmission station(s) and Transmission substation(s) that if rendered</p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p>inoperable or damaged could result in <b>widespread</b> instability, uncontrolled separation, or Cascading within an Interconnection. <i>[VRF: High; Time-Horizon: Long-term Planning]</i></p> <p><b>1.1.</b> Subsequent risk assessments shall be performed:</p> <ul style="list-style-type: none"> <li>At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in <b>widespread</b> instability, uncontrolled separation, or Cascading within an Interconnection; or</li> <li>At least once every 60 calendar months for a Transmission Owner that</li> </ul>		<p>inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection. <i>[VRF: High; Time-Horizon: Long-term Planning]</i></p> <p><b>1.1.</b> Subsequent risk assessments shall be performed:</p> <ul style="list-style-type: none"> <li>At least once every 30 calendar months for a Transmission Owner that has identified in its previous risk assessment (as verified according to Requirement R2) one or more Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection; or</li> <li>At least once every 60 calendar months for a Transmission Owner that has not identified in its previous risk assessment (as verified according to</li> </ul>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p>has not identified in its previous risk assessment (as verified according to Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in <b>widespread</b> instability, uncontrolled separation, or Cascading within an Interconnection.</p> <p><b>1.2.</b> The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.</p>		<p>Requirement R2) any Transmission stations or Transmission substations that if rendered inoperable or damaged could result in instability, uncontrolled separation, or Cascading within an Interconnection.</p> <p><b>1.2.</b> The Transmission Owner shall identify the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment.</p>
<p><b>R2.</b> Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with</p>	Retained from previous version	<p><b>R2.</b> Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or</p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p>or after the risk assessment performed under Requirement R1. <i>[VRF: Medium; Time-Horizon: Long-term Planning]</i></p> <p><b>2.1.</b> Each Transmission Owner shall select an unaffiliated verifying entity that is either:</p> <ul style="list-style-type: none"> <li>• A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or</li> <li>• An entity that has transmission planning or analysis experience.</li> </ul> <p><b>2.2.</b> The unaffiliated third party verification shall verify the Transmission Owner’s risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90</p>		<p>after the risk assessment performed under Requirement R1. <i>[VRF: Medium; Time-Horizon: Long-term Planning]</i></p> <p><b>2.1.</b> Each Transmission Owner shall select an unaffiliated verifying entity that is either:</p> <ul style="list-style-type: none"> <li>• A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator; or</li> <li>• An entity that has transmission planning or analysis experience.</li> </ul> <p><b>2.2.</b> The unaffiliated third party verification shall verify the Transmission Owner’s risk assessment performed under Requirement R1, which may include recommendations for the addition or deletion of a Transmission station(s) or Transmission substation(s). The Transmission Owner shall ensure the verification is completed within 90</p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p>calendar days following the completion of the Requirement R1 risk assessment.</p> <p><b>2.3.</b> If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:</p> <ul style="list-style-type: none"> <li>• Modify its identification under Requirement R1 consistent with the recommendation; or</li> <li>• Document the technical basis for not modifying the identification in accordance with the recommendation.</li> </ul>		<p>calendar days following the completion of the Requirement R1 risk assessment.</p> <p><b>2.3.</b> If the unaffiliated verifying entity recommends that the Transmission Owner add a Transmission station(s) or Transmission substation(s) to, or remove a Transmission station(s) or Transmission substation(s) from, its identification under Requirement R1, the Transmission Owner shall either, within 60 calendar days of completion of the verification, for each recommended addition or removal of a Transmission station or Transmission substation:</p> <ul style="list-style-type: none"> <li>• Modify its identification under Requirement R1 consistent with the recommendation; or</li> <li>• Document the technical basis for not modifying the identification in accordance with the recommendation.</li> </ul>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p><b>2.4.</b> Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.</p>		<p><b>2.4.</b> Each Transmission Owner shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.</p>
<p><b>R3.</b> For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the</p>	Retained from previous version	<p><b>R3.</b> For a primary control center(s) identified by the Transmission Owner according to Requirement R1, Part 1.2 that a) operationally controls an identified Transmission station or Transmission substation verified according to Requirement R2, and b) is not under the operational control of the Transmission Owner: the Transmission Owner shall, within seven calendar days following completion of Requirement R2, notify the Transmission Operator that has operational control of the</p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p>primary control center of such identification and the date of completion of Requirement R2. <i>[VRF: Lower; Time-Horizon: Long-term Planning]</i></p> <p><b>3.1.</b> If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.</p>		<p>primary control center of such identification and the date of completion of Requirement R2. <i>[VRF: Lower; Time-Horizon: Long-term Planning]</i></p> <p><b>3.1.</b> If a Transmission station or Transmission substation previously identified under Requirement R1 and verified according to Requirement R2 is removed from the identification during a subsequent risk assessment performed according to Requirement R1 or a verification according to Requirement R2, then the Transmission Owner shall, within seven calendar days following the verification or the subsequent risk assessment, notify the Transmission Operator that has operational control of the primary control center of the removal.</p>
	Retained from previous version	

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p><b>R4.</b> 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: <i>[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]</i></p> <p><b>4.1.</b> Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);</p> <p><b>4.2.</b> Prior history of attack on similar facilities taking into account the frequency,</p>	<p>Retained from previous version</p>	<p><b>R4.</b> 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: <i>[VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]</i></p> <p><b>4.1.</b> Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);</p> <p><b>4.2.</b> Prior history of attack on similar facilities taking into account the frequency,</p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p>geographic proximity, and severity of past physical security related events; and</p> <p><b>4.3.</b> 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.</p>		<p>geographic proximity, and severity of past physical security related events; and</p> <p><b>4.3.</b> 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.</p>
<p><b>R5.</b> Each Transmission Owner that identified a Transmission station, Transmission substation, or 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 develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and</p>	Retained from previous version	<p><b>R5.</b> Each Transmission Owner that identified a Transmission station, Transmission substation, or 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 develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary</p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p>primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: <i>[VRF: High; Time-Horizon: Long-term Planning]</i></p> <p><b>5.1.</b> 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.</p> <p><b>5.2.</b> Law enforcement contact and coordination information.</p> <p><b>5.3.</b> A timeline for executing the physical security enhancements and modifications specified in the physical security plan.</p>		<p>control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes: <i>[VRF: High; Time-Horizon: Long-term Planning]</i></p> <p><b>5.1.</b> 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.</p> <p><b>5.2.</b> Law enforcement contact and coordination information.</p> <p><b>5.3.</b> A timeline for executing the physical security enhancements and modifications specified in the physical security plan.</p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p><b>5.4.</b> Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).</p>		<p><b>5.4.</b> Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).</p>
<p><b>R6.</b> Each Transmission Owner that identified a Transmission station, Transmission substation, or 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 have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. <i>[VRF: Medium; Time-Horizon: Long-term Planning]</i></p>	<p>Retained from previous version</p>	<p><b>R6.</b> Each Transmission Owner that identified a Transmission station, Transmission substation, or 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 have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5. <i>[VRF: Medium; Time-Horizon: Long-term Planning]</i></p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p><b>6.1.</b> Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:</p> <ul style="list-style-type: none"> <li>• An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.</li> <li>• An entity or organization approved by the ERO.</li> <li>• A governmental agency with physical security expertise.</li> <li>• An entity or organization with demonstrated law enforcement, government, or military physical security expertise.</li> </ul>		<p><b>6.1.</b> Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:</p> <ul style="list-style-type: none"> <li>• An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification.</li> <li>• An entity or organization approved by the ERO.</li> <li>• A governmental agency with physical security expertise.</li> <li>• An entity or organization with demonstrated law enforcement, government, or military physical security expertise.</li> </ul>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<p><b>6.2.</b> The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.</p> <p><b>6.3.</b> If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:</p>		<p><b>6.2.</b> The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.</p> <p><b>6.3.</b> If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation:</p>

Standard: CIP-014-2, Physical Security		
Requirement in Approved Standard	Translation to New Standard or Other Action	Comments
<ul style="list-style-type: none"> <li>• Modify its evaluation or security plan(s) consistent with the recommendation; or</li> <li>• Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.</li> </ul> <p><b>6.4.</b> Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.</p>		<ul style="list-style-type: none"> <li>• Modify its evaluation or security plan(s) consistent with the recommendation; or</li> <li>• Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.</li> </ul> <p><b>6.4.</b> Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.</p>