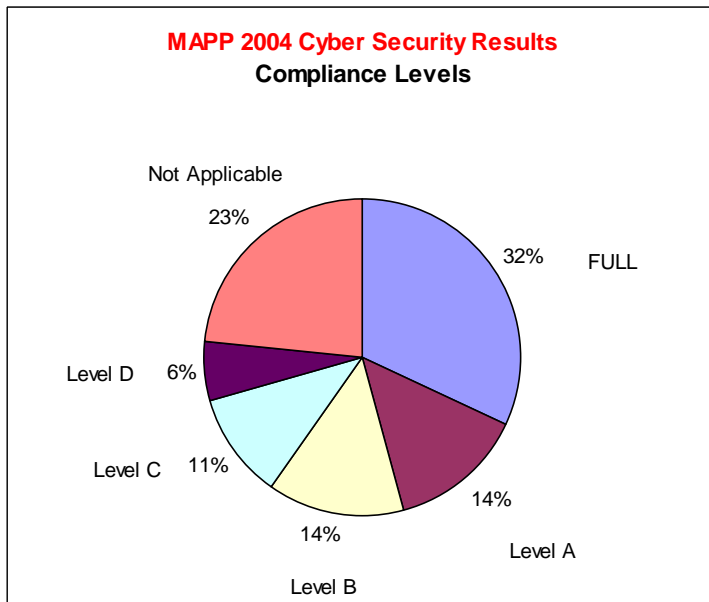


2004 MAPP CYBER SECURITY STANDARDS REPORT

For the 2004 Compliance Program, NERC has directed that the following 16 Cyber Security items be answered. All members in MAPP compliance program were asked to reply based on the individual cyber security situation **as of February 15, 2004**. No mitigation plan was required for any non-compliance response. A report was sent to NERC with the aggregate numbers for each standard based on the control area responses. However, this report reflects the aggregate responses for each standard based on responses that were received by MAPP.

MAPP 2004 Cyber Security Results

Template Name	Brief Description	Full	Level 1 or A	Level 2 or B	Level 3 or C	Level 4 or D	N/A
1201	Cyber Security Policy	12	1	3	7		7
1202	Critical Cyber Assets	16	7				7
1203	Electronic Security Perimeter	14	1	8			7
1204	Electronic Access Controls	12	3	8			8
1205	Physical Security Perimeter	13	3	7			7
1206	Physical Access Controls	13	1	9			7
1207	Personnel	10	2	8	3		7
1208	Monitoring Physical Access	12	11				7
1209	Monitoring Electronic Access	10	13				7
1210	Information Protection	8	1	0	15		7
1211	Training	3	1	1	2	16	7
1212	Systems Management	8	0	0	3	13	7
1213	Test Procedures	4	19				7
1214	Electronic Incident Response Actions	6	0	5	12		7
1215	Physical Incident Response Actions	7	0	5	11		7
1216	Recovery Plans	6	4	13			7
Total =		154	67	67	53	29	113



1201 — Cyber Security Policy

Measures Checklist

- (1) The responsible entity shall maintain its written cyber security policy stating the entity's commitment to protect critical cyber assets.
- (2) The responsible entity shall review the cyber security policy at least annually.
- (3) The current senior management official responsible for the cyber security program shall be identified by name, title, phone, address, and date of designation.
- (4) The responsible entity shall maintain documentation justifying any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.

100% Compliant 12 **Noncompliant**

- | | |
|---|--------------|
| (A) A current senior management official was not designated | <u> 1 </u> |
| (B) No cyber security policy exists. | <u> 3 </u> |
| (C) Both | <u> 7 </u> |

NOT RESPONSIBLE - 7

1202 — Critical Cyber Assets

Measures Checklist

- (1) The responsible entity shall maintain a document identifying critical cyber assets.
- (2) The responsible entity shall review and update its critical cyber asset identification document at least annually or within 90 days of the addition or removal of any critical cyber assets.

100% Compliant 16 **Noncompliant**

- | | |
|-------------------------|--------------|
| (A) No document exists. | <u> 7 </u> |
|-------------------------|--------------|

NOT RESPONSIBLE - 7

1203 — Electronic Security Perimeter

Measures Checklist

- (1) The responsible entity shall maintain a document depicting the electronic security perimeter(s), all interconnected critical cyber assets, and all electronic access points to the interconnected environment(s). The document shall verify that all critical cyber assets are within the electronic security perimeter(s).
- (2) The responsible entity shall review and update its document referenced in 1203.2.1 at least annually or within 90 days of the modification of the network.

100% Compliant 14 **Noncompliant**

- | | |
|--|--------------|
| (1) Document exists, but no verification that all critical assets are within the perimeter(s) described. | <u> 1 </u> |
| (2) No document exists. | <u> 8 </u> |

NOT RESPONSIBLE - 7

1204 — Electronic Access Controls

Measures Checklist

- (1) The responsible entity shall maintain a document identifying the access controls and their implementation for each electronic access point to the electronic security perimeter(s).
- (2) The responsible entity shall review and update the documentation referenced in 1204.2.1 at least annually or within 90 days of the modification of the electronic security perimeter or the electronic access controls.

100% Compliant 12 **Noncompliant**

- (1) Document exists, but the document does not identify the electronic access controls for one or more access points. 3
- (2) No document exists. 8

NOT RESPONSIBLE - 8

1205 — Physical Security Perimeter

Measures Checklist

- (1) The responsible entity shall maintain a document depicting the physical security perimeter(s) and all physical access points to every such perimeter. The document shall verify that all critical cyber assets are within the physical security perimeter(s).
- (2) The responsible entity shall review and update the document referenced in 1205.2.1 at least annually or within 90 days of the modification of the network.

100% Compliant 13 **Noncompliant**

- (A) Document exists, but no verification that all critical cyber assets are within the perimeter(s) described. 3
- (B) No document exists. 7

NOT RESPONSIBLE - 7

1206 — Physical Access Controls

Measures Checklist

- (1) The responsible entity shall maintain a document identifying the access controls and their implementation for each physical access point to the electronic security perimeter(s).
- (2) The responsible entity shall review and update the documentation referenced in 1206.2.1 at least annually or within 90 days of the modification of the physical security perimeter(s) or the physical access controls.

100% Compliant 13 **Noncompliant**

- (1) Document exists, but the document does not identify the physical access controls for one or more access points. 1
- (2) No document exists. 9

NOT RESPONSIBLE - 7

1207 — Personnel

Measures Checklist

- (1) The responsible entity shall maintain a list of all personnel granted access to critical cyber assets, including the specific electronic and physical access rights to the security perimeter(s).
- (2) The responsible entity shall review the document referred to in 1207.2.1 at least quarterly and update the document within 24 hours of any change.
- (3) The responsible entity shall conduct background screening of personnel consistent with the degree of access they are granted, in accordance with federal, state, provincial, and local laws.

100% Compliant 10 **Noncompliant**

- (1A) Access control rights list is available, but does not include service vendors 2
- (1B) No personnel background screening conducted. 8
- (2) Access control rights list does not exist. 4

NOT RESPONSIBLE - 7

1208 — Monitoring Physical Access

Measures Checklist

- (1) The responsible entity shall maintain a document identifying its tools and procedures for physical access monitoring. This document shall verify that the tools and procedures are functioning and being used as planned.
- (2) The responsible entity shall document physical access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights or controlled by video or other physical monitoring.

100% Compliant 11 **Noncompliant**No monitoring of access exists. 11 NOT RESPONSIBLE - 7

1209 — Monitoring Electronic Access

Measures Checklist

- (1) The responsible entity shall maintain a document identifying electronic access monitoring tools and procedures. This document shall verify that the tools and procedures are functioning and being used as planned.
- (2) The responsible entity shall document electronic access to critical cyber assets via access records (e.g., logs). Access records shall be verified against the list of access control rights.

100% Compliant 10 **Noncompliant**No monitoring of access exists 13

NOT RESPONSIBLE - 7

1210 — Information Protection

Measures Checklist

- (1) The responsible entity shall maintain a document identifying the access limitations to sensitive information related to critical cyber assets. At a minimum, this document must address access to procedures, critical asset inventories, maps, floor plans, equipment layouts and configurations.
- (2) The responsible entity shall review and update the document referred to in 1210.2.1 as necessary and at least annually.

100% Compliant 8 **Noncompliant**

- | | |
|---|--------------|
| (A) Document exists, but does not cover one of the specific items identified. | <u> 1 </u> |
| (B) Document exists, but does not cover three of the specific items identified. | <u> 0 </u> |
| (C) No document exists. | <u> 15 </u> |

NOT RESPONSIBLE - 7

1211 — Training

Measures Checklist

- (1) The responsible entity shall develop and maintain a company-specific cyber security training program that includes, at a minimum, the following required items:
 - The cyber security policy;
 - Physical and electronic access controls to critical cyber assets;
 - The release of critical cyber asset information;
 - Potential threat incident reporting; and
 - Action plans and procedures to recover or re-establish critical cyber assets following a cyber security incident.
- (2) The responsible entity shall maintain a document identifying all personnel who have access to critical cyber assets and the date of the successful completion of their training.
- (3) The responsible entity shall document that it has reviewed its training program at least annually.

100% Compliant 3 **Noncompliant**

- | | |
|--|--------------|
| (A) Training program exists, but records of training either do not exist or reveal some key personnel not trained as required. | <u> 1 </u> |
| (B) Training program exists, but does not cover one of the specific items identified. | <u> 1 </u> |
| (C) Document exists, but does not cover two of the specific items identified. | <u> 2 </u> |
| (D) No training program exists addressing critical cyber assets. | <u> 16 </u> |

NOT RESPONSIBLE - 7

1212 — Systems Management

Measures Checklist

- (1) The responsible entity shall maintain a document identifying system management policies and procedures.
- (2) The responsible entity shall review and update the document referred to in 1212.2.1 as necessary and at least annually.
- (3) The system management policies and procedures document shall address all items in requirement 1212.1.
- (4) The responsible entity shall implement system management policies and procedures as described in the system management policies and procedures document.

100% Compliant 8 **Noncompliant**

- | | |
|---|--------------|
| (A) Document exists, but does not cover one of the specific items identified | <u> 0 </u> |
| (B) Document exists, but does not cover three of the specific items identified. | <u> 0 </u> |
| (C) Document exists, but does not cover five of the specific items identified. | <u> 2 </u> |
| (D) No document exists. | <u> 13 </u> |

NOT RESPONSIBLE - 7

1213 — Test Procedures

Measures Checklist

- (1) The responsible entity shall maintain a document identifying test and acceptance criteria for the installation or modification of critical cyber assets.
- (2) The responsible entity shall maintain a document verifying that it has implemented the test and acceptance criteria.

100% Compliant 4 **Noncompliant**

- | | |
|--|--------------|
| Test procedures and acceptance criteria document does not exist. | <u> 19 </u> |
|--|--------------|

NOT RESPONSIBLE - 7

1214 — Electronic Incident Response Actions

Measures Checklist

- (1) The responsible entity shall maintain a document defining the electronic incident response action, including actions, roles and responsibilities.
- (2) The document in 1214.2.1 shall require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure*.

100% Compliant 6 **Noncompliant**

- | | |
|--|--------------|
| (1A) Document exists, but does not assign responsibilities; or | <u> 1 </u> |
| (1B) Document exists, but does not require that incidents involving critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the <i>NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure</i> . | <u> 5 </u> |
| (2) No document exists. | <u> 12 </u> |

NOT RESPONSIBLE - 7

1215 — Physical Incident Response Actions

Measures Checklist

- (1) The responsible entity shall maintain a document defining the physical incident response action, including actions, roles and responsibilities.
- (2) The document in 1215.2.1 shall require that incidents involving physical assets used to protect critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the *NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure*.

100% Compliant 7 **Noncompliant**

- | | |
|--|--------------|
| (1A) Document exists, but does not assign responsibilities | <u> 1 </u> |
| (1B) Document exists, but does not require that incidents involving physical assets used to protect critical cyber assets shall be reported to the electricity sector information sharing and analysis center in accordance with the <i>NERC-NIPC Indications, Analysis, Warnings Program Standard Operating Procedure</i> . | <u> 5 </u> |
| (2) No document exists. | <u> 11 </u> |

NOT RESPONSIBLE - 7

1216 — Recovery Plans**Measures Checklist**

- (1) The responsible entity shall maintain a document defining the action plan and procedures used to recover or re-establish critical cyber assets following a cyber security event, including actions, roles and responsibilities.
- (2) The responsible entity shall maintain a document verifying that the action plan is exercised via drill at least annually.

100% Compliant 6 **Noncompliant**

- (1) Action plans and procedures do not define specific roles and responsibilities.
- (2) No action plans or procedures exist.

 3 14 NOT RESPONSIBLE - **7**