NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Reliability Standard Audit Worksheet[1]

CIP-003-6 – Cyber Security — Security Management Controls

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

Applicability of Requirements

	BA	DP	GO	GOP	IA	LSE	PA	PSE	RC	RP	RSG	TO	TOP	TP	TSP
R1	X	X	X	X	X				X			X	X		
R2	X	X	X	X	X				X			X	X		
R3	X	X	X	X	X				X			X	X		
R4	X	X	X	X	X				X			X	X		

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

[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.

Findings

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

Req.	Finding	Summary and Documentation	Functions Monitored
R1			
R2			
P2.1			
P2.2			
P2.3			
P2.4			
P2.5			
P2.6			
R3			
R4			

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)

R1 Supporting Evidence and Documentation

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

- **1.1** For its high impact and medium impact BES Cyber Systems, if any:
  - **1.1.1.** Personnel & training (CIP-004);
  - **1.1.2.** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
  - **1.1.3.** Physical security of BES Cyber Systems (CIP-006);
  - **1.1.4.** System security management (CIP-007);
  - **1.1.5.** Incident reporting and response planning (CIP-008);
  - **1.1.6.** Recovery plans for BES Cyber Systems (CIP-009);
  - **1.1.7.** Configuration change management and vulnerability assessments (CIP-010);
  - **1.1.8.** Information protection (CIP-011); and
  - **1.1.9.** Declaring and responding to CIP Exceptional Circumstances.
- **1.2** For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:
  - **1.2.1.** Cyber security awareness;
  - **1.2.2.** Physical security controls;
  - **1.2.3.** Electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity
  - **1.2.4.** Incident response to a Cyber Security Incident

M1. Examples of evidence may include, but are not limited to, policy documents; revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber security policy.

Registered Entity Response (Required):

Question: Is R1 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any high impact or medium impact BES Cyber Systems.

☐ Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

Provide a brief explanation, in your own words, of how you comply with this Requirement. References to supplied

evidence, including links to the appropriate page, are recommended.

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
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-003-6, R1

This section to be completed by the Compliance Enforcement Authority

	For high impact and medium impact BES Cyber Systems, verify the policy or policies provided address each of the following: 1. Personnel & training (CIP-004); 2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access; 3. Physical security of BES Cyber Systems (CIP-006); 4. System security management (CIP-007); 5. Incident reporting and response planning (CIP-008); 6. Recovery plans for BES Cyber Systems (CIP-009); 7. Configuration change management and vulnerability assessments (CIP-010); 8. Information protection (CIP-011); and 9. Declaring and responding to CIP Exceptional Circumstances.
	For assets identified in CIP-002 containing low impact BES Cyber Systems, verify the policy or policies provided address each of the following: 1. Cyber security awareness; 2. Physical security controls; 3. Electronic access controls for Low Impact External Routable Connectivity and Dial-up Connectivity. 4. Incident response to a Cyber Security Incident.
	Verify each policy to meet this Requirement has been reviewed at least once every 15 calendar months.
	Verify the CIP Senior Manager has approved each policy to meet this Requirement at least once every 15 calendar months.

	Verify the approval by the CIP Senior Manager of each policy to meet this Requirement has occurred as required by the "Implementation Plan for Version 5 CIP Cyber Security Standards."
Note to Auditor:	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) that include the applicable elements in Attachment 1. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

Note: An inventory, list, or discrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required. Lists of authorized users are not required.

M2. Evidence must include each of the documented cyber security plan(s) that collectively include each of the applicable elements in Attachment 1.

Registered Entity Response (Required):

Question: Is R2 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not have any low impact BES Cyber Systems.

☐ Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
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-003-6, R2

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has documented at least one cyber security plan that includes cyber security awareness reinforcement using direct communications, indirect communications, or management support and reinforcement.
	Verify that the Responsible Entity has reinforced cyber security awareness of its cyber security practices at least once every 15 calendar months.
	Verify that the Responsible Entity has documented and implemented a plan that includes at least one of the physical access controls in Attachment 1, Section 2.1 to the asset or the low impact BES Cyber Systems within the asset.
	Verify that the Responsible Entity has documented and implemented a plan that includes at least one of the physical access controls in Attachment 1, Section 2.2 to the Cyber Asset containing the Low Impact BES Cyber System Electronic Access Point.
	Verify that the Responsible Entity has documented and implemented a Low Impact BES Cyber System Electronic Access Point that permits only necessary inbound and outbound access and denies all other access.
	Verify that the Responsible Entity has documented and implemented authentication for all Dial-up Connectivity.
	Verify that the Responsible Entity has Incident Response plan by asset or group of assets that includes: 1. Process for Identification, classification, and response to Cyber Security Incidents. 2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident and subsequent notification to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 3. Roles and responsibilities of Cyber Security Incident response by groups or individuals. 4. Incident handling procedures for Cyber Security Incidents. 5. Test each Cyber Security Incident Response plan(s) at least once every 36 calendar months: 1. By responding to an actual Reportable Cyber Security Incident. 2. With a paper drill or tabletop exercise of a Reportable Cyber Security Incident. 3. With an operational exercise of a Reportable Cyber Security Incident. 6. Retain records related to Reportable Cyber Security Incidents. 7. Update of each Cyber Security Incident Response plan(s) within 180 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident.
Note to Auditor:	

Auditor Notes:

R3 Supporting Evidence and Documentation

R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

M3. An example of evidence may include, but is not limited to, a dated and approved document from a high level official designating the name of the individual identified as the CIP Senior Manager.

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
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-003-6, R3

This section to be completed by the Compliance Enforcement Authority

	Verify the CIP Senior Manager has been identified by name.
	Verify that the date the CIP Senior Manager was identified has been recorded.
	Verify that any changes made to the CIP Senior Manager were dated and documented within 30 calendar days of the change.
	Verify the CIP Senior Manager is a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards.
Note to Auditor:	

Auditor Notes:

R4 Supporting Evidence and Documentation

R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. *[Violation Risk Factor: Lower] [Time Horizon: Operations Planning]*

M4. An example of evidence may include, but is not limited to, a dated document, approved by the CIP Senior Manager, listing individuals (by name or title) who are delegated the authority to approve or authorize specifically identified items.

Registered Entity Response (Required):

Question: Is R4 applicable to this audit? ☐ Yes ☐ No

If "No," why not?

☐ This entity does not delegate authority.

☐ Other: [Provide explanation below]

Registered Entity Response (Required):

Compliance Narrative:

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

Registered Entity Evidence (Required):

The following information is requested for each document submitted as evidence. Also, evidence submitted should be highlighted and bookmarked, as appropriate, to identify the exact location where evidence of compliance may be found.					
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-003-6, R4

This section to be completed by the Compliance Enforcement Authority

	Verify that the Responsible Entity has implemented a documented process to delegate authority.
	Verify that all delegates have been identified by name or title.
	Verify that the delegation of authority includes the specific action delegated.
	Verify specific actions delegated by the CIP Senior Manager are allowed by the CIP Standards.
	Verify that the dates for all delegations have been recorded.
	Verify that the CIP Senior Manager approved all delegations.
	Verify that any changes made to delegations were dated and documented within 30 calendar days of the change.
Note to Auditor:	

Auditor Notes:

Additional Information:

Reliability Standard

The full text of CIP-003-6 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

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

See FERC Order 706
See FERC Order 791

Revision History for RSAW

Version	Date	Reviewers	Revision Description
Draft1 V0	06/17/2014	Posted for Industry Comment	New Document
Draft2v0	09/17/2014	CIP RSAW Development Team	Address comments received in response to Draft1v0.