



---

---

**IMO Reliability Compliance Program -  
Certification Form  
Standard Authority Template: 1200  
Cyber Security**

---

---

Submit this form to:



Attention:  
IMO Reliability Compliance Program  
Market Operations and Forecasts, IMO  
Station A Box 4474 Toronto ON M5W 4E5  
E-mail: [IRCP@theIMO.com](mailto:IRCP@theIMO.com)  
Fax No.: (905) 855-6372

All information submitted in this process will be used by the *IMO* solely in support of its obligations under the “*Electricity Act, 1998*”, the “*Ontario Energy Board Act, 1998*”, the “*Market Rules*” and associated policies, standards and procedures and its licence. All submitted information will be assigned the appropriate confidentiality level upon receipt.

Terms and acronyms used in this Form that are italicized have the meanings ascribed thereto in Chapter 11 of the “*Market Rules*”.

---

*This form, in combination with supporting documentation as appropriate, facilitates certification of compliance in accordance with the requirements and measures of the subject standard authority reliability compliance Template.*

**PART 1 – GENERAL INFORMATION**

<b>Market Participant Name:</b> _____	
<b>Market Participant ID:</b> _____	
<b>Reliability Compliance Contact</b>	
<b>Name:</b> _____	
<b>Telephone No.:</b> _____	<b>Fax No.:</b> _____
<b>E-mail Address:</b> _____	
<b>Assessment Date:</b> _____	

**PART 2 – STANDARD**

**Standard:**

**1201 - Cyber Security Policy:**

*Facility* owners shall create and maintain a cyber security policy for the implementation of this standard and assign a member of senior management with responsibility for leading and managing its' cyber security program. This person must authorize any deviation or exception from the requirements of this standard. Justification for any such deviation or exemption must be documented.

**1202 - Critical Cyber Assets:**

*Facility* owners shall Identify and maintain a current list of critical cyber assets.

**1204 - Electronic Access Controls:**

*Facility* owners shall Identify and implement electronic access controls for access to critical cyber assets within the electronic security perimeter.

**1209 - Monitoring Electronic Access:**

*Facility* owners shall monitor electronic access to critical cyber assets, 24 hours a day, 7 days a week.

**1211 - Training:**

*Facility* owners shall train personnel commensurate with their access to critical cyber assets. The training shall address, at a minimum: 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. Training shall be conducted upon initial employment and reviewed annually.

**1212 - Systems Security Management:**

*Facility* owners shall establish systems security management policies and procedures for configuring and securing critical cyber assets. At a minimum, these policies and procedures shall address:

- The use of effective password management that periodically requires changing of passwords, including default passwords for newly installed equipment;
- The authorization and periodic review of computer accounts and access rights;
- The disabling of unauthorized, invalidated, expired, or unused computer accounts and physical access rights;
- The disabling of unused network services and ports;
- Secure dial-up modem connections;
- Firewall management;
- Intrusion detection processes;
- Security patch management;
- The installation and update of anti-virus software;
- The retention and review of operator logs, application logs, and intrusion detection logs; and
- Identification of vulnerabilities and responses.

**1214 - Electronic Incident Response Actions:**

*Facility* owners shall define electronic incident response actions, including roles and responsibilities assigned by individual or job function.

## PART 3 – MEASURES

### Measurement:

#### 1201 - Cyber Security Policy:

*Facility* owner maintains a written cyber security policy stating the *market participant's* commitment to protect critical cyber assets.

#### 1202 - Critical Cyber Assets:

*Facility* owner maintains a document, which is reviewed at least annually, identifying critical cyber assets.

#### 1204 - Electronic Access Controls:

*Facility* owner maintains a document, which is reviewed at least annually, identifying the access controls and their implementation for each electronic access point to the electronic security perimeter(s).

#### 1209 - Monitoring Electronic Access:

*Facility* owner maintains 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.

#### 1211 - Personnel Training:

*Facility* owner has developed, implemented and maintains 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.

#### 1212 - Systems Security Management:

*Facility* owner maintains a document identifying its' systems security management policies and procedures. These systems security management policies and procedures shall address all items listed above in Part 2 Standard - **1212**.

#### 1214 - Electronic Incident Response Actions:

*Facility* owner maintains a document defining the electronic incident response action, including actions, roles and responsibilities; and

The document requires incidents involving critical cyber assets to be reported to the *IMO* and the electricity sector information sharing and analysis center in accordance with the *NERC* - "**NIPC Indications, Analysis, Warnings Program Standard Operating Procedure**".

**PART 4 – CERTIFICATION OF COMPLIANCE**

**THE REPORTING MARKET PARTICIPANT CERTIFIES THAT IT IS IN:**

- Full 100% Compliance:** Facility owner fully satisfies each of the measures as listed above in Part 3 Measurements.
  - Cyber Security Policy** in place (1201);
  - Documentation listing **Critical Cyber Assets** is in place and is reviewed & updated as appropriate annually (1202):
  - Documentation for **Electronic Access Control** exists and is reviewed & updated as appropriate annually (1204):
  - Electronic Monitoring of Access** exists (1209):
  - Personnel Training program** addressing critical cyber assets exists and is fully implemented.:
  - Systems Security Management** policies and procedures documentation exist. (1212): and
  - Documentation identifying **Electronic Incident Response Actions** exists (1214).
  
- Non-Compliance:** *(The market participant is to indicate it's level of non compliance and provide its' mitigation plan to become compliant).*
  - Level 1:** Facility owner partially fails any one of the measures as indicated below:
    - Cyber Security Policy (1201)** exists but was not updated in the last calendar year;
    - Critical Cyber Asset list (1202)** exists but was not updated within 90 days of known changes or reviewed in the last 12 months.
    - Electronic Access Control (1204)** document exists but was not updated within 90 days of known changes or reviewed in the last 12 months;
    - Electronic Monitoring of Access (1209)** is in place, but a gap in the access records exists;
    - Personnel Training program (1211)** is in place but records of training either do not exist or reveal key personnel not trained as required;
    - Systems Security Management (1212)** policies and procedures exists but fails to address one of the specific items identified; or
    - Electronic Incident Response Actions (1214)** exists, but does not require that incidents involving critical cyber assets be reported to the *IMO* or the electricity sector information sharing & analysis center in accordance with the *NERC - "NIPC Indications, Analysis, Warnings Program Standard Operating Procedure"*.
  - Level 2:**  
Not Applicable
  - Level 3:**  
Not Applicable

- Level 4: *Facility* owner fails to fully satisfy any one of the following measures.
- Cyber Security Policy (1201)** does not exist
  - Documentation listing **Critical Cyber Assets (1202)** does not exist
  - No documentation exists for **Electronic Access Control (1204)**
  - No **Electronic Monitoring of Access** exists (1209)
  - No **Personnel Training Program** addressing critical cyber assets exists (1211)
  - Systems Security Management** policies and procedures documentation does not exist. (1212) or
  - Documentation identifying **Electronic Incident Response Actions** does not exist. (1214)

Mitigation plan: (Defines the corrective steps that will taken and the timeframe, in which the market participant will meet 100% compliance.)

Mitigation plan attached.

Comments/Explanations:

Comments/explanations attached.

I have authority to bind the *market participant* named above. I certify that all information set out or referred to above is true and complete as at the date of this certification. I further understand that the foregoing information is being provided in accordance with the requirements of the *IMO reliability* compliance program (IRCP). I understand that this certification is submitted in lieu of a detailed review or “audit” by the *IMO* that may occur in the future. I acknowledge that such a review will require all information set out or referred to on this form be verified by appropriate documentation.

Certified by: \_\_\_\_\_  
Signature of Authority

Title: \_\_\_\_\_

Date of Certification: \_\_\_\_\_