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, for its high impact and medium impact BES Cyber Systems, 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** Personnel & training (CIP-004);
- **1.2** Electronic Security Perimeters (CIP-005) including Interactive Remote Access;
- **1.3** Physical security of BES Cyber Systems (CIP-006);
- **1.4** System security management (CIP-007);
- **1.5** Incident reporting and response planning (CIP-008);
- **1.6** Recovery plans for BES Cyber Systems (CIP-009);
- **1.7** Configuration change management and vulnerability assessments (CIP-010);
- **1.8** Information protection (CIP-011); and
- **1.9** Declaring and responding to CIP Exceptional Circumstances.

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]

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

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.

All applicable documented cyber security policy or policies for compliance with this Requirement.
Policy or policies provided should cover all of the following areas: 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.
Evidence of CIP Senior Manager approval for each policy that is used to meet this Requirement.

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

	Review the applicability of this Requirement to this entity. If the Requirement is not applicable, skip the remaining items in this list.
	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.

	Verify the CIP Senior Manager has approved each policy provided to meet this Requirement at least once every 15 calendar months.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R2 Supporting Evidence and Documentation

R2. Each Responsible Entity for its assets containing low impact BES Cyber Systems shall perform each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets. [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 applicable documented policies and processes that collectively include each of the applicable requirement parts in *CIP-003-6 Table R2 – Low Impact Assets* and any additional evidence to demonstrate implementation as described in the Measures column of the table.

R2 Part 2.1

CIP-003-6 Table R2– Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	Low Impact BES Cyber Systems	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 topics in CIP-003-6, Requirement R2, Parts 2.2 – 2.6.	An example of evidence may include, but is not limited to, one or more documented cyber security policies that address each of the areas in Requirement R2, Parts 2.2 – 2.6 and includes evidence of review and CIP Senior Manager approval at least every 15 calendar months.

Registered Entity Response (Required):
Question: [Text of question?] ☐ Yes ☐ No
[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.]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
Evidence that the CIP Senior Manager has approved all applicable documented processes that address Requirement R2, Parts 2.2 – 2.6.

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, Part 2.1

This section to be completed by the Compliance Enforcement Authority

	Verify that the CIP Senior Manager has approved each applicable documented process at least once every 15 calendar months.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
Note to Auditor:	

Auditor Notes:

R2 Part 2.2

CIP-003-6 Table R2– Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	Low Impact BES Cyber Systems	Implement one or more documented processes that include operational or procedural control(s) to restrict physical access.	An example of evidence may include, but is not limited to, documentation of the operational or procedural control(s).

Registered Entity Response (Required):
Question: [Text of question?] ☐ Yes ☐ No
[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.]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
List of assets which contain a BES Cyber System. Include the following information for each asset in the list: • An identification of the asset (name, number, etc.), • The location of the asset (GPS coordinates, street address, etc.), • The identification of all impact levels of the BES Cyber Systems (high, medium, low) contained by the asset, • An indication of whether any BES Cyber System contained by the asset employs an external routable protocol path, • An indication of whether the asset is or contains a Control Center, • If the asset is or contains a Control Center, an indication of whether any BES Cyber System contained by the Control Center employs an external routable protocol path, • An indication of whether any BES Cyber System contained by the asset employs Dial-up Connectivity.

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**	**Document**	**Relevant**	**Description of Applicability**

		or Version	Date	Page(s) or Section(s)	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 Part 2.2

This section to be completed by the Compliance Enforcement Authority

	Review the applicable processes. Verify the scope of the processes collectively includes all low impact BES Cyber Systems. Verify the processes include controls which are sufficient to restrict physical access to their applicable BES Cyber Systems.
	Select a sample of assets from the supplied list.
	For each asset in the sample, perform a site visit to verify the following: 1. The applicable operational or procedural controls to restrict physical access have been implemented.

Note to Auditor:

1. The scope of the processes may identify low impact BES Cyber Systems by asset, rather than by individual BES Cyber System.
2. The sample selected should be a judgmental sample. The size of the sample should be selected with consideration of the needs and scope of the audit. The assets may be selected with location as a consideration.
3. The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at a BES asset. The Responsible Entity has flexibility in the controls used and the granularity of those controls. The entity is to document its operational or physical controls that restrict access to the low impact BES Cyber Systems at the asset. Entities may utilize perimeter controls (fences with locked gates, guards, site access policies, etc.) and/or more granular areas of access control in areas where low impact BES Cyber Systems are located, such as control rooms or control houses. Lists of authorized users are not required.

Auditor Notes:

R2 Part 2.3

CIP-003-6 Table R2– Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.3	Low Impact BES Cyber Systems at Control Centers	Implement one or more documented processes that collectively include the following: 2.3.1. Escorted access of visitors; and 2.3.2. For Control Centers with external routable protocol paths, monitoring physical access point(s).	Examples of evidence may include, but are not limited to: • For 2.3.1, documentation of visitor escort procedure(s) at Control Centers. • For 2.3.2, documentation describing how the Responsible Entity monitors physical access points into Control Centers that have external routable protocol paths.

Registered Entity Response (Required):
Question: [Text of question?] ☐ Yes ☐ No
[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.]

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
List of assets which contain a BES Cyber System. Include the following information for each asset in the list: • An identification of the asset (name, number, etc.), • The location of the asset (GPS coordinates, street address, etc.), • The identification of all impact levels of the BES Cyber Systems (high, medium, low) contained by the asset, • An indication of whether any BES Cyber System contained by the asset employs an external routable protocol path, • An indication of whether the asset is or contains a Control Center, • If the asset is or contains a Control Center, an indication of whether any BES Cyber System contained by the Control Center employs an external routable protocol path,

- An indication of whether any BES Cyber System contained by the asset employs Dial-up Connectivity.

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, Part 2.3

This section to be completed by the Compliance Enforcement Authority

	Review the applicable processes. Verify the scope of the processes collectively includes all low impact BES Cyber Systems. Verify the processes include controls which are sufficient to: 1. Require escorted access of visitors. 2. In the case of a Control Center with external routable protocol paths, require monitoring of physical access points.
	From the supplied list, select a sample of assets which are or contain a Control Center.
	For each asset in the sample, perform a site visit to verify the following: 1. Escorted access of visitors. 2. For Control Centers with external routable protocol paths, monitoring of physical access points is implemented.

Note to Auditor:

1. The scope of the processes may identify low impact BES Cyber Systems by asset, rather than by individual BES Cyber System.
2. The sample selected should be a judgmental sample. The size of the sample should be selected with consideration of the needs and scope of the audit. The assets may be selected with location as a consideration.
3. The Responsible Entity must document and implement processes that include the physical security of the low impact BES Cyber Systems at Control Centers. For Control Centers, the entity should further describe the process for handling escorted access of visitors. For Control Centers that have external routable connectivity, monitoring of physical access points is also required. Monitoring does not imply logging and maintaining logs, but monitoring that access has been granted through an access point (door alarm, etc.). The monitoring does not need to be per low impact BES Cyber System but should be at the level as determined by the entity's controls.

Auditor Notes:

R2 Part 2.4

CIP-003-6 Table R2– Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.4	Low Impact BES Cyber Systems	Implement one or more documented processes that collectively include the following: 2.4.1. All external routable protocol paths, if any, must be through one or more identified access point(s). 2.4.2. For each identified access point, if any, require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. 2.4.3. Authentication when establishing Dial-up Connectivity, per Cyber Asset capability.	Examples of evidence may include, but are not limited to: • For 2.4.1, documentation of external routable protocol paths through identified access points. • For 2.4.2, a representative sample of a list of restrictions (e.g., firewall rules, access control lists, data diode, etc.) that demonstrates that only permitted access is allowed and that each access rule has a reason documented individually or by group. • For 2.4.3, documentation of authentication controls applied to dial-up access connections.

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented processes for implementation of this Part.
List of assets which contain a BES Cyber System. Include the following information for each asset in the list: • An identification of the asset (name, number, etc.), • The location of the asset (GPS coordinates, street address, etc.), • The identification of all impact levels of the BES Cyber Systems (high, medium, low) contained by the asset, • An indication of whether any BES Cyber System contained by the asset employs an external routable protocol path, • An indication of whether the asset is or contains a Control Center, • If the asset is or contains a Control Center, an indication of whether any BES Cyber System contained by the Control Center employs an external routable protocol path,

• An indication of whether any BES Cyber System contained by the asset employs Dial-up Connectivity.
From the sampled assets: 1. Provide drawings or other documentation that demonstrates all external routable communications paths go through one or more identified access point(s). 2. Provide the configuration information for the identified access point(s). 3. Evidence that each identified access point has: a. Inbound and outbound access permissions b. Reasons for granting access c. Denial by default for all other access 4. Evidence that all Dial-up Connectivity is authenticated, per Cyber Asset capability.

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, Part 2.4

This section to be completed by the Compliance Enforcement Authority

	Review the applicable processes. Verify the scope of the processes collectively includes all low impact BES Cyber Systems. Verify the processes include controls which are sufficient to: 1. Require that all external routable protocol paths go through one or more identified access points. 2. Require that each identified access point has inbound and outbound access permissions, including the reason for granting access, and denies all other access by default. 3. Require authentication for any Dial-up Connectivity.
	From the supplied list, select a sample of assets which contain BES Cyber System(s) that employ one or more external routable protocol paths.
	For each asset in the sample, perform a site visit to verify the following: 1. The drawings or other documentation demonstrates that all external routable communications paths go through one or more identified access point(s). 2. Each identified access point has: a. Inbound and outbound access permissions b. Reasons for granting access

	c. Denial by default for all other access 3. Authentication for Dial-up Connectivity

Note to Auditor:

1. The scope of the processes may identify low impact BES Cyber Systems by asset, rather than by individual BES Cyber System.
2. The sample selected should be a judgmental sample. The size of the sample should be selected with consideration of the needs and scope of the audit. The assets may be selected with location as a consideration.
3. The drawings, configuration information, and any other documentation provided should be reviewed holistically such that each evidence corroborates the others. For example, the configuration information should demonstrate through its permission settings that all external routable protocol paths go through the access point and the corresponding drawing corroborates the configuration of the access point.

Auditor Notes:

R2 Part 2.5

CIP-003-6 Table R2– Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.5	Low Impact BES Cyber Systems	Implement one or more Cyber Security Incident response plan(s) that collectively include the following: 2.5.1. Identification, classification, and response to Cyber Security Incidents. 2.5.2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 2.5.3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. 2.5.4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 2.5.5. Incident handling procedures for Cyber Security Incidents. 2.5.6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to: • One or more documented cyber security incident response plans that include the requirement parts. • Dated evidence that shows the testing or execution of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documented plan(s) for implementation of this Part. The plan(s) should collectively cover: 1. Identification, classification, and response to Cyber Security Incidents. 2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident. 3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law. If notification to the ES-ISAC is prohibited by law, provide the specific law and its applicability to the Responsible Entity. 4. The roles and responsibilities of Cyber Security Incident response groups or individuals. 5. Incident handling procedures for Cyber Security Incidents. 6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.
List of assets which contain a BES Cyber System. Include the following information for each asset in the list: • An identification of the asset (name, number, etc.), • The location of the asset (GPS coordinates, street address, etc.), • The identification of all impact levels of the BES Cyber Systems (high, medium, low) contained by the asset, • An indication of whether any BES Cyber System contained by the asset employs an external routable protocol path, • An indication of whether the asset is or contains a Control Center, • If the asset is or contains a Control Center, an indication of whether any BES Cyber System contained by the Control Center employs an external routable protocol path, • An indication of whether any BES Cyber System contained by the asset employs Dial-up Connectivity.
List of Cyber Security Incidents that impacted Low Impact BES Cyber Systems; If no Cyber Security Incidents have occurred, provide a null list.
Evidence the Cyber Security Incident response plan has been tested, covering the entire audit period.
From the sampled Cyber Security Incidents, provide evidence of the implementation of the plan(s) provided above.

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, Part 2.5

This section to be completed by the Compliance Enforcement Authority

Review the applicable plan(s). Verify the scope of the plan(s) collectively includes all Low Impact BES Cyber Systems. Verify the plan(s) include:

1. Identification, classification, and response to Cyber Security Incidents.
    a. Verify the plan(s) provided have specific criteria to identify Cyber Security Incidents.
    b. Verify the plan(s) provided have specific criteria to classify Cyber Security Incidents.
    c. Verify the plan(s) provided have specific actions to respond to a Cyber Security Incident.
2. Determination of whether an identified Cyber Security Incident is a Reportable Cyber Security Incident.
    a. Verify the plan(s) provided have specific measures, methodology, and guidelines to determine whether a Cyber Security Incident is a Reportable Cyber Security Incident.
3. Notification of Reportable Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), unless prohibited by law.
    a. Verify the plan(s) provided have accurate contact information and explicit instructions to notify the ES-ISAC, unless prohibited by law.
    b. Verify that all sampled identified Cyber Security Incidents which were not reported to the ES-ISAC did not meet criteria for a Reportable Cyber Security Incident.
4. The roles and responsibilities of Cyber Security Incident response groups or individuals.
    a. Verify the plan(s) define different roles for Cyber Security Incident response, such as monitoring, reporting, and documenting.
    b. Verify the plan(s) specify who is responsible, either individually or by group, for each role defined. If responsibility has been specified by group, then verify that each member of the group has been assigned a role.
5. Incident handling procedures for Cyber Security Incidents.
    a. Verify the procedures provided have specific actions that are to be performed in the event of a Cyber Security Incident.
    b. Verify the procedures address various types of threats such as malware, unauthorized access, and denial of service.
6. Testing of the plan(s) at least once per 36 calendar months, either through a paper drill, tabletop exercise, or a response to an actual Reportable Cyber Security Incident.
    a. Verify the Cyber Security Incident response plan has been tested at least once every 15 calendar months.
    b. Verify the testing method is one of the following:

	i. A response to an actual Reportable Cyber Security Incident. 1. Verify there is documentation of the Reportable Cyber Security Incident. 2. Verify the Cyber Security Incident response followed the Reportable Cyber Security Incident response plan. ii. With a paper drill or tabletop exercise of a Reportable Cyber Security Incident. 1. Verify the drill or exercise included all groups (and each member of the group) and all individuals listed as having roles to respond to Cyber Security Incidents. 2. Verify there is documentation demonstrating that the plan was exercised.
	From the supplied list, select a sample of Cyber Security Incidents that impacted Low Impact BES Cyber Systems.
	For each Cyber Security Incident in the sample, verify the following: 1. The Cyber Security Incident was correctly identified, classified, and responded to, per the plan(s). 2. Determined whether the Cyber Security Incident was a Reportable Cyber Security Incident, per the plan(s). 3. Upon the determination of a Reportable Cyber Security Incident, the ES-ISAC was notified, unless prohibited by law.
Note to Auditor: 1. The scope of the processes may identify low impact BES Cyber Systems by asset, rather than by individual BES Cyber System. 2. The sample selected should be a judgmental sample. The size of the sample should be selected with consideration of the needs and scope of the audit. The assets may be selected with location as a consideration. 3. If reporting of a Reportable Cyber Security Incident is prohibited by law, review the relevant law and verify its applicability to the Responsible Entity.	

Auditor Notes:

R2 Part 2.6

CIP-003-6 Table R2– Low Impact Assets			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.6	Low Impact BES Cyber Systems	Implement a security awareness program that reinforces cyber security practices at least quarterly. Once every 15 calendar months, the program shall reinforce Parts 2.2, 2.3, 2.4, and 2.5 above.	An example of evidence may include, but is not limited to, one or more documents describing how the Responsible Entity is implementing its cyber security awareness program per 2.6.

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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
All applicable documentation of a security awareness program for implementation of this Part.
List of assets which contain a BES Cyber System. Include the following information for each asset in the list: • An identification of the asset (name, number, etc.), • The location of the asset (GPS coordinates, street address, etc.), • The identification of all impact levels of the BES Cyber Systems (high, medium, low) contained by the asset, • An indication of whether any BES Cyber System contained by the asset employs an external routable protocol path, • An indication of whether the asset is or contains a Control Center, • If the asset is or contains a Control Center, an indication of whether any BES Cyber System contained by the Control Center employs an external routable protocol path, • An indication of whether any BES Cyber System contained by the asset employs Dial-up Connectivity.
Evidence of the implementation of the security awareness program.
Evidence that the program reinforces cyber security practices at least every quarter.
Evidence that the program reinforces Parts 2.2, 2.3, 2.4, and 2.5.

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, Part 2.6

This section to be completed by the Compliance Enforcement Authority

	Review the applicable program and verify that: 1. The security awareness program is documented. 2. The security awareness program has methods to reinforce cyber security practices. 3. The security awareness program has methods to reinforce Parts 2.2, 2.3, 2.4, and 2.5.
	Verify that the program reinforces cyber security practices at least every quarter.
	Verify that the program reinforces Parts 2.2, 2.3, 2.4, and 2.5 at least once every 15 calendar months
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.

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
Evidence that a CIP Senior Manager has been identified by name.
Evidence of when the CIP Senior Manager was identified.
Evidence of approved documentation of any changes that were made to the CIP Senior Manager.

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.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.

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]

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

Evidence Requested[i]:

Provide the following evidence, or other evidence to demonstrate compliance.
Evidence of any authority delegations, including name or title, by the CIP Senior Manager.
Evidence of specific actions delegated by the CIP Senior Manager.
Evidence of dates for delegations.
Evidence of CIP Senior Manager approval for all delegations.
Evidence that any changes to delegations were documented.

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**	**Description of Applicability of Document**

				Section(s)	

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 all delegates have been identified by name or title.
	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.
	If any of the "verify" steps above fail, then a finding of Possible Violation should be returned.
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

Selected Glossary Terms

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
Draft1 V0	06/17/2014	Posted for Industry Comment	New Document

[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.