NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Reliability Standard Audit Worksheet[1]

CIP-014-2 – Physical Security

This section to be completed by the Compliance Enforcement Authority.

Audit ID:	Audit ID if available; or REG-NCRnnnnn-YYYYMMDD
Registered Entity:	Registered name of entity being audited
NCR Number:	NCRnnnnn
Compliance Enforcement Authority:	Region or NERC performing audit
Compliance Assessment Date(s)[2]:	Month DD, YYYY, to Month DD, YYYY
Compliance Monitoring Method:	[On-site Audit | Off-site Audit | Spot Check]
Names of Auditors:	Supplied by CEA

[1] NERC developed this Reliability Standard Audit Worksheet (RSAW) language in order to facilitate NERC's and the Regional Entities' assessment of a registered entity's compliance with this Reliability Standard. The NERC RSAW language is written to specific versions of each NERC Reliability Standard. Entities using this RSAW should choose the version of the RSAW applicable to the Reliability Standard being assessed. While the information included in this RSAW provides some of the methodology that NERC has elected to use to assess compliance with the requirements of the Reliability Standard, this document should not be treated as a substitute for the Reliability Standard or viewed as additional Reliability Standard requirements. In all cases, the Regional Entity should rely on the language contained in the Reliability Standard itself, and not on the language contained in this RSAW, to determine compliance with the Reliability Standard. NERC's Reliability Standards can be found on NERC's website. Additionally, NERC Reliability Standards are updated frequently, and this RSAW may not necessarily be updated with the same frequency. Therefore, it is imperative that entities treat this RSAW as a reference document only, and not as a substitute or replacement for the Reliability Standard. It is the responsibility of the registered entity to verify its compliance with the latest approved version of the Reliability Standards, by the applicable governmental authority, relevant to its registration status.

The NERC RSAW language contained within this document provides a non-exclusive list, for informational purposes only, of examples of the types of evidence a registered entity may produce or may be asked to produce to demonstrate compliance with the Reliability Standard. A registered entity's adherence to the examples contained within this RSAW does not necessarily constitute compliance with the applicable Reliability Standard, and NERC and the Regional Entity using this RSAW reserves the right to request additional evidence from the registered entity that is not included in this RSAW. Additionally, this RSAW includes excerpts from FERC Orders and other regulatory references. The FERC order cites are provided for ease of reference only, and this document does not necessarily include all applicable Order provisions. In the event of a discrepancy between FERC orders, and the language included in this document, FERC orders shall prevail.

[2] Compliance Assessment Date(s): The date(s) the actual compliance assessment (on-site audit, off-site spot check, etc.) occurs.

Applicability of Requirements ~~*[RSAW developer to insert correct applicability]*~~

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1												X[3,4]			
R2												X[3,4]			
R3												X[3,4]			
R4												X[3,4]	X[4]		
R5												X[3,4]	X[4]		
R6												X[3,4]	X[4]		

Legend:

Text with blue background:	Fixed text – do not edit
Text entry area with Green background:	Entity-supplied information
Text entry area with white background:	Auditor-supplied information

[3] Applicability is further defined to owners of transmission Facilities operated at 500 kV or higher (see section 4.1.1.1 of the Standard) and owners of certain transmission Facilities operating between 200 kV and 499 kV where the station or substation is connected at 200 kV or higher voltages to three or more other Transmission stations or substations, per section 4.1.1.2 of the Standard. In addition, sections 4.1.1.3 and 4.1.1.4 bring additional transmission Facilities identified as either critical to the derivation of Interconnection Reliability Operating Limits and Nuclear Plant Interface, respectively, within the purview of the standard. Please see the referenced sections of the Standard for additional details regarding applicability of the Requirements to Transmission Owners.

[4] Facilities in a "protected area," as defined in 10 C.F.R. § 73.2, within the scope of a security plan approved or accepted by the Nuclear Regulatory Commission are not subject to this Standard; or, Facilities within the scope of a security plan approved or accepted by the Canadian Nuclear Safety Commission are not subject to this Standard.

Findings

(This section to be completed by the Compliance Enforcement Authority)

Req.	Finding	Summary and Documentation	Functions Monitored

Req.	Areas of Concern

Req.	Recommendations

Req.	Positive Observations

Subject Matter Experts

Identify the Subject Matter Expert(s) responsible for this Reliability Standard.

Registered Entity Response (Required; Insert additional rows if needed):

SME Name	Title	Organization	Requirement(s)

Note to Auditors Concerning Third Party Verifications and Reviews

Requirements R2 and R6 prescribe, respectively, unaffiliated third party verifications for Requirement R1 and unaffiliated third party reviews for Requirements R4 and R5. Auditors are encouraged to rely on the verifications and reviews performed in cases where the verifying or reviewing entities are qualified, unaffiliated with the audited entity, and the scope of their verification or review is clear. The concept of reliance means using the work of others to avoid duplication of efforts and is consistent with recognized professional auditing standards, which are required for Compliance Audits per NERC's Rules of Procedure. Reliance in the context of this Reliability Standard means using the Requirement R2 verifications and Requirement R6 reviews to reduce audit risk and the related rigor of audit testing for Requirements R1, R4, and R5. However, in cases where the verifying or reviewing entity lacks the qualifications specified in Requirement R2 for verifications, or Requirement R6 for reviewers, the required unaffiliation from the audited entity, or where the scope of the third party entity's verification or review is unclear, auditors may need to apply audit testing of Requirements R1, R4, or R5. For this reason, the Evidence Requested and Compliance Assessment Approach Sections are still present in this RSAW for Requirements R1, R4, and R5. We anticipate those sections will also facilitate expectations for entities and their unaffiliated third party verifiers and reviewers, assist Electric Reliability Organization (ERO) auditors to understand the audit procedures applied by unaffiliated third party verifiers and reviewers, and provide transparency between ERO auditors and Industry, should circumstances require audit testing of Requirements R1, R4, or R5. Further, it is an objective of the ERO to have transparent Evidence Requests and Compliance Assessment Approaches for every enforceable standard, whether they are in audit scope or not.

R1 Supporting Evidence and Documentation

R1. 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 inoperable or damaged, could result in instability, uncontrolled separation, or Cascading within an Interconnection.

1.1. Subsequent risk assessments shall be performed:

- 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
- At least once every 60 calendar months for a Transmission Owner that 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 instability, uncontrolled separation, or Cascading within an Interconnection.

1.2. 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.

M1. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the risk assessment of its Transmission stations and Transmission substations (existing and planned to be in service within 24 months) that meet the criteria in Applicability Section 4.1.1 as specified in Requirement R1. Additionally, examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation of the identification of the primary control center that operationally controls each Transmission station or Transmission substation identified in the Requirement R1 risk assessment as specified in Requirement R1, Part 1.2.

Registered Entity Response (Required):

Question: Do you own any Transmission stations/substations, either existing or planned in the next 24 months, meeting the applicability requirements of Section 4.1.1? ☐ Yes ☐ No

☐ This entity does not have any applicable Transmission stations/substations.

☐ Other: [Provide explanation below]

[Include additional information regarding the question here, including the type of response and format of the response requested, as appropriate.]

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R1) Provide the current and the immediately preceding dated risk assessments.
(R1) List of existing Transmission stations/substations that meet the criteria specified in Section 4.1.1.
(R1) List of Transmission stations/substations planned in the next 24 months that meet criteria specified in Section 4.1.1.
(R1 Part 1.2) List of primary control centers that operationally control each identified Transmission station/substation.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	Document Title	Revision or Version	Document Date	Relevant Page(s) or Section(s)	Description of Applicability of Document

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-2~~1~~, R1

This section to be completed by the Compliance Enforcement Authority

	~~*The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.*~~
	(R1) Review entity's process for determining Transmission stations/substations subject to identification in accordance with Requirement R1, including weighting described in Section 4.1.1.2.
	(R1) Review entity's risk assessment process to determine the Transmission stations/substations that if rendered inoperable or damaged could result in ~~widespread~~ instability, uncontrolled separation, or Cascading within an interconnection.
	(R1) Ensure entity's risk assessment process includes Transmission stations/substations planned in the next 24 months.

	(R1) Ensure risk assessment(s) covers each Transmission station/substation meeting applicability described in Section 4.1.
	(R1 Part 1.1) If applicable, review any prior risk assessments and verify whether or not Transmission stations/substations were identified.
	(R1 Part 1.1) Review evidence that risk assessment was performed and verify that it occurred within the past 30 months where items were identified in the previous risk assessment and 60 months where no items were identified in the previous risk assessment.

Note to Auditor: Review entity's answer to the above Question and if the auditor can verify the answer is 'no,' Requirements R3-R6 do not apply and no further audit testing of Requirements R3-R6 is necessary, unless the entity performs the Transmission Operator function for a station/substation meeting the criteria of Requirement R1 Part 1.2.

The 24 month period referenced for Transmission stations/substations planned to be in service is as of the date of the risk assessment not the date of the audit.

See Implementation Plan of the standard for information on the initial performance of periodic requirements.

See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Transmission Owner shall have an unaffiliated third party verify the risk assessment performed under Requirement R1. The verification may occur concurrent with or after the risk assessment performed under Requirement R1.

2.1. Each Transmission Owner shall select an unaffiliated verifying entity that is either:

- A registered Planning Coordinator, Transmission Planner, or Reliability Coordinator;
- An entity that has transmission planning or analysis experience.

2.2. 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 calendar days following the completion of the Requirement R1 risk assessment.

2.3. 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 s Transmission station or Transmission substation:~~:~~

- Modify its identification under Requirement R1 consistent with the recommendation; or
- Document the technical basis for not modifying the identification in accordance with the recommendation.

2.4. 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 ~~verifying entity~~third party verifier and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M2. Examples of acceptable evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner completed an unaffiliated third verification of the Requirement R1 risk assessment and satisfied all of the applicable provisions of Requirement R2, including, if applicable, documenting the technical basis for not modifying the Requirement R1 identification as specified under Part 2.3. Additionally~~, examples~~, examples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 2.4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R2) Dated evidence of third party verification of the entity's risk assessment performed under Requirement R1.
(R2 Part 2.1) Documented qualifications of the verifying party.
(R2 Part 2.3) Recommendations, if any, of the verifying party related to Requirement R1 risk assessments.
(R2 Part 2.3) Documentation of modifications and implementation of recommendations or technical basis for not implementing recommendations of the verifying party.
(R2 Part 2.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-2~~1~~, R2

This section to be completed by the Compliance Enforcement Authority

	~~*The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.*~~
	(R2) Review evidence of third party verification of the entity's risk assessment and verify the following:
	(R2 Part 2.1) The reviewing entity is registered in accordance with Part 2.1 or has transmission planning or analysis experience.
	(R2 Part 2.2) Verification was completed within 90 calendar days of risk assessment.
	(R2 Part 2.3) Verifying entity's recommendations, if any, were used to modify the entity's Requirement R1 identification or the technical basis for not modifying the Requirement R1 identification is documented within 60 calendar days of completion of the verification.
	(R2 Part 2.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between the entity and third party were implemented.
Note to Auditor See Guidelines and Technical Basis section of the standard and Rationale for Requirement R2 associated with the Standard for additional details regarding the term 'unaffiliated.'	

See Implementation Plan of the standard for information on the initial performance of periodic requirements.

The third party verification may occur concurrent with or after the risk assessment performed under Requirement R1.

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. 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 primary control center of such identification and the date of completion of Requirement R2.

3.1. 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.

M3. Examples of acceptable evidence may include, but are not limited to, dated written or electronic notifications or communications that the Transmission Owner notified each Transmission Operator, as applicable, according to Requirement R3.

Registered Entity Response (Required):

Question: Are there any primary control centers identified in Requirement R1, Part 1.2 that are not under operational control of your NERC registration? ☐ Yes ☐ No

[Note: A separate spreadsheet or other document may be used. If so, provide the document reference below.]

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R3) If applicable, dated communications with Transmission Operators demonstrating notification and the date of completion of Requirement R2.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-21, R3

This section to be completed by the Compliance Enforcement Authority

	~~*The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.*~~
	(R3) For each applicable primary control center identified in Requirement R1 Part 1.2 not under the control of the entity's registration, verify notification exists and contains the date of completion of Requirement R2, and ensure the responsible Transmission Operator was notified within seven calendar days of the completion of R2.
	(R3 Part 3.1) For each Transmission station/substation removed under Part 3.1, ensure the responsible Transmission Operator was notified of the removal within seven calendar days of removal from identification.
Note to Auditor: Note the entity's response to the above Question. If auditor can verify the entity's answer of 'No,' then Requirement R3 is not applicable and no further audit testing is required. See Implementation Plan of the standard for information on the initial performance of periodic requirements.	

Auditor Notes:

R4 Supporting Evidence and Documentation

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 evaluation shall consider the following:

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.

M4. Examples of evidence may include, but are not limited to, dated written or electronic documentation that the Transmission Owner or Transmission Operator conducted an evaluation of the potential threats and vulnerabilities of a physical attack to their respective Transmission station(s), Transmission substation(s) and primary control center(s) as specified in Requirement R4.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R4) A description of the entity's process for executing the evaluation prescribed in Requirement R4.
(R4) Dated evidence of the evaluation prescribed in Requirement R4.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-2~~1~~, R4

This section to be completed by the Compliance Enforcement Authority

	~~*The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.*~~
	(R4) Review evidence of evaluation and verify it considers the following:
	(R4) Potential threats and vulnerabilities as described in Requirement R4.
	(R4 Part 4.1) Unique characteristics as described in Requirement R4 Part 4.1.
	(R4 Part 4.2) Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events.
	(R4 Part 4.3) Intelligence or warnings as described in Part 4.3.

Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement.

Auditor should cross reference the Transmission stations/substations and primary control centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 to ensure it is complete.

See Implementation Plan of the standard for information on the initial performance of periodic requirements.

Auditor Notes:

R5 Supporting Evidence and Documentation

R5. Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center identified 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 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:

5.1. Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.

5.2. Law enforcement contact and coordination information.

5.3. A timeline for executing the physical security enhancements and modifications specified in the physical security plan.

5.4. Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).

M5. Examples of evidence may include, but are not limited to, dated written or electronic documentation of its physical security plan(s) that covers their respective identified and verified Transmission station(s), Transmission substation(s), and primary control center(s) as specified in Requirement R5, and additional evidence demonstrating execution of the physical security plan according to the timeline specified in the physical security plan.

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R5) Dated physical security plan(s).

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-21, R5

This section to be completed by the Compliance Enforcement Authority

	~~*The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.*~~
	(R5) Review evidence and verify the physical security plan(s) covers the Transmission stations/substations and primary controls identified in Requirements R1 and/or R2, and verify plan was developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). In addition, verify the plan includes the following attributes:
	(R5 Part 5.1) Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.
	(R5 Part 5.2) Law enforcement contact and coordination information.
	(R5 Part 5.3) A timeline for executing physical security enhancements and modifications specified in the physical security plan.
	(R5 Part 5.4) Provisions to evaluate evolving physical threats, and their corresponding security measures in accordance with R5 Part 5.4
	(R5) Verify implementation of physical security plan(s). See 'Note to Auditor' for details.
Note to Auditor: See above Note Concerning Third Party Verifications for important details regarding audit risk assessment and related rigor of audit procedures to be applied for this Requirement. Auditor should cross reference the Transmission stations/substations and primary control centers identified in the risk assessment performed under Requirement R1 to the evaluation prescribed in Requirement R4 and the security plan(s) prescribed in Requirement R5 to ensure the plan addresses vulnerabilities to	

physical attacks per the evaluation conducted in Requirement R4.

Requirement R5 includes implementation of the security plan(s), which is not within the scope of the third party review described in Requirement R6. Auditors can gain reasonable assurance security plan(s) was/were implemented by determining if specific actions prescribed by the plan(s) have taken place within the timelines established by the plan(s). For example, if the plan calls for certain procedures to occur, then auditors could ask for evidence demonstrating the procedure has been implemented within the timeline established in the security plan. Also, if the plan calls for construction of a barrier, an auditor could verify evidence that such a barrier was constructed in accordance with the entity's timeline. As auditors should obtain reasonable, not absolute, assurance the plan(s) was/were implemented, testing implementation on a sample basis may be appropriate.

See Implementation Plan of the standard for information on the initial performance of periodic requirements.

Auditor Notes:

R6 Supporting Evidence and Documentation

R6. Each Transmission Owner ~~identifies~~ that identified a Transmission station, Transmission substation, or primary control center identified 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

6.1. Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following:

- 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.
- An entity or organization approved by the ERO.
- A governmental agency with physical security expertise.
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

6.2. 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.

6.3. 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:

- Modify its evaluation or security plan(s) consistent with the recommendation; or
- Document the reason for not modifying the evaluation or security plan(s) consistent with the recommendation.

6.4. 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 ~~reviewing entity~~third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.

M6. Examples of evidence may include, but are not limited to, written or electronic documentation that the Transmission Owner or Transmission Operator had an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5 as specified in Requirement R6 including, if applicable, documenting the reasons for not modifying the evaluation or security

plan(s) in accordance with a recommendation under Part 6.3. ~~Aditionally~~Additionally, e~~E~~xamples of evidence may include, but are not limited to, written or electronic documentation of procedures to protect information under Part 6.4

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation of how you comply with this Requirement. References to supplied evidence, including links to the appropriate page, are recommended.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
(R6) Dated Evidence of unaffiliated third party review of entity's Requirement R4 evaluation and Requirement R5 security plan(s).
(R6 Part 6.1) Evidence that reviewing entity staff meets qualifications identified in Part 6.1.
(R6 Part 6.3) Recommendations of reviewing party related to Requirement R4 evaluation and Requirement R5 security plan.
(R6 Part 6.3) Dated documentation of modifications and implementation of recommendations or reasons and compensating mitigating measures for not implementing recommendations of the reviewing party.
(R6 Part 6.4) Evidence that procedures were implemented to protect sensitive and confidential information.

Registered Entity Evidence (Required):

The following information is required for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location of the evidence.					
File Name	**Document Title**	**Revision or Version**	**Document Date**	**Relevant Page(s) or Section(s)**	**Description of Applicability of Document**

Audit Team Evidence Reviewed (This section to be completed by the Compliance Enforcement Authority):

Compliance Assessment Approach Specific to CIP-014-21, R6

This section to be completed by the Compliance Enforcement Authority

	~~*The RSAW Developer will complete this section with a set of detailed steps for the audit process. See the RSAW Developer's Guide for more information.*~~
	(R6) Review evidence and verify the physical security plan(s) and the Requirement R4 evaluation have been reviewed by an unaffiliated third party. Also, review evidence and verify the following:
	(R6 Part 6.1) Reviewing party has the qualifications identified in Part 6.1.
	(R6 Part 6.2) Review is dated within 90 calendar days of completion of the Requirement R5 security plan.
	(R6 Part 6.3) Reviewing entity recommended changes to security plan(s) were made by entity or the reason(s) for not making the change(s) was/were documented within 60 calendar days of the completion of the unaffiliated third party review.
	(R6 Part 6.4) Review non-disclosure agreement (or other evidence) to verify procedures for protecting sensitive or confidential information between entity and third party were implemented.

Note to Auditor: The third party review may occur concurrent with or after the evaluation performed under Requirement R4 or the security plan develop under Requirement R5.

See Guidelines and Technical Basis associated with the Standard for additional details related to qualifications of reviewing entities that may inform audited entities selection of a reviewing entity.

See Implementation Plan of the standard for information on the initial performance of periodic requirements.

Auditor Notes:

Additional Information:

Reliability Standard

The RSAW developer should provide the following information without hyperlinks. Update the information below as appropriate.

The full text of CIP-014-1 may be found on the NERC Web Site (www.nerc.com) under "Program Areas & Departments", "Reliability Standards."

In addition to the Reliability Standard, there is an applicable Implementation Plan available on the NERC Web Site.

In addition to the Reliability Standard, there is background information available on the NERC Web Site.

Capitalized terms in the Reliability Standard refer to terms in the NERC Glossary, which may be found on the NERC Web Site.

Sampling Methodology [If developer deems reference applicable]

Sampling is essential for auditing compliance with NERC Reliability Standards since it is not always possible or practical to test 100% of either the equipment, documentation, or both, associated with the full suite of enforceable standards. The Sampling Methodology Guidelines and Criteria (see NERC website), or sample guidelines, provided by the Electric Reliability Organization help to establish a minimum sample set for monitoring and enforcement uses in audits of NERC Reliability Standards.

Regulatory Language [Developer to ensure RSAW has been provided to NERC Legal for links to appropriate Regulatory Language – See example below]

E.g. FERC Order No. 742 paragraph 34: "Based on NERC's…….

E.g. FERC Order No. 742 Paragraph 55, Commission Determination: "We affirm NERC's…….

Selected Glossary Terms [If developer deems applicable]

The following Glossary terms are provided for convenience only. Please refer to the NERC web site for the current enforceable terms.

Revision History for RSAW

Version	Date	Reviewers	Revision Description
1	03/06/2015	Physical Security RSAW Task Force	New Document. Removed word 'widespread' from Requirement 1. Updated title page and footer for version 2.
2	04/20/2015	NERC Compliance, NERC Standards	Correction of errors noted during review period.

[i] Items in the Evidence Requested section are suggested evidence that may, but will not necessarily, demonstrate compliance. These items are not mandatory and other forms and types of evidence may be submitted at the entity's discretion.