National Energy Board (NEB) INTERROGATORY #1.01

Engineering Matters

Reference:

i. Hydro One, Application to Perform Upgrade and Replacement Work Impacting IPLs under Certificates EC-III-6 as amended and EC-III-13 as amended (Application), Exhibit A-2-1, page 1 of 2, (PDF page 10 of 317), A80806-1

ii. Hydro One, Application, Exhibit B, Tab 1, Schedule 1, page 7 of 9, (PDF page 31 of 317), A80806-1

Preamble:

Reference i) states: "ITC [International Transmission Company] understands that the activities in phase 1 & 2 will at times require that the shared lines be out of-service. The upgrade of these facilities should help to maintain the reliability of the power system. ITC and Hydro One will coordinate an outage plan as per the amended and restated Interconnection Facilities Agreement dated August 8, 2011 as amended on March 23, 2012."

Reference ii) states: that Lambton [Transformer Station (TS)] #2 work will be designed, constructed and tested in accordance with the latest revision of applicable standards of the following regulatory agencies, and institutes and local regulatory bodies having jurisdiction over such apparatus. The completed installation will comply with Hydro One's work specifications, standards, policies, the Market Rules issued by the Independent Electricity System Operator (IESO) and the requirements of the Northeast Power Coordinating Council (NPCC) and North American Electric Reliability Corporation (NERC).

Interrogatory:

a) Confirm Hydro One has coordinated the outage in accordance with applicable NERC reliability standards and provide:
   a.1) the NERC Standard names and requirements;
   a.2) the name(s) of affected Transmission Operators and their Reliability Coordinators;
   a.3) confirmation as to whether the NERC Standard TOP-002-2-1b (R.11) is applicable to the proposed work and to Hydro One.

b) Provide the specific applicable standards, including safety standards for construction, used to assure the quality of design, construction and operation.

Response:

a) Hydro One confirms it continues to operate both IPLs L4D and L51D in compliance with applicable NERC reliability standards.

1. Hydro One would like to clarify, and confirm, that Hydro One has provided notification to the IESO of the future need for the IPL outages and will coordinate those outages according to the Interconnection Agreement between Hydro One and ITC, and the requirements of the respective Reliability Coordinators, including the **Midcontinent Independent System Operator** ("**MISO**").

   Hydro One notes that the coordination of the outage is not performed "according to NERC standards". The standards that apply to outage coordination planning are set out in Chapter 7: Part 7.3: Outage Management of the IESO Market Manual (for Hydro One in Ontario) and the MISO (who administers the market that ITC operates in on the US side). Hydro One confirms that the outages required have already been submitted to the Reliability Coordinator (IESO). Approval is expected approximately 2 weeks before the scheduled start date, which is within the IESO's standard operating timeframe. The dates requested have been coordinated with both ITC and Hydro One project managers.

2. Hydro One and the IESO are both Transmission Operators for the Ontario facilities. The IESO and Hydro One have a detailed agreement that delineates which entity is accountable for each responsibility, in terms of the Transmission Operator role. The IESO's Accountabilities Matrix referenced below in part a) #3, and provided as Attachment 1 to this response, outlines which entity is accountable for specific elements. The Reliability Coordinator is the IESO (Ontario). The Transmission Operator for the Michigan facilities is ITC Transmission, and the Reliability Coordinator is the MISO.

3. Hydro One confirms the NERC Standard TOP-002-2-1b (R.11) is applicable to the proposed project work; however, that standard is the accountability of the IESO. It applies to the proposed project work from the perspective that the IESO (as the Transmission Operator) will perform the described studies as required.

Please refer to the *IESO-Transmitter: Assignment of NERC Transmission Operator Accountabilities Matrix (effective October 2016)* excel matrix file which can be found on the IESO's website at the following location:
http://www.ieso.ca/Pages/Participate/Reliability-Requirements/Reliability-Standards-Compliance.aspx
Additionally, a PDF version is included as Attachment 1 to this Information Request Response 1.01.

b) Hydro One confirms that as a company, it always works in accordance with the **Occupational Health and Safety Act, R.S.O. 1990, c. O.1- O. Reg. 213/91: Construction Projects**. This regulation provides the over-all governance and safety standards for construction projects in Ontario[1].

Additionally, Hydro One's Project construction work will be carried out in accordance with the CSA Group's (formerly the Canadian Standards Association) standard **CSA 22.3 NO. 1-15-Overhead Systems**[2]. This Standard applies to electric supply and communication lines and equipment located entirely outside of buildings and fenced supply stations and applies to existing installations (including maintenance replacements, additions, and alterations) meeting the original designs that currently comply with prior editions of The Standard. This standard forms part of the **Canadian Electrical Code, Part III** requirements for the construction of overhead systems.

Attachment 2 of this Information Request 1.01 provides Hydro One's **Job Step Planning and /Work Operation Tool for Stringing Conductor and/or Sheildwire**. As shown in the Attachment, it requires construction crews to follow two main Hydro One detailed internal standards for this type of construction work. Refer to Attachment 3 of this Information Request 1.01 for the two standards:

- **Stringing System Strength Requirements** [HO 4191 R3]
- **Line Stringing Over 50 kV – Safety Basics** [PR 0164].

In referring to Hydro One's work planning tool for Stringing Conductor and/or Sheildwire (Attachment 2), the document contains two major columns of information. The left column

[1] https://www.ontario.ca/laws/regulation/910213

[2] http://shop.csa.ca/en/canada/canadian-electrical-code-part-iii-electricity-distribution-and-transmission/c223-no-1-15/invt/27014792015

is used to identify and itemize potential 'Work Activities and/or Hazards' that could be required, or present, during a construction job such as the one at the core of this Application. The right hand column of the tool contains, for each item identified, all the Hydro One internal work standards, policies and guidelines that **must** be followed during the performance of each activity/hazard (in addition to any external codes or Acts outlines above (e.g. **OH&S Act, R.S.O. 1990, c. O.1- O. Reg. 213/91**). For reference, the Hydro One Internal Standard can be identified in the table in **Bold** text using nomenclature developed by, and unique to, Hydro One. Hydro One submits that due to the extensive length and size of the list, providing each document in the work planning tool would be excessive given the Tool is designed to cover a wide array of Construction Job types and not each and every item would always be applicable to each and every construction type.

Project construction work, namely the installation of the OPGW and the replacement of the teleprotection systems will be designed, constructed and tested to comply with the external standards referred to and described above, in combination with Hydro One's internally developed standards (including those provided and referred to in the Attachments to this Information Request 1.01 part b) that draw on further applicable standards of the following regulatory agencies and institutes;

Name of Organisation	Provincial / Federal /Other	Applicable Standards
Canadian Standards Association (CSA)	Other (USA, Canada, UK etc.)	The main CSA standards applicable to this project relate to: (1) Construction and Engineering (2) Electrical (3) Energy (4) Environmental (5) Health and Safety (6) Information Technology & Telecommunication (7) Infrastructure (8) Mechanical & Industrial Equipment (9) Quality and Business Management

Electrical Safety Authority (ESA)	Provincial (Ontario)	The Project construction and operation will adhere to following four major areas of regulations established by the ESA: (1) Ontario Electrical Safety Code (2) Licensing of Electrical Contractors and Master Electricians (3) Electrical Distribution Safety (4) Electrical Product Safety.
American National Standards Institute (ANSI)	Other (USA)	ANSI standards as they relate to energy distribution.
International Electrotechnical Commission (IEC)	Other (International)	IEC standards related to power systems transmission, distribution, telecom etc. from this organization.
National Electrical Manufacturers Association (NEMA)	Other (USA)	NEMA standards related to electrical equipment manufacturing.
American Society for Testing and Materials (ASTM)	Other (International)	ASTM standards related to product quality, health and safety etc.
Institute of Electrical and Electronics Engineers (IEEE)	Other (International)	IEEE standards related to electrical and electronics engineering.
Independent Electricity System Operator (IESO)	Provincial	Market Rules, Metering, Market Operations, System Operations, Reliability Compliance The IESO is the organisation that represents NERC in Ontario and will ensure compliance with NERC standards.
Northeast Power Coordinating Council (NPCC)	Other (North America)	The Major specific standard relevant in this is NPCC Directory #4, NPCC Directory #7, NPCC Directory #8East Region)
North American Electric Reliability Corporation (NERC)	Other (North America)	Standards relate to Critical Infrastructure Protection, Protection and Control

1

Hydro One confirms its extensive library of internally developed standards, policy and procedure documents must be followed during any construction or maintenance project. These encompass the requirements from applicable regulatory agencies and institutes and safety councils and laws etc., as listed above. Hydro One has identified and assigned to appropriate staff, the roles the responsibilities to be undertaken to administer and perform an oversight function aimed at ensuring the underlying requirements of all the applicable developed standards are followed. For this Project's construction work, the *Project Team/External Contacts and Accountabilities List* is provided in Attachment 1 to Information Request 1.12, page 2, of the Environmental Specification document.

TOP Matrix - Redline Changes

	red-marked cells refer to the requirements that existed in the current Matrix and will be deleted from the updated matrix either because they are now retired or their accountability don't fall on either of IESO or H1.
	green-marked cells refer to the requirements that are newly added in the updated version (did not exist in the current version).
	yellow-marked cells refer to requirements that existed in the current version and will stay in the updated version; however, the accountability assignment has changed.
	Non-marked cells refer to the requirements that status did not change from the current version to the updated version.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
BAL-005-0.2b	Automatic Generation Control	Effective	R1.2.	Each Transmission Operator with transmission facilities operating in an Interconnection shall ensure that those transmission facilities are included within the metered boundaries of a Balancing Authority Area.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	✓		Each entity is responsible for its own requirements (CIP-003 through CIP-009), except for CIP-002 R1/R2 which requires the IESO to develop the risk-based methodology for identifying each entity's critical assets.	
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.2.	The risk-based assessment shall consider the following assets:	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.2.4.	Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R1.2.7.	Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.	✓			
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R2.	Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R3.	Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	✓	✓	Each entity is responsible for its own requirements (CIP-003 through CIP-009).	
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R3.1.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	✓	✓		
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	✓	✓		
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R3.3.	The Cyber Asset is dial-up accessible.	✓	✓		
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	Effective	R4.	Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	✓	✓		
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	Future Effective	R1.	Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: [Violation Risk Factor: High][Time Horizon: Operations Planning] i.Control Centers and backup Control Centers; ii.Transmission stations and substations; iii.Generation resources; iv.Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v.Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi.For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	Future Effective	R1.1.	Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;	✓			
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	Future Effective	R1.2.	Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and	✓			
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	Future Effective	R1.3.	Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).	✓			
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	Future Effective	R2.	The Responsible Entity shall: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓			
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	Future Effective	R2.1.	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and	✓			
CIP-002-5.1	Cyber Security — BES Cyber System Categorization	Future Effective	R2.2.	Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.	✓			
CIP-003-3	Cyber Security - Security Management Controls	Effective	R1.	Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002-3 through CIP-009-3, including provision for emergency situations.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R2.	Leadership — The Responsible Entity shall assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R2.1.	The senior manager shall be identified by name, title, and date of designation.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R2.3.	Where allowed by Standards CIP-002-3 through CIP-009-3, the senior manager may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented in the same manner as R2.1 and R2.2, and approved by the senior manager.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R2.4.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-003-3	Cyber Security - Security Management Controls	Effective	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002-3, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R4.3.	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R5.1.1.	Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R5.2.	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.	✓	✓		
CIP-003-3	Cyber Security - Security Management Controls	Effective	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-003-3	Cyber Security - Security Management Controls	Effective	R6.	Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	✓	✓		
CIP-003-6	Cyber Security - Security Management Controls	Future Effective	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]	✓	✓		
CIP-003-6	Cyber Security - Security Management Controls	Future Effective	R1.1.	1.1 For its high impact and medium impact BES Cyber Systems, if any: 1.1.1. Personnel and 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.	✓	✓		
CIP-003-6	Cyber Security - Security Management Controls	Future Effective	R1.2.	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 (LERC) and Dial-up Connectivity; and 1.2.4. Cyber Security Incident response	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-003-6	Cyber Security - Security Management Controls	Future Effective	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) for its low impact BES Cyber Systems that include the sections 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.	✓	✓		
CIP-003-6	Cyber Security - Security Management Controls	Future Effective	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]	✓	✓		
CIP-003-6	Cyber Security - Security Management Controls	Future Effective	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]	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R1.	Awareness —The Responsible Entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as: • Direct communications (e.g., emails, memos, computer based training, etc.); • Indirect communications (e.g., posters, intranet, brochures, etc.); • Management support and reinforcement (e.g., presentations, meetings, etc.).	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R2.	Training —The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R2.2.1.	The proper use of Critical Cyber Assets;	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R2.3.	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R3.	Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency. The personnel risk assessment program shall at a minimum include:	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R3.1.	The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and sevenyear criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R3.2.	The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R3.3.	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-3.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R4.	Access —The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R4.1.	The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.	✓	✓		
CIP-004-3a	Cyber Security - Personnel & Training	Effective	R4.2.	The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.	✓	✓		
CIP-004-6	Cyber Security - Personnel & Training	Future Effective	R1.	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-6 Table R1 – Security Awareness Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-004-6	Cyber Security - Personnel & Training	Future Effective	R2.	Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-6 Table R2 – Cyber Security Training Program. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓	✓		
CIP-004-6	Cyber Security - Personnel & Training	Future Effective	R3.	Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-6 Table R3 – Personnel Risk Assessment Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	✓	✓		
CIP-004-6	Cyber Security - Personnel & Training	Future Effective	R4.	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R4 – Access Management Program. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	✓	✓		
CIP-004-6	Cyber Security - Personnel & Training	Future Effective	R5.	Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-6 Table R5 – Access Revocation. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Planning].	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R1.	Electronic Security Perimeter —The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R1.1.	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R1.2.	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R1.3.	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R1.4.	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R1.5.	Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R1.6.	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.	Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.1.	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.2.	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.3.	The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.4.	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.5.	The required documentation shall, at least, identify and describe:	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.5.1.	The processes for access request and authorization.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.5.2.	The authentication methods.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R2.5.4.	The controls used to secure dial-up accessible connections.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R3.	Monitoring Electronic Access —The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R3.1.	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R3.2.	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R4.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R4.1.	A document identifying the vulnerability assessment process;	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R4.4.	A review of controls for default accounts, passwords, and network management community strings;	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R4.5.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R5.	Documentation Review and Maintenance —The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R5.2.	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.	✓	✓		
CIP-005-3a	Cyber Security — Electronic Security Perimeter(s)	Effective	R5.3.	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	✓	✓		
CIP-005-5	Cyber Security — Electronic Security Perimeter(s)	Future Effective	R1.	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-5 Table R1 – Electronic Security Perimeter. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	✓	✓		
CIP-005-5	Cyber Security — Electronic Security Perimeter(s)	Future Effective	R2.	Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-5 Table R2 – Interactive Remote Access Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning and Same Day Operations].	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.	Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.1.	All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.2.	Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.4.	Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.5.	Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.6.	A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.6.1	Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.6.2	Continuous escorted access of visitors within the Physical Security Perimeter.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.7.	Update of the physical security plan within thirty calendar days of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter, physical access controls, monitoring controls, or logging controls.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R1.8.	Annual review of the physical security plan.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R2.	Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R2.1.	Be protected from unauthorized physical access.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R2.2.	Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R3.	Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R4.	Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R5.	Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R6.	Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R7.	Access Log Retention — The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R8.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R8.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R8.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R8.1.	✓	✓		
CIP-006-3c	Cyber Security — Physical Security of Critical Cyber Assets	Effective	R8.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	✓	✓		
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Future Effective	R1.	Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].	✓	✓		
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Future Effective	R2.	Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]	✓	✓		
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Future Effective	R3.	Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R1.	Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R1.1.	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R1.3.	The Responsible Entity shall document test results.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R2.	Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R2.2.	The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R2.3.	In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R3.2.	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R4.	Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R4.1.	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R4.2.	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention “signatures.” The process must address testing and installing the signatures.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.	Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.1.	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.1.2.	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.2.	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.2.1.	The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.2.3.	Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.3.1.	Each password shall be a minimum of six characters.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R6.	Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R6.1.	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R6.3.	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R7.	Disposal or Redeployment — The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R7.1.	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R7.2.	Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R8.	Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R8.1.	A document identifying the vulnerability assessment process;	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R8.2.	A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R8.3.	A review of controls for default accounts; and,	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R8.4.	Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.	✓	✓		
CIP-007-3a	Cyber Security - Systems Security Management	Effective	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007-3 at least annually. Changes resulting from modifications to the systems or controls shall be documented within thirty calendar days of the change being completed.	✓	✓		
CIP-007-6	Cyber Security - Systems Security Management	Future Effective	R1.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations.]	✓	✓		
CIP-007-6	Cyber Security - Systems Security Management	Future Effective	R2.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	✓	✓		
CIP-007-6	Cyber Security - Systems Security Management	Future Effective	R3.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations].	✓	✓		
CIP-007-6	Cyber Security - Systems Security Management	Future Effective	R4.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Same Day Operations and Operations Assessment.]	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-007-6	Cyber Security - Systems Security Management	Future Effective	R5.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	✓	✓		
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	Effective	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:	✓	✓		
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	Effective	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	✓	✓		
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	Effective	R1.2.	Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.	✓	✓		
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	Effective	R1.3.	Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.	✓			
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	Effective	R1.4.	Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.	✓	✓		
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	Effective	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	✓	✓		
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	Effective	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	✓	✓		
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	Effective	R2.	Cyber Security Incident Documentation — The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.	✓	✓		
CIP-008-5	Cyber Security — Incident Reporting and Response Planning	Future Effective	R1.	Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-5 Table R1 – Cyber Security Incident Response Plan Specifications. [Violation Risk Factor: Lower] [Time Horizon: Long Term Planning].	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-008-5	Cyber Security — Incident Reporting and Response Planning	Future Effective	R2.	Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-Time Operations].	✓	✓		
CIP-008-5	Cyber Security — Incident Reporting and Response Planning	Future Effective	R3.	Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].	✓	✓		
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	Effective	R1.	Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:	✓	✓		
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	Effective	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	✓	✓		
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	Effective	R1.2.	Define the roles and responsibilities of responders.	✓	✓		
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	Effective	R2.	Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.	✓	✓		
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	Effective	R3.	Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within thirty calendar days of the change being completed.	✓	✓		
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	Effective	R4.	Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.	✓	✓		
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	Effective	R5.	Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	Future Effective	R1.	Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning].	✓	✓		
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	Future Effective	R2.	Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning and Real-time Operations.]	✓	✓		
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	Future Effective	R3.	Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication. [Violation Risk Factor: Lower] [Time Horizon: Operations Assessment].	✓	✓		
CIP-010-2	Cyber Security — Configuration Change Management and Vulnerability Assessments	Future Effective	R1.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R1 – Configuration Change Management. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	✓	✓		
CIP-010-2	Cyber Security — Configuration Change Management and Vulnerability Assessments	Future Effective	R2.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R2 – Configuration Monitoring. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	✓	✓		
CIP-010-2	Cyber Security — Configuration Change Management and Vulnerability Assessments	Future Effective	R3.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-2 Table R3– Vulnerability Assessments. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]	✓	✓		
CIP-010-2	Cyber Security — Configuration Change Management and Vulnerability Assessments	Future Effective	R4.	Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1. [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning and Operations Planning]	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-011-1	Cyber Security Information Protection	To be retired	R1.	Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-1 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	✓	✓		
CIP-011-1	Cyber Security Information Protection	To be retired	R2.	Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-011-1 Table R2 – BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].	✓	✓		
CIP-011-2	Cyber Security Information Protection	Future Effective	R1.	Each Responsible Entity shall implement one or more documented information protection program(s) that collectively includes each of the applicable requirement parts in CIP-011-2 Table R1 – Information Protection. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning].	✓	✓		
CIP-011-2	Cyber Security Information Protection	Future Effective	R2.	Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning].	✓	✓		
CIP-014-2	Physical Security	Effective	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: [VRF: Medium; Time-Horizon: Operations Planning, Long-term Planning]		✓		R4 and R5 are effective 120 days after the completion of R1.
CIP-014-2	Physical Security	Effective	R4.1.	Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);		✓		R4 and R5 are effective 120 days after the completion of R1.
CIP-014-2	Physical Security	Effective	R4.2.	Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and		✓		R4 and R5 are effective 120 days after the completion of R1.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-014-2	Physical Security	Effective	R4.3.	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.		✓		R4 and R5 are effective 120 days after the completion of R1.
CIP-014-2	Physical Security	Effective	R5.	Each Transmission Owner that identified a Transmission station, Transmission substation, or 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 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: [VRF: High; Time-Horizon: Long-term Planning]		✓		R4 and R5 are effective 120 days after the completion of R1.
CIP-014-2	Physical Security	Effective	R5.1.	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.		✓		R4 and R5 are effective 120 days after the completion of R1.
CIP-014-2	Physical Security	Effective	R5.2.	Law enforcement contact and coordination information.		✓		R4 and R5 are effective as of April 21, 2016 in Ontario.
CIP-014-2	Physical Security	Effective	R5.3.	A timeline for executing the physical security enhancements and modifications specified in the physical security plan.		✓		R4 and R5 are effective 120 days after the completion of R1.
CIP-014-2	Physical Security	Effective	R5.4.	Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).		✓		R4 and R5 are effective 120 days after the completion of R1.
CIP-014-2	Physical Security	Future Effective	R6.	Each Transmission Owner that identified a Transmission station, Transmission substation, or 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 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. [VRF: Medium; Time-Horizon: Long-term Planning]		✓		R6 is effective 90 days after the completion of R4 and R5.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
CIP-014-2	Physical Security	Future Effective	R6.1.	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.		✓		R6 is effective 90 days after the completion of R4 and R5.
CIP-014-2	Physical Security	Future Effective	R6.2.	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.		✓		R6 is effective 90 days after the completion of R4 and R5.
CIP-014-2	Physical Security	Future Effective	R6.3.	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(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.		✓		R6 is effective 90 days after the completion of R4 and R5.
CIP-014-2	Physical Security	Future Effective	R6.4.	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 third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.		✓		R6 is effective 90 days after the completion of R4 and R5.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
COM-001-1.1	Telecommunications	Effective	R4.	Unless agreed to otherwise, each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use English as the language for all communications between and among operating personnel responsible for the real-time generation control and operation of the interconnected Bulk Electric System. Transmission Operators and Balancing Authorities may use an alternate language for internal operations.	✓	✓	The COM standards define the required communication systems and protocols. While each entity is responsible for its own requirements, Hydro One must maintain and follow the communciation protocols of the IESO.	Only R4 of COM-001-1.1 will retire on June 30, 2016 as the retirement of this requirement is pursuant to the Ontario Enforcement Date (July 1, 2016) of COM-002-4 which incorporates this requirement.
COM-001-2.1	Communications	Effective	R3.	Each Transmission Operator shall have Interpersonal Communication capability with the following entities (unless the Transmission Operator detects a failure of its Interpersonal Communication capability in which case Requirement R10 shall apply):	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R3.1.	Its Reliability Coordinator.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R3.2.	Each Balancing Authority within its Transmission Operator Area.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R3.3.	Each Distribution Provider within its Transmission Operator Area.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R3.4.	Each Generator Operator within its Transmission Operator Area.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R3.5.	Each adjacent Transmission Operator synchronously connected.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R3.6.	Each adjacent Transmission Operator asynchronously connected.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R4.	Each Transmission Operator shall designate an Alternative Interpersonal Communication capability with the following entities: [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R4.1.	Its Reliability Coordinator.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R4.2.	Each Balancing Authority within its Transmission Operator Area.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R4.3.	Each adjacent Transmission Operator synchronously connected.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R4.4.	Each adjacent Transmission Operator asynchronously connected.	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
COM-001-2.1	Communications	Effective	R9.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall test its Alternative Interpersonal Communication capability at least once each calendar month. If the test is unsuccessful, the responsible entity shall initiate action to repair or designate a replacement Alternative Interpersonal Communication capability within 2 hours. [Violation Risk Factor: Medium][Time Horizon: Real-time Operations, Same-day Operations]	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-001-2.1	Communications	Effective	R10.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall notify entities as identified in Requirements R1, R3, and R5, respectively within 60 minutes of the detection of a failure of its Interpersonal Communication capability that lasts 30 minutes or longer. [Violation Risk Factor: Medium] [Time Horizon: Real-time Operations]	✓	✓		COM-001-2.1 has an Ontario Enforcement date of November 13, 2015.
COM-002-2	Communications and Coordination	Effective	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall have communications (voice and data links) with appropriate Reliability Coordinators, Balancing Authorities, and Transmission Operators. Such communications shall be staffed and available for addressing a real-time emergency condition.	✓	✓	The COM standards define the required communication systems and protocols. While the requirement applies to the IESO, Hydro One must maintain the systems and follow the protocols of the IESO	COM-002-2 retires on June 30, 2016 in Ontario.
COM-002-2	Communications and Coordination	Effective	R1.1.	Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator, and all other potentially affected Balancing Authorities and Transmission Operators through predetermined communication paths of any condition that could threaten the reliability of its area or when firm load shedding is anticipated.	✓	✓	The COM standards define the required communication systems and protocols. While each entity is responsible for its own requirements, Hydro One must maintain and follow the communication protocols of the IESO.	COM-002-2 retires on June 30, 2016 in Ontario.
COM-002-2	Communications and Coordination	Effective	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall issue directives in a clear, concise, and definitive manner; shall ensure the recipient of the directive repeats the information back correctly; and shall acknowledge the response as correct or repeat the original statement to resolve any misunderstandings.	✓		The COM standards define the required communication systems and protocols. While the requirement applies to the IESO, Hydro One must maintain the systems and follow the protocols of the IESO	COM-002-2 retires on June 30, 2016 in Ontario.
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R1.	Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall develop documented communications protocols for its operating personnel that issue and receive Operating Instructions. The protocols shall, at a minimum: [Violation Risk Factor: Low][Time Horizon: Long-term Planning]	✓	✓		Hydro One will comply with this requirement when communicating with the IESO and other (neighboring) TOPs. The IESO will be responsible for any communication with all other NERC entities.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R1.1.	Require its operating personnel that issue and receive an oral or written Operating Instruction to use the English language, unless agreed to otherwise. An alternate language may be used for internal operations.	✓	✓		
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R1.2.	Require its operating personnel that issue an oral two-party, person-to-person Operating Instruction to take one of the following actions: Confirm the receiver's response if the repeated information is correct. Reissue the Operating Instruction if the repeated information is incorrect or if requested by the receiver. Take an alternative action if a response is not received or if the Operating Instruction was not understood by the receiver.	✓			Hydro One would not issue an Operating Instruction without the IESO's involvement. Thus changed to only's IESO responsibility.
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R1.3.	Require its operating personnel that receive an oral two-party, person-to-person Operating Instruction to take one of the following actions: Repeat, not necessarily verbatim, the Operating Instruction and receive confirmation from the issuer that the response was correct. Request that the issuer reissue the Operating Instruction.	✓	✓		
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R1.4.	Require its operating personnel that issue a written or oral single-party to multiple-party burst Operating Instruction to confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction.	✓			Hydro One would not issue an Operating Instruction without the IESO's involvement. Thus changed to only's IESO responsibility.
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R1.5.	Specify the instances that require time identification when issuing an oral or written Operating Instruction and the format for that time identification.	✓			Hydro One would not issue an Operating Instruction without the IESO's involvement. Thus changed to only's IESO responsibility.
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R1.6.	Specify the nomenclature for Transmission interface Elements and Transmission interface Facilities when issuing an oral or written Operating Instruction.	✓			Hydro One would not issue an Operating Instruction without the IESO's involvement. Thus changed to only's IESO responsibility.
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R2.	Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall conduct initial training for each of its operating personnel responsible for the Real-time operation of the interconnected Bulk Electric System on the documented communications protocols developed in Requirement R1 prior to that individual operator issuing an Operating Instruction. [Violation Risk Factor: Low][Time Horizon: Long-term Planning]	✓	✓		
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R4.	Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall at least once every twelve (12) calendar months: [Violation Risk Factor: Medium][Time Horizon: Operations Planning]	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R4.1.	Assess adherence to the documented communications protocols in Requirement R1 by its operating personnel that issue and receive Operating Instructions, provide feedback to those operating personnel and take corrective action, as deemed appropriate by the entity, to address deviations from the documented protocols.	✓	✓		
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R4.2.	Assess the effectiveness of its documented communications protocols in Requirement R1 for its operating personnel that issue and receive Operating Instructions and modify its documented communication protocols, as necessary.	✓	✓		
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R5.	Each Balancing Authority, Reliability Coordinator, and Transmission Operator that issues an oral two-party, person-to-person Operating Instruction during an Emergency, excluding written or oral single-party to multiple-party burst Operating Instructions, shall either: [Violation Risk Factor: High][Time Horizon: Real-time Operations] ▯ Confirm the receiver's response if the repeated information is correct (in accordance with Requirement R6). ▯ Reissue the Operating Instruction if the repeated information is incorrect or if requested by the receiver, or ▯ Take an alternative action if a response is not received or if the Operating Instruction was not understood by the receiver.	✓			Hydro One would not issue an Operating Instruction without the IESO's involvement. Thus changed to only's IESO responsibility.
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R6.	Each Balancing Authority, Distribution Provider, Generator Operator, and Transmission Operator that receives an oral two-party, person-to-person Operating Instruction during an Emergency, excluding written or oral single-party to multiple-party burst Operating Instructions, shall either: [Violation Risk Factor: High][Time Horizon: Real-time Operations] ▯ Repeat, not necessarily verbatim, the Operating Instruction and receive confirmation from the issuer that the response was correct, or ▯ Request that the issuer reissue the Operating Instruction.	✓	✓		
COM-002-4	Operating Personnel Communications Protocols	Future Effective	R7.	Each Balancing Authority, Reliability Coordinator, and Transmission Operator that issues a written or oral single-party to multiple-party burst Operating Instruction during an Emergency shall confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction. [Violation Risk Factor: High][Time Horizon: Real-time Operations]	✓			Hydro One would not issue an Operating Instruction without the IESO's involvement. Thus changed to only's IESO responsibility.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-001-2.1b	Emergency Operations Planning	Effective	R2.	Each Transmission Operator and Balancing Authority shall:	✓	✓		
EOP-001-2.1b	Emergency Operations Planning	Effective	R2.1.	Develop, maintain, and implement a set of plans to mitigate operating emergencies for insufficient generating capacity.	✓			
EOP-001-2.1b	Emergency Operations Planning	Effective	R2.2.	Develop, maintain, and implement a set of plans to mitigate operating emergencies on the transmission system.	✓	✓		
EOP-001-2.1b	Emergency Operations Planning	Effective	R2.3.	Develop, maintain, and implement a set of plans for load shedding.	✓	✓		
EOP-001-2.1b	Emergency Operations Planning	Effective	R3.	Each Transmission Operator and Balancing Authority shall have emergency plans that will enable it to mitigate operating emergencies. At a minimum, Transmission Operator and Balancing Authority emergency plans shall include:	✓	✓		
EOP-001-2.1b	Emergency Operations Planning	Effective	R3.1.	Communications protocols to be used during emergencies.	✓			
EOP-001-2.1b	Emergency Operations Planning	Effective	R3.2.	A list of controlling actions to resolve the emergency. Load reduction, in sufficient quantity to resolve the emergency within NERC-established timelines, shall be one of the controlling actions.	✓	✓		
EOP-001-2.1b	Emergency Operations Planning	Effective	R3.3.	The tasks to be coordinated with and among adjacent Transmission Operators and Balancing Authorities.	✓	✓		
EOP-001-2.1b	Emergency Operations Planning	Effective	R3.4.	Staffing levels for the emergency.	✓	✓		
EOP-001-2.1b	Emergency Operations Planning	Effective	R4.	Each Transmission Operator and Balancing Authority shall include the applicable elements in Attachment 1-EOP-001 when developing an emergency plan.	✓	✓		
EOP-001-2.1b	Emergency Operations Planning	Effective	R5.	The Transmission Operator and Balancing Authority shall annually review and update each emergency plan. The Transmission Operator and Balancing Authority shall provide a copy of its updated emergency plans to its Reliability Coordinator and to neighboring Transmission Operators and Balancing Authorities.	✓	✓	The IESO shares its Ontario Power System Restoration Plan (OPSRP) with its neighbouring Transmission Operators and Balancing Authorities.	
EOP-001-2.1b	Emergency Operations Planning	Effective	R6.	The Transmission Operator and Balancing Authority shall coordinate its emergency plans with other Transmission Operators and Balancing Authorities as appropriate. This coordination includes the following steps, as applicable:	✓			
EOP-001-2.1b	Emergency Operations Planning	Effective	R6.1.	The Transmission Operator and Balancing Authority shall establish and maintain reliable communications between interconnected systems.	✓			
EOP-001-2.1b	Emergency Operations Planning	Effective	R6.2.	The Transmission Operator and Balancing Authority shall arrange new interchange agreements to provide for emergency capacity or energy transfers if existing agreements cannot be used.	✓			

					Responsibility			
Standard Number	Standard Name	Requirement	Requirement No.	Text of Requirement	IESO	Transmitter	Comments/Details	IESO Comments
EOP-001-2.1b	Emergency Operations Planning	Effective	R6.3.	The Transmission Operator and Balancing Authority shall coordinate transmission and generator maintenance schedules to maximize capacity or conserve the fuel in short supply. (This includes water for hydro generators.)	✓			
EOP-001-2.1b	Emergency Operations Planning	Effective	R6.4.	The Transmission Operator and Balancing Authority shall arrange deliveries of electrical energy or fuel from remote systems through normal operating channels.	✓			
EOP-003-2	Load Shedding Plans	Effective	R1.	After taking all other remedial steps, a Transmission Operator or Balancing Authority operating with insufficient generation or transmission capacity shall shed customer load rather than risk an uncontrolled failure of components or cascading outages of the Interconnection.	✓	✓		
EOP-003-2	Load Shedding Plans	Effective	R2.	Each Transmission Operator shall establish plans for automatic load shedding for undervoltage conditions if the Transmission Operator or its associated Transmission Planner(s) or Planning Coordinator(s) determine that an under-voltage load shedding scheme is required.	✓			
EOP-003-2	Load Shedding Plans	Effective	R3.	Each Transmission Operator and Balancing Authority shall coordinate load shedding plans, excluding automatic under-frequency load shedding plans, among other interconnected Transmission Operators and Balancing Authorities.	✓			
EOP-003-2	Load Shedding Plans	Effective	R4.	A Transmission Operator shall consider one or more of these factors in designing an automatic under voltage load shedding scheme: voltage level, rate of voltage decay, or power flow levels.	✓			
EOP-003-2	Load Shedding Plans	Effective	R5.	A Transmission Operator or Balancing Authority shall implement load shedding, excluding automatic under-frequency load shedding, in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.	✓	✓		
EOP-003-2	Load Shedding Plans	Effective	R6.	After a Transmission Operator or Balancing Authority Area separates from the Interconnection, if there is insufficient generating capacity to restore system frequency following automatic underfrequency load shedding, the Transmission Operator or Balancing Authority shall shed additional load.	✓	✓		
EOP-003-2	Load Shedding Plans	Effective	R7.	The Transmission Operator shall coordinate automatic undervoltage load shedding throughout their areas with tripping of shunt capacitors, and other automatic actions that will occur under abnormal voltage, or power flow conditions	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-003-2	Load Shedding Plans	Effective	R8.	Each Transmission Operator or Balancing Authority shall have plans for operator controlled manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be capable of implementing the load shedding in a timeframe adequate for responding to the emergency.	✓	✓		
EOP-004-2	Event Reporting	Effective	R1.	Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority).	✓	✓	The IESO is the only entity that reports "events" to NERC (ERO). However, for R1 Hydro One is still required to have an Operating Plan that includes the protocol(s) for reporting to other organizations. According to the MOU between the IESO, NERC and NPCC, the IESO is accountable to report to NERC (ERO) and NPCC (RE) on behalf of Ontario. Hydro One will report to the IESO, internally and to law enforcement.	The IESO is the only entity that reports "events" to NERC (ERO). However, for R1 Hydro One is still required to have an Operating Plan that includes the protocol(s) for reporting to other organizations.
EOP-004-2	Event Reporting	Effective	R2.	Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time).	✓	✓	The current acceptable practice is that Hydro One reports all events to the IESO verbally. Writen reports/forms only need to be filled out if explicity requested by the IESO on a case by case basis.	
EOP-004-2	Event Reporting	Effective	R3.	Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year.	✓	✓	The IESO is the only entity that reports "events" to NERC (ERO). However, for R3, Hydro One is still required to have an Operating Plan that includes contact information pursuant to Requirement R1 each calendar year. According to the MOU between the IESO, NERC and NPCC, the IESO is accountable to report to NERC (ERO) and NPCC (RE) on behalf of Ontario. Hydro One will report to the IESO, internally and to law enforcement.	The IESO is the only entity that reports "events" to NERC (ERO). However, for R3 Hydro One is still required to have an Operating Plan that includes contact information pursuant to Requirement R1 each calendar year
EOP-004-3	Event Reporting	Future Effective	R1.	Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2-3 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority). [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓	✓	The IESO is the only entity that reports "events" to NERC (ERO). However, for R1 Hydro One is still required to have an Operating Plan that includes the protocol(s) for reporting to other organizations. According to the MOU between the IESO, NERC and NPCC, the IESO is accountable to report to NERC (ERO) and NPCC (RE) on behalf of Ontario. Hydro One will report to the IESO, internally and to law enforcement.	The IESO is the only entity that reports "events" to NERC (ERO). However, for R1 Hydro One is still required to have an Operating Plan that includes the protocol(s) for reporting to other organizations.
EOP-004-3	Event Reporting	Future Effective	R2.	Each Responsible Entity shall report events per their Operating Plan within 24 hours of recognition of meeting an event type threshold for reporting or by the end of the next business day if the event occurs on a weekend (which is recognized to be 4 PM local time on Friday to 8 AM Monday local time). [Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]	✓	✓	The current acceptable practice is that Hydro One reports all events to the IESO verbally. Writen reports/forms only need to be filled out if explicity requested by the IESO on a case by case basis.	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-004-3	Event Reporting	Future Effective	R3.	Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	✓	✓	The IESO is the only entity that reports "events" to NERC (ERO). However, for R3, Hydro One is still required to have an Operating Plan that includes contact information pursuant to Requirement R1 each calendar year. According to the MOU between the IESO, NERC and NPCC, the IESO is accountable to report to NERC (ERO) and NPCC (RE) on behalf of Ontario. Hydro One will report to the IESO, internally and to law enforcement.	The IESO is the only entity that reports "events" to NERC (ERO). However, for R3 Hydro One is still required to have an Operating Plan that includes contact information pursuant to Requirement R1 each calendar year
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.	Each Transmission Operator shall have a restoration plan approved by its Reliability Coordinator. The restoration plan shall allow for restoring the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shut down area to service, to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include:	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.1.	Strategies for system restoration that are coordinated with the Reliability Coordinator's high level strategy for restoring the Interconnection.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.2.	A description of how all Agreements or mutually agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.3.	Procedures for restoring interconnections with other Transmission Operators under the direction of the Reliability Coordinator.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.4.	Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.5.	Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.6.	Identification of acceptable operating voltage and frequency limits during restoration.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.7.	Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.8.	Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R1.9.	Operating Processes for transferring authority back to the Balancing Authority in accordance with the Reliability Coordinator's criteria.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R2.	Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R3.	Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually agreed predetermined schedule.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R4.	Each Transmission Operator shall update its restoration plan within 90 calendar days after identifying any unplanned permanent System modifications, or prior to implementing a planned BES modification, that would change the implementation of its restoration plan.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R4.1.	Each Transmission Operator shall submit its revised restoration plan to itsReliability Coordinator for approval within the same 90 calendar day period.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R5.	Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its implementation date.	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R6.	Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify:	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R6.1.	The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R6.2.	The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R6.3.	The capability of generating resources required to control voltages and frequency within acceptable operating limits.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-005-2	System Restoration from Blackstart Resources	Effective	R7.	Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, each affected Transmission Operator shall implement its restoration plan. If the restoration plan cannot be executed as expected the Transmission Operator shall utilize its restoration strategies to facilitate restoration.	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R8.	Following a Disturbance in which one or more areas of the BES shuts down and the use of Blackstart Resources is required to restore the shut down area to service, the Transmission Operator shall resynchronize area(s) with neighboring Transmission Operator area(s) only with the authorization of the Reliability Coordinator or in accordance with the established procedures of the Reliability Coordinator.	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R9.	Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include:	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R9.1.	The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R9.2.	A list of required tests including:	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R9.2.1.	The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R9.2.2.	The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R9.3.	The minimum duration of each of the required tests.	✓			
EOP-005-2	System Restoration from Blackstart Resources	Effective	R10.	Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators to assure the proper execution of its restoration plan. This training program shall include training on the following:	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-005-2	System Restoration from Blackstart Resources	Effective	R10.1.	System restoration plan including coordination with the Reliability Coordinator and Generator Operators included in the restoration plan.	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R10.2.	Restoration priorities.	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R10.3.	Building of cranking paths.	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R10.4.	Synchronizing (re-energized sections of the System).	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R11.	Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks.		✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R12.	Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator.	✓	✓		
EOP-005-2	System Restoration from Blackstart Resources	Effective	R13.	Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements.	✓			
EOP-008-1	Loss of Control Center Functionality	Effective	R1.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a current Operating Plan describing the manner in which it continues to meet its functional obligations with regard to the reliable operations of the BES in the event that its primary control center functionality is lost. This Operating Plan for backup functionality shall include the following, at a minimum:	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.1	The location and method of implementation for providing backup functionality for the time it takes to restore the primary control center functionality.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.2.	A summary description of the elements required to support the backup functionality. These elements shall include, at a minimum:	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.2.1.	Tools and applications to ensure that System Operators have situational awareness of the BES.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.2.2.	Data communications.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-008-1	Loss of Control Center Functionality	Effective	R1.2.3.	Voice communications.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.2.4.	Power source(s).	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.2.5.	Physical and cyber security.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.3.	An Operating Process for keeping the backup functionality consistent with the primary control center.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.4.	Operating Procedures, including decision authority, for use in determining when to implement the Operating Plan for backup functionality.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.5.	A transition period between the loss of primary control center functionality and the time to fully implement the backup functionality that is less than or equal to two hours.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.6.	An Operating Process describing the actions to be taken during the transition period between the loss of primary control center functionality and the time to fully implement backup functionality elements identified in Requirement R1, Part 1.2. The Operating Process shall include at a minimum:	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.6.1.	A list of all entities to notify when there is a change in operating locations.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.6.2.	Actions to manage the risk to the BES during the transition from primary to backup functionality as well as during outages of the primary or backup functionality.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R1.6.3.	Identification of the roles for personnel involved during the initiation and implementation of the Operating Plan for backup functionality.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R2.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a copy of its current Operating Plan for backup functionality available at its primary control center and at the location providing backup functionality.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-008-1	Loss of Control Center Functionality	Effective	R4.	Each Balancing Authority and Transmission Operator shall have backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) that includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that depend on a Balancing Authority and Transmission Operator's primary control center functionality respectively. To avoid requiring tertiary functionality, backup functionality is not required during: • Planned outages of the primary or backup functionality of two weeks or less • Unplanned outages of the primary or backup functionality	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R5.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator, shall annually review and approve its Operating Plan for backup functionality.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R5.1.	An update and approval of the Operating Plan for backup functionality shall take place within sixty calendar days of any changes to any part of the Operating Plan described in Requirement R1.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R6.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have primary and backup functionality that do not depend on each other for the control center functionality required to maintain compliance with Reliability Standards.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R7.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct and document results of an annual test of its Operating Plan that demonstrates:	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R7.1.	The transition time between the simulated loss of primary control center functionality and the time to fully implement the backup functionality.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R7.2.	The backup functionality for a minimum of two continuous hours.	✓	✓		
EOP-008-1	Loss of Control Center Functionality	Effective	R8.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator that has experienced a loss of its primary or backup functionality and that anticipates that the loss of primary or backup functionality will last for more than six calendar months shall provide a plan to its Regional Entity within six calendar months of the date when the functionality is lost, showing how it will re-establish primary or backup functionality.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-010-1	Geomagnetic Disturbance Operations	Effective	R3	Each Transmission Operator shall develop, maintain, and implement a GMD Operating Procedure or Operating Process to mitigate the effects of GMD events on the reliable operation of its respective system. At a minimum, the Operating Procedure or Operating Process shall include: [Violation Risk Factor: Medium] [Time Horizon: Long-term Planning, Operations Planning, Same-day Operations, Real-Time Operations]	✓	✓		
EOP-010-1	Geomagnetic Disturbance Operations	Effective	R3.1	Steps or tasks to receive space weather information.	✓	✓		
EOP-010-1	Geomagnetic Disturbance Operations	Effective	R3.2	System Operator actions to be initiated based on predetermined conditions.	✓	✓		
EOP-010-1	Geomagnetic Disturbance Operations	Future Effective	R3.3.	The conditions for terminating the Operating Procedure or Operating Process.	✓	✓		
EOP-011-1	Emergency Operations	Future Effective	R1.	Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable: [Violation Risk Factor: High] [Time Horizon: Real-Time Operations, Operations Planning, Long-term Planning]	✓	✓		
EOP-011-1	Emergency Operations	Future Effective	R1.1.	Roles and responsibilities for activating the Operating Plan(s);	✓			
EOP-011-1	Emergency Operations	Future Effective	R1.2.	Processes to prepare for and mitigate Emergencies including:	✓			
EOP-011-1	Emergency Operations	Future Effective	R1.2.1.	Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;	✓			
EOP-011-1	Emergency Operations	Future Effective	R1.2.2.	Cancellation or recall of Transmission and generation outages;	✓			
EOP-011-1	Emergency Operations	Future Effective	R1.2.3.	Transmission system reconfiguration;	✓	✓	MR 5, Section 3.4.1.4 (Obligations of Transmitters) MR 5, Section 5.1.2.10 (System Security Obligations) MR 5, Section 5.9 (Operation under a High-Risk Operating State) MR 5, Section 10.3 (Demand Control Initiated by the IESO in an Emergency Operating State)	
EOP-011-1	Emergency Operations	Future Effective	R1.2.4.	Redispatch of generation request;	✓			
EOP-011-1	Emergency Operations	Future Effective	R1.2.5.	Provisions for operator-controlled manual Load shedding that minimizes the overlap with automatic Load shedding and are capable of being implemented in a timeframe adequate for mitigating the Emergency; and	✓	✓	MR 5, Section 10 (Demand Control) MR 5, Section 3.4.1.2 (Obligations	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
EOP-011-1	Emergency Operations	Future Effective	R1.2.6.	Reliability impacts of extreme weather conditions.	✓			
EOP-011-1	Emergency Operations	Future Effective	R4.	Each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator within a time period specified by its Reliability Coordinator. [Violation Risk Factor: High] [Time Horizon: Operation Planning]	✓	✓		
FAC-014-2	Establish and Communicate System Operating Limits	Effective	R2.	The Transmission Operator shall establish SOLs (as directed by its Reliability Coordinator) for its portion of the Reliability Coordinator Area that are consistent with its Reliability Coordinator's SOL Methodology.	✓			
FAC-014-2	Establish and Communicate System Operating Limits	Effective	R5.2.	The Transmission Operator shall provide any SOLs it developed to its Reliability Coordinator and to the Transmission Service Providers that share its portion of the Reliability Coordinator Area.	✓			
IRO-001-1.1	Reliability Coordination - Responsibilities and Authorities	Effective	R8.	Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. Under these circumstances, the Transmission Operator, Balancing Authority, Generator Operator, Transmission Service Provider, Load-Serving Entity, or Purchasing-Selling Entity shall immediately inform the Reliability Coordinator of the inability to perform the directive so that the Reliability Coordinator may implement alternate remedial actions.	✓	✓		
IRO-001-4	Reliability Coordination – Responsibilities	Future Effective	R2.	Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall comply with its Reliability Coordinator's Operating Instructions unless compliance with the Operating Instructions cannot be physically implemented or unless such actions would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
IRO-001-4	Reliability Coordination – Responsibilities	Future Effective	R3.	Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall inform its Reliability Coordinator of its inability to perform the Operating Instruction issued by its Reliability Coordinator in Requirement R1. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-time Operations]	✓			
IRO-002-2	Reliability Coordination - Facilities	Effective	R2.	Each Reliability Coordinator — or its Transmission Operators and Balancing Authorities — shall provide, or arrange provisions for, data exchange to other Reliability Coordinators or Transmission Operators and Balancing Authorities via a secure network.	✓			
IRO-004-2	Reliability Coordination - Operations Planning	Effective	R1.	Each Transmission Operator, Balancing Authority, and Transmission Service Provider shall comply with the directives of its Reliability Coordinator based on the next day assessments in the same manner in which it would comply during real time operating events.	✓	✓		
IRO-005-3.1a	Reliability Coordination — Current Day Operations	Effective	R5.	Each Reliability Coordinator shall monitor system frequency and its Balancing Authorities' performance and direct any necessary rebalancing to return to CPS and DCS compliance. The Transmission Operators and Balancing Authorities shall utilize all resources, including firm load shedding, as directed by its Reliability Coordinator to relieve the emergent condition.	✓	✓		
IRO-005-3.1a	Reliability Coordination — Current Day Operations	Effective	R9.	Whenever a Special Protection System that may have an inter-Balancing Authority, or inter-Transmission Operator impact (e.g., could potentially affect transmission flows resulting in a SOL or IROL violation) is armed, the Reliability Coordinators shall be aware of the impact of the operation of that Special Protection System on inter-area flows. The Transmission Operator shall immediately inform the Reliability Coordinator of the status of the Special Protection System including any degradation or potential failure to operate as expected.	✓	✓		
IRO-005-3.1a	Reliability Coordination — Current Day Operations	Effective	R10.	In instances where there is a difference in derived limits, the Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities shall always operate the Bulk Electric System to the most limiting parameter.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
IRO-010-1a	Reliability Coordinator Data Specification and Collection	Effective	R3.	Each Balancing Authority, Generator Owner, Generator Operator, Interchange Authority, Load-serving Entity, Reliability Coordinator, Transmission Operator, and Transmission Owner shall provide data and information, as specified, to the Reliability Coordinator(s) with which it has a reliability relationship. (Violation Risk Factor: Medium) (Time Horizon: Operations Planning; Same-day Operations; Real-time Operations)	✓	✓		
IRO-010-2	Reliability Coordinator Data Specification and Collection	Future Effective	R3.	Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Load-Serving Entity, Transmission Operator, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R2 shall satisfy the obligations of the documented specifications using: (Violation Risk Factor: Medium) (Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations)	✓	✓	Hydro One is the TO	
IRO-010-2	Reliability Coordinator Data Specification and Collection	Future Effective	R3.1.	A mutually agreeable format	✓	✓	Hydro One is the TO	
IRO-010-2	Reliability Coordinator Data Specification and Collection	Future Effective	R3.2.	A mutually agreeable process for resolving data conflicts	✓	✓	Hydro One is the TO	
IRO-010-2	Reliability Coordinator Data Specification and Collection	Future Effective	R3.3.	A mutually agreeable security protocol	✓	✓	Hydro One is the TO	
IRO-017-1	Outage Coordination	Future Effective	R2.	Each Transmission Operator and Balancing Authority shall perform the functions specified in its Reliability Coordinator's outage coordination process. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	✓	✓	Hydro One has an extensive Outage Planning department, which communicates the TO outages with the RC IESO	
MOD-001-1a	Available Transmission System Capability	Effective	R1.	Each Transmission Operator shall select one of the methodologies listed below for calculating Available Transfer Capability (ATC) or Available Flowgate Capability (AFC) for each ATC Path per time period identified in R2 for those Facilities within its Transmission operating area: [Time Horizon: Operations Planning] ? The Area Interchange Methodology, as described in MOD-028 ? The Rated System Path Methodology, as described in MOD-029 ? The Flowgate Methodology, as described in MOD-030	✓			
MOD-001-1a	Available Transmission System Capability	Effective	R6.	When calculating Total Transfer Capability (TTC) or Total Flowgate Capability (TFC) the Transmission Operator shall use assumptions no more limiting than those used in the planning of operations for the corresponding time period studied, providing such planning of operations has been performed for that time period. [Time Horizon: Operations Planning]	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R1.	Each Transmission Operator shall prepare and keep current a TRM Implementation Document (TRMID) that includes, as a minimum, the following information: [Time Horizon: Operations Planning]	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R1.1.	Identification of (on each of its respective ATC Paths or Flowgates) each of the following components of uncertainty if used in establishing TRM, and a description of how that component is used to establish a TRM value: - Aggregate Load forecast. - Load distribution uncertainty. - Forecast uncertainty in Transmission system topology (including, but not limited to, forced or unplanned outages and maintenance outages). - Allowances for parallel path (loop flow) impacts. - Allowances for simultaneous path interactions. - Variations in generation dispatch (including, but not limited to, forced or unplanned outages, maintenance outages and location of future generation). - Short-term System Operator response (Operating Reserve actions). - Reserve sharing requirements. - Inertial response and frequency bias.	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R1.2.	The description of the method used to allocate TRM across ATC Paths or Flowgates.	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R1.3.	The identification of the TRM calculation used for the following time periods:	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R1.3.1.	Same day and real-time.	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R1.3.2.	Day-ahead and pre-schedule.	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R1.3.3.	Beyond day-ahead and pre-schedule, up to thirteen months ahead.	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R2.	Each Transmission Operator shall only use the components of uncertainty from R1.1 to establish TRM, and shall not include any of the components of Capacity Benefit Margin (CBM). Transmission capacity set aside for reserve sharing agreements can be included in TRM. [Time Horizon: Operations Planning]	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R3.	Each Transmission Operator shall make available its TRMID, and if requested, underlying documentation (if any) used to determine TRM, in the format used by the Transmission Operator, to any of the following who make a written request no more than 30 calendar days after receiving the request. [Time Horizon: Operations Planning] • Transmission Service Providers • Reliability Coordinators • Planning Coordinators • Transmission Planner • Transmission Operators	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R4.	Each Transmission Operator that maintains TRM shall establish TRM values in accordance with the TRMID at least once every 13 months. [Time Horizon: Operations Planning]	✓			
MOD-008-1	Transmission Reliability Margin Calculation Methodology	Effective	R5.	The Transmission Operator that maintains TRM shall provide the TRM values to its Transmission Service Provider(s) and Transmission Planner(s) no more than seven calendar days after a TRM value is initially established or subsequently changed. [Time Horizon: Operations Planning]	✓			
MOD-028-2	Area Interchange Methodology	Effective	R2.	When calculating TTC for ATC Paths, the Transmission Operator shall use a Transmission model that contains all of the following: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓			
MOD-028-2	Area Interchange Methodology	Effective	R2.1.	Modeling data and topology of its Reliability Coordinator's area of responsibility. Equivalent representation of radial lines and facilities 161 kV or below is allowed.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R2.2.	Modeling data and topology (or equivalent representation) for immediately adjacent and beyond Reliability Coordination areas.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R2.3.	Facility Ratings specified by the Generator Owners and Transmission Owners.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R3.	When calculating TTCs for ATC Paths, the Transmission Operator shall include the following data for the Transmission Service Provider's area. The Transmission Operator shall also include the following data associated with Facilities that are explicitly represented in the Transmission model, as provided by adjacent Transmission Service Providers and any other Transmission Service Providers with which coordination agreements have been executed: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓			
MOD-028-2	Area Interchange Methodology	Effective	R3.1.	For TTCs, use the following (as well as any other values and additional parameters as specified in the ATCID):	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-028-2	Area Interchange Methodology	Effective	R3.1.1.	Expected generation and Transmission outages, additions, and retirements, included as specified in the ATCID.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R3.1.2.	A daily or hourly load forecast for TTCs used in current-day and next-day ATC calculations.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R3.1.3.	A daily load forecast for TTCs used in ATC calculations for days two through 31.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R3.1.4.	A monthly load forecast for TTCs used in ATC calculations for months two through 13 months TTCs.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R3.1.5.	Unit commitment and dispatch order, to include all designated network resources and other resources that are committed or have the legal obligation to run, (within or out of economic dispatch) as they are expected to run.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R4.	When calculating TTCs for ATC Paths, the Transmission Operator shall meet all of the following conditions: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓			
MOD-028-2	Area Interchange Methodology	Effective	R4.1.	Use all Contingencies meeting the criteria described in the ATCID.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R4.2.	Respect any contractual allocations of TTC.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R4.3.	Include, for each time period, the Firm Transmission Service expected to be scheduled as specified in the ATCID (filtered to reduce or eliminate duplicate impacts from transactions using Transmission service from multiple Transmission Service Providers) for the Transmission Service Provider, all adjacent Transmission Service Providers, and any Transmission Service Providers with which coordination agreements have been executed modeling the source and sink as follows: - If the source, as specified in the ATCID, has been identified in the reservation and it is discretely modeled in the Transmission Service Provider's Transmission model, use the discretely modeled point as the source. - If the source, as specified in the ATCID, has been identified in the reservation and the point can be mapped to an "equivalence" or "aggregate representation" in the Transmission Service Provider's Transmission model, use the modeled equivalence or aggregate as the source. - If the source, as specified in the ATCID, has been identified in the reservation and the point cannot be mapped to a discretely modeled point, an "equivalence," or an "aggregate	✓			
MOD-028-2	Area Interchange Methodology	Effective	R5.	Each Transmission Operator shall establish TTC for each ATC Path as defined below: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓			
MOD-028-2	Area Interchange Methodology	Effective	R5.1.	At least once within the seven calendar days prior to the specified period for TTCs used in hourly and daily ATC calculations.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-028-2	Area Interchange Methodology	Effective	R5.2.	At least once per calendar month for TTCs used in monthly ATC calculations.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R5.3.	Within 24 hours of the unexpected outage of a 500 kV or higher transmission Facility or a transformer with a low-side voltage of 200 kV or higher for TTCs in effect during the anticipated duration of the outage, provided such outage is expected to last 24 hours or longer.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R6.	Each Transmission Operator shall establish TTC for each ATC Path using the following process: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓			
MOD-028-2	Area Interchange Methodology	Effective	R6.1.	Determine the incremental Transfer Capability for each ATC Path by increasing generation and/or decreasing load within the source Balancing Authority area and decreasing generation and/or increasing load within the sink Balancing Authority area until either: - A System Operating Limit is reached on the Transmission Service Provider's system, or - A SOL is reached on any other adjacent system in the Transmission model that is not on the study path and the distribution factor is 5% or greater1.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R6.2.	If the limit in step R6.1 can not be reached by adjusting any combination of load or generation, then set the incremental Transfer Capability by the results of the case where the maximum adjustments were applied.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R6.3.	Use (as the TTC) the lesser of: – The sum of the incremental Transfer Capability and the impacts of Firm Transmission Services, as specified in the Transmission Service Provider's ATCID, that were included in the study model, or – The sum of Facility Ratings of all ties comprising the ATC Path.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R6.4.	For ATC Paths whose capacity uses jointly-owned or allocated Facilities, limit TTC for each Transmission Service Provider so the TTC does not exceed each Transmission Service Provider's contractual rights.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R7.	The Transmission Operator shall provide the Transmission Service Provider of that ATC Path with the most current value for TTC for that ATC Path no more than: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]	✓			
MOD-028-2	Area Interchange Methodology	Effective	R7.1.	One calendar day after its determination for TTCs used in hourly and daily ATC calculations.	✓			
MOD-028-2	Area Interchange Methodology	Effective	R7.2.	Seven calendar days after its determination for TTCs used in monthly ATC calculations.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-029-1a	Rated System Path Methodology	Effective	R1.	When calculating TTCs for ATC Paths, the Transmission Operator shall use a Transmission model which satisfies the following requirements: [Time Horizon: Operations Planning]	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.	The model utilizes data and assumptions consistent with the time period being studied and that meets the following criteria:	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.1.	Includes at least:	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.1.1.	The Transmission Operator area. Equivalent representation of radial lines and facilities 161kV or below is allowed.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.1.2.	All Transmission Operator areas contiguous with its own Transmission Operator area. (Equivalent representation is allowed.)	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.1.3.	Any other Transmission Operator area linked to the Transmission Operator's area by joint operating agreement. (Equivalent representation is allowed.)	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.10.	Includes any other modeling requirements or criteria specified in the ATCID.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.2.	Models all system Elements as in-service for the assumed initial conditions.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.3.	Models all generation (may be either a single generator or multiple generators) that is greater than 20 MVA at the point of interconnection in the studied area.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.4.	Models phase shifters in non-regulating mode, unless otherwise specified in the Available Transfer Capability Implementation Document (ATCID).	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.5.	Uses Load forecast by Balancing Authority.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.6.	Uses Transmission Facility additions and retirements.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.7.	Uses Generation Facility additions and retirements.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.8.	Uses Special Protection System (SPS) models where currently existing or projected for implementation within the studied time horizon.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.1.9.	Models series compensation for each line at the expected operating level unless specified otherwise in the ATCID.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R1.2.	Uses Facility Ratings as provided by the Transmission Owner and Generator Owner	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.	The Transmission Operator shall use the following process to determine TTC: [Time Horizon: Operations Planning]	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.1.	Except where otherwise specified within MOD-029-1, adjust base case generation and Load levels within the updated power flow model to determine the TTC (maximum flow or reliability limit) that can be simulated on the ATC Path while at the same time satisfying all planning criteria contingencies as follows:	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-029-1a	Rated System Path Methodology	Effective	R2.1.1.	When modeling normal conditions, all Transmission Elements will be modeled at or below 100% of their continuous rating.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.1.2.	When modeling contingencies the system shall demonstrate transient, dynamic and voltage stability, with no Transmission Element modeled above its Emergency Rating.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.1.3.	Uncontrolled separation shall not occur.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.2.	Where it is impossible to actually simulate a reliability-limited flow in a direction counter to prevailing flows (on an alternating current Transmission line), set the TTC for the non-prevailing direction equal to the TTC in the prevailing direction. If the TTC in the prevailing flow direction is dependant on a Special Protection System (SPS), set the TTC for the non-prevailing flow direction equal to the greater of the maximum flow that can be simulated in the non-prevailing flow direction or the maximum TTC that can be achieved in the prevailing flow direction without use of a SPS.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.3.	For an ATC Path whose capacity is limited by contract, set TTC on the ATC Path at the lesser of the maximum allowable contract capacity or the reliability limit as determined by R2.1.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.4.	For an ATC Path whose TTC varies due to simultaneous interaction with one or more other paths, develop a nomogram describing the interaction of the paths and the resulting TTC under specified conditions.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.5.	The Transmission Operator shall identify when the TTC for the ATC Path being studied has an adverse impact on the TTC value of any existing path. Do this by modeling the flow on the path being studied at its proposed new TTC level simultaneous with the flow on the existing path at its TTC level while at the same time honoring the reliability criteria outlined in R2.1. The Transmission Operator shall include the resolution of this adverse impact in its study report for the ATC Path.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.6.	Where multiple ownership of Transmission rights exists on an ATC Path, allocate TTC of that ATC Path in accordance with the contractual agreement made by the multiple owners of that ATC Path.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R2.7.	For ATC Paths whose path rating, adjusted for seasonal variance, was established, known and used in operation since January 1, 1994, and no action has been taken to have the path rated using a different method, set the TTC at that previously established amount.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-029-1a	Rated System Path Methodology	Effective	R2.8.	Create a study report that describes the steps above that were undertaken (R2.1 - R2.7), including the contingencies and assumptions used, when determining the TTC and the results of the study. Where three phase fault damping is used to determine stability limits, that report shall also identify the percent used and include justification for use unless specified otherwise in the ATCID.	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R3.	Each Transmission Operator shall establish the TTC at the lesser of the value calculated in R2 or any System Operating Limit (SOL) for that ATC Path. [Time Horizon: Operations Planning]	✓			
MOD-029-1a	Rated System Path Methodology	Effective	R4.	Within seven calendar days of the finalization of the study report, the Transmission Operator shall make available to the Transmission Service Provider of the ATC Path, the most current value for TTC and the TTC study report documenting the assumptions used and steps taken in determining the current value for TTC for that ATC Path. [Time Horizon: Operations Planning]	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.	The Transmission Operator shall perform the following: [Time Horizon: Operations Planning]	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.	Include Flowgates used in the AFC process based, at a minimum, on the following criteria:	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.1.	Results of a first Contingency transfer analysis for ATC Paths internal to a Transmission Operator's system up to the path capability such that at a minimum the first three limiting Elements and their worst associated Contingency combinations with an OTDF of at least 5% and within the Transmission Operator's system are included as Flowgates.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.1.1.	Use first Contingency criteria consistent with those first Contingency criteria used in planning of operations for the applicable time periods, including use of Special Protection Systems.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.1.2.	Only the most limiting element in a series configuration needs to be included as a Flowgate.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.1.3.	If any limiting element is kept within its limit for its associated worst Contingency by operating within the limits of another Flowgate, then no new Flowgate needs to be established for such limiting elements or Contingencies.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-030-2	Flowgate Methodology	Effective	R2.1.2.	Results of a first Contingency transfer analysis from all adjacent Balancing Authority source and sink (as defined in the ATCID) combinations up to the path capability such that at a minimum the first three limiting Elements and their worst associated Contingency combinations with an Outage Transfer Distribution Factor (OTDF) of at least 5% and within the Transmission Operator's system are included as Flowgates unless the interface between such adjacent Balancing Authorities is accounted for using another ATC methodology.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.2.1.	Use first Contingency criteria consistent with those first Contingency criteria used in planning of operations for the applicable time periods, including use of Special Protection Systems.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.2.2.	Only the most limiting element in a series configuration needs to be included as a Flowgate.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.2.3.	If any limiting element is kept within its limit for its associated worst Contingency by operating within the limits of another Flowgate, then no new Flowgate needs to be established for such limiting elements or Contingencies.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.3.	Any limiting Element/Contingency combination at least within its Reliability Coordinator's Area that has been subjected to an Interconnection-wide congestion management procedure within the last 12 months, unless the limiting Element/Contingency combination is accounted for using another ATC methodology or was created to address temporary operating conditions.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.4.	Any limiting Element/Contingency combination within the Transmission model that has been requested to be included by any other Transmission Service Provider using the Flowgate Methodology or Area Interchange Methodology, where:	✓			

					Responsibility			
Standard Number	Standard Name	Requirement	Requirement No.	Text of Requirement	IESO	Transmitter	Comments/Details	IESO Comments
MOD-030-2	Flowgate Methodology	Effective	R2.1.4.1.	The coordination of the limiting Element/Contingency combination is not already addressed through a different methodology, and - Any generator within the Transmission Service Provider's area has at least a 5% Power Transfer Distribution Factor (PTDF) or Outage Transfer Distribution Factor (OTDF) impact on the Flowgate when delivered to the aggregate load of its own area, or - A transfer from any Balancing Area within the Transmission Service Provider's area to a Balancing Area adjacent has at least a 5% PTDF or OTDF impact on the Flowgate. - The Transmission Operator may utilize distribution factors less than 5% if desired.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.1.4.2.	The limiting Element/Contingency combination is included in the requesting Transmission Service Provider's methodology.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.2.	At a minimum, establish a list of Flowgates by creating, modifying, or deleting Flowgate definitions at least once per calendar year.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.3.	At a minimum, establish a list of Flowgates by creating, modifying, or deleting Flowgates that have been requested as part of R2.1.4 within thirty calendar days from the request.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.4.	Establish the TFC of each of the defined Flowgates as equal to: - For thermal limits, the System Operating Limit (SOL) of the Flowgate. - For voltage or stability limits, the flow that will respect the SOL of the Flowgate.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.5.	At a minimum, establish the TFC once per calendar year.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.5.1.	If notified of a change in the Rating by the Transmission Owner that would affect the TFC of a flowgate used in the AFC process, the TFC should be updated within seven calendar days of the notification.	✓			
MOD-030-2	Flowgate Methodology	Effective	R2.6.	Provide the Transmission Service Provider with the TFCs within seven calendar days of their establishment.	✓			
MOD-030-2	Flowgate Methodology	Effective	R3.	The Transmission Operator shall make available to the Transmission Service Provider a Transmission model to determine Available Flowgate Capability (AFC) that meets the following criteria: [Time Horizon: Operations Planning]	✓			
MOD-030-2	Flowgate Methodology	Effective	R3.1.	Contains generation Facility Ratings, such as generation maximum and minimum output levels, specified by the Generator Owners of the Facilities within the model.	✓			
MOD-030-2	Flowgate Methodology	Effective	R3.2.	Updated at least once per day for AFC calculations for intra-day, next day, and days two through 30.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
MOD-030-2	Flowgate Methodology	Effective	R3.3.	Updated at least once per month for AFC calculations for months two through 13.	✓			
MOD-030-2	Flowgate Methodology	Effective	R3.4.	Contains modeling data and system topology for the Facilities within its Reliability Coordinator's Area. Equivalent representation of radial lines and Facilities161kV or below is allowed.	✓			
MOD-030-2	Flowgate Methodology	Effective	R3.5.	Contains modeling data and system topology (or equivalent representation) for immediately adjacent and beyond Reliability Coordination Areas.	✓			
MOD-033-1	Steady-State and Dynamic System Model Validation	Future Effective	R2.	Each Reliability Coordinator and Transmission Operator shall provide actual system behavior data (or a written response that it does not have the requested data) to any Planning Coordinator performing validation under Requirement R1 within 30 calendar days of a written request, such as, but not limited to, state estimator case or other Real-time data (including disturbance data recordings) necessary for actual system response validation. [Violation Risk Factor: Lower] [Time Horizon: Long-term Planning]	✓			
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R2	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R3	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator.:	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R4	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R4.1	Incorporate the NPIRs into their operating analyses of the electric system.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R4.2	Operate the electric system to meet the NPIRs.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R4.3	Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R6	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R8	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include the following elements in aggregate within the Agreement(s) identified in R2. --Where multiple Agreements with a single Transmission Entity are put into effect, the R9 elements must be addressed in aggregate within the Agreements; however, each Agreement does not have to contain each element. The Nuclear Plant Generator Operator and the Transmission Entity are responsible for ensuring all the R9 elements are addressed in aggregate within the Agreements. -- Where Agreements with multiple Transmission Entities are required, the Nuclear Plant Generator Operator is responsible for ensuring all the R9 elements are addressed in aggregate within the Agreements with the Transmission Entities. The Agreements with each Transmission Entity do not have to contain each element; however, the Agreements with the multiple Transmission Entities, in the aggregate, must address all R9 elements. For each Agreement(s), the Nuclear Plant Generator Operator and the Transmission Entity are responsible to ensure the Agreement(s) contain(s) the elements of R9 applicable to that	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.2	Technical requirements and analysis:	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.2.1	Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the Agreement.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.2.2	Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.2.3	Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.3	Operations and maintenance coordination	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.3.1	Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.3.2	Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.3.3	Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.3.4	Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.3.5	Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.3.6	Coordination of physical and cyber security protection at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.3.7	Coordination of the NPIRs with transmission system Remedial Action Schemes and any programs that reduce or shed load based on underfrequency or undervoltage.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.4	Communications and training Administrative elements:	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.4.1	Provisions for communications affecting the NPIRs between the Nuclear Plant Generator Operator and Transmission Entities, including	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.4.2	Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.4.3	Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.4.4	Provisions for supplying information necessary to report to government agencies, as related to NPIRs.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.
NUC-001-3	Nuclear Plant Interface Coordination	Effective	R9.4.5	Provisions for personnel training, as related to NPIRs.	✓	✓		NUC-001-3 was enforced in Ontario on April 1, 2016.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
PER-001-0.2	Operating Personnel Responsibility and Authority	Effective	R1.	Each Transmission Operator and Balancing Authority shall provide operating personnel with the responsibility and authority to implement real-time actions to ensure the stable and reliable operation of the Bulk Electric System.	✓	✓		
PER-003-1	Operating Personnel Credentials	Effective	R2.	Each Transmission Operator shall staff its Real-time operating positions performing Transmission Operator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates (1	✓	✓		
PER-003-1	Operating Personnel Credentials	Effective	R2.1.	Areas of Competency	✓	✓		
PER-003-1	Operating Personnel Credentials	Effective	R2.1.1.	Transmission operations	✓	✓		
PER-003-1	Operating Personnel Credentials	Effective	R2.1.2.	Emergency preparedness and operations	✓	✓		
PER-003-1	Operating Personnel Credentials	Effective	R2.1.3.	System operations	✓	✓		
PER-003-1	Operating Personnel Credentials	Effective	R2.1.4.	Protection and control	✓	✓		
PER-003-1	Operating Personnel Credentials	Effective	R2.1.5.	Voltage and reactive	✓	✓		
PER-003-1	Operating Personnel Credentials	Effective	R2.2.	Certificates • Reliability Operator • Balancing, Interchange and Transmission Operator • Transmission Operator	✓	✓		
PER-005-1	System Personnel Training	Effective	R1.	Each Reliability Coordinator, Balancing Authority and Transmission Operator shall use a systematic approach to training to establish a training program for the BES company-specific reliability-related tasks performed by its System Operators and shall implement the program. [Time Horizon: Long-term Planning]	✓	✓		
PER-005-1	System Personnel Training	Effective	R1.1.	Each Reliability Coordinator, Balancing Authority and Transmission Operator shall create a list of BES company-specific reliability-related tasks performed by its System Operators.	✓	✓		
PER-005-1	System Personnel Training	Effective	R1.1.1.	Each Reliability Coordinator, Balancing Authority and Transmission Operator shall update its list of BES company-specific reliability-related tasks performed by its System Operators each calendar year to identify new or modified tasks for inclusion in training.	✓	✓		
PER-005-1	System Personnel Training	Effective	R1.2.	Each Reliability Coordinator, Balancing Authority and Transmission Operator shall design and develop learning objectives and training materials based on the task list created in R1.1.	✓	✓		
PER-005-1	System Personnel Training	Effective	R1.3.	Each Reliability Coordinator, Balancing Authority and Transmission Operator shall deliver the training established in R1.2.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
PER-005-1	System Personnel Training	Effective	R1.4.	Each Reliability Coordinator, Balancing Authority and Transmission Operator shall conduct an annual evaluation of the training program established in R1, to identify any needed changes to the training program and shall implement the changes identified.	✓	✓		
PER-005-1	System Personnel Training	Effective	R2.	Each Reliability Coordinator, Balancing Authority and Transmission Operator shall verify each of its System Operator's capabilities to perform each assigned task identified in R1.1 at least one time. [Time Horizon: Long-term Planning]	✓	✓		
PER-005-1	System Personnel Training	Effective	R2.1.	Within six months of a modification of the BES company-specific reliability-related tasks, each Reliability Coordinator, Balancing Authority and Transmission Operator shall verify each of its System Operator's capabilities to perform the new or modified tasks.	✓	✓		
PER-005-1	System Personnel Training	Effective	R3.	At least every 12 months each Reliability Coordinator, Balancing Authority and Transmission Operator shall provide each of its System Operators with at least 32 hours of emergency operations training applicable to its organization that reflects emergency operations topics, which includes system restoration using drills, exercises or other training required to maintain qualified personnel. [Time Horizon: Long-term Planning]	✓	✓		
PER-005-1	System Personnel Training	Effective	R3.1.	Each Reliability Coordinator, Balancing Authority and Transmission Operator that has operational authority or control over Facilities with established IROLs or has established operating guides or protection systems to mitigate IROL violations shall provide each System Operator with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that replicates the operational behavior of the BES during normal and emergency conditions.	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall use a systematic approach to develop and implement a training program for its System Operators as follows:	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R1.1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall create a list of Bulk Electric System (BES) company-specific Real-time reliability-related tasks based on a defined and documented methodology.	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R1.1.1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R1.2	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R1.3	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
PER-005-2	Operations Personnel Training	Future Effective	R1.4	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R3	Each Reliability Coordinator, Balancing Authority, Transmission Operator, and	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R3.1	Within six months of a modification or addition of a BES company-specific Real-time reliability-	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R4	Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner that (1) has operational authority or control over Facilities with established Interconnection Reliability Operating Limits (IROLs), or (2) has established protection systems or operating guides to mitigate IROL violations, shall provide its personnel identified in Requirement R1 or Requirement R2 with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that replicates the operational behavior of the BES.	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R4.1	A Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner that did not previously meet the criteria of Requirement R4, shall comply with Requirement R4 within 12 months of meeting the criteria.	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R5	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall use a systematic approach to develop and implement training for its identified Operations Support Personnel on how their job function(s) impact those BES company-specific Real-time reliability-related tasks identified by the entity pursuant to Requirement R1 part 1.1.	✓	✓		
PER-005-2	Operations Personnel Training	Future Effective	R5.1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct an evaluation each calendar year of the training established in Requirement R5 to identify and implement changes to the training.	✓	✓		
PRC-001-1.1(ii)	System Protection Coordination	Effective	R1.	Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of Protection System schemes applied in its area.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
PRC-001-1.1(ii)	System Protection Coordination	Effective	R2.	Each Generator Operator and Transmission Operator shall notify reliability entities of relay or equipment failures as follows:	✓	✓	This standard refers to the reliability entities listed in the sub-requirements: Reliability Coordinator, Balancing Authority, and TOP (all of which are the IESO). Therefore, under R2.2, Hydro One as the owner (and operator of the asset) may be directed by the IESO as the RC/BA/TOP to take corrective actions. R2 and its sub-requirements are being proposed to be retired as they have been addressed in the proposed TOP/IRO where the RC, BA and TOP can issue operating instructions (reliability directives) to Hydro One (as the owner and operator of an asset) in order to return the system to a stable state. Hence, R2 & R2.2 should be applicable to both, in that Hydro One as the TOP (operator of an asset) would need to follow the IESO directives, and the IESO as the RC and BA would be issuing to itself as a TOP, the directives of the RC and BA.	This standard refers to the reliability entities listed in the sub-requirements: Reliability Coordinator, Balancing Authority, and TOP (all of which are the IESO). Therefore, under R2.2, Hydro One as the owner (and operator of the asset) may be directed by the IESO as the RC/BA/TOP to take corrective actions. R2 and its sub-requirements are being proposed to be retired as they have been addressed in the proposed TOP/IRO where the RC, BA and TOP can issue operating instructions (reliability directives) to Hydro One (as the owner and operator of an asset) in order to return the system to a stable state. Hence, R2 & R2.2 should be applicable to both, in that Hydro One as the TOP (operator of an asset) would need to follow the IESO directives, and the IESO as the RC and BA would be issuing to itself as a
PRC-001-1.1(ii)	System Protection Coordination	Effective	R2.2.	If a protective relay or equipment failure reduces system reliability, the Transmission Operator shall notify its Reliability Coordinator and affected Transmission Operators and Balancing Authorities. The Transmission Operator shall take corrective action as soon as possible.	✓	✓		
PRC-001-1.1(ii)	System Protection Coordination	Effective	R3.	A Generator Operator or Transmission Operator shall coordinate new protective systems and changes as follows.		✓		
PRC-001-1.1(ii)	System Protection Coordination	Effective	R3.2.	Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.		✓		
PRC-001-1.1(ii)	System Protection Coordination	Effective	R4.	Each Transmission Operator shall coordinate Protection Systems on major transmission lines and interconnections with neighboring Generator Operators, Transmission Operators, and Balancing Authorities.		✓		
PRC-001-1.1(ii)	System Protection Coordination	Effective	R5.	A Generator Operator or Transmission Operator shall coordinate changes in generation, transmission, load or operating conditions that could require changes in the Protection Systems of others:	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
PRC-001-1.1(ii)	System Protection Coordination	Effective	R5.2.	Each Transmission Operator shall notify neighboring Transmission Operators in advance of changes in generation, transmission, load, or operating conditions that could require changes in the other Transmission Operators' Protection Systems.	✓	✓		
PRC-001-1.1(ii)	System Protection Coordination	Effective	R6.	Each Transmission Operator and Balancing Authority shall monitor the status of each Special Protection System in their area, and shall notify affected Transmission Operators and Balancing Authorities of each change in status.	✓	✓		
PRC-010-0	Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program	Effective	R1.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall periodically (at least every five years or as required by changes in system conditions) conduct and document an assessment of the effectiveness of the UVLS program. This assessment shall be conducted with the associated Transmission Planner(s) and Planning Authority(ies).	✓	✓		Presently, there are no UVLS programs in Ontario.
PRC-010-0	Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program	Effective	R1.1.	This assessment shall include, but is not limited to:	✓	✓		Presently, there are no UVLS programs in Ontario.
PRC-010-0	Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program	Effective	R1.1.1.	Coordination of the UVLS programs with other protection and control systems in the Region and with other Regional Reliability Organizations, as appropriate.	✓	✓		Presently, there are no UVLS programs in Ontario.
PRC-010-0	Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program	Effective	R1.1.2.	Simulations that demonstrate that the UVLS programs performance is consistent with Reliability Standards TPL-001-0, TPL-002-0, TPL-003-0 and TPL-004-0.	✓	✓		Presently, there are no UVLS programs in Ontario.
PRC-010-0	Technical Assessment of the Design and Effectiveness of Undervoltage Load Shedding Program	Effective	R1.1.3.	A review of the voltage set points and timing.	✓	✓		Presently, there are no UVLS programs in Ontario.
PRC-022-1	Under-Voltage Load Shedding Program Performance	Effective	R1.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program to mitigate the risk of voltage collapse or voltage instability in the BES shall analyze and document all UVLS operations and Misoperations. The analysis shall include:		✓		Presently, there are no UVLS programs in Ontario.
PRC-022-1	Under-Voltage Load Shedding Program Performance	Effective	R1.1.	A description of the event including initiating conditions.		✓		Presently, there are no UVLS programs in Ontario.
PRC-022-1	Under-Voltage Load Shedding Program Performance	Effective	R1.2.	A review of the UVLS set points and tripping times.		✓		Presently, there are no UVLS programs in Ontario.

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
PRC-022-1	Under-Voltage Load Shedding Program Performance	Effective	R1.3.	A simulation of the event, if deemed appropriate by the Regional Reliability Organization. For most events, analysis of sequence of events may be sufficient and dynamic simulations may not be needed.		✓		Presently, there are no UVLS programs in Ontario.
PRC-022-1	Under-Voltage Load Shedding Program Performance	Effective	R1.4.	A summary of the findings.		✓		Presently, there are no UVLS programs in Ontario.
PRC-022-1	Under-Voltage Load Shedding Program Performance	Effective	R1.5.	For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.		✓		Presently, there are no UVLS programs in Ontario.
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R1.	Each Transmission Operator shall have the responsibility and clear decision-making authority to take whatever actions are needed to ensure the reliability of its area and shall exercise specific authority to alleviate operating emergencies.	✓		H1 takes action under the direction of the IESO (MR. Ch. 5, S.3.4.1.5). H1 will take independent action for safety, equipment, and environment (focus on H1's equipment) but must notify IESO ASAP (MR. Ch.5, S.1.2.3.) Hydro One-IESO Operating Agreement	
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R2.	Each Transmission Operator shall take immediate actions to alleviate operating emergencies including curtailing transmission service or energy schedules, operating equipment (e.g., generators, phase shifters, breakers), shedding firm load, etc.	✓		H1 will take independent action for safety, equipment, and environment (focus on H1's equipment) but must notify IESO ASAP (MR. Ch.5, S.1.2.3). MR Chapter 5 section 10.4.3 The facility owner performs this as a Transmission Owner.	
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall comply with reliability directives issued by the Reliability Coordinator, and each Balancing Authority and Generator Operator shall comply with reliability directives issued by the Transmission Operator, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances the Transmission Operator, Balancing Authority, or Generator Operator shall immediately inform the Reliability Coordinator or Transmission Operator of the inability to perform the directive so that the Reliability Coordinator or Transmission Operator can implement alternate remedial actions.	✓	✓	MR. Ch. 5, S.3.4.1.5 specifics obligation of transmitter to comply with IESO directives. Similar obligations for all market participants. Ch.5, S.2.1 and operating agreement with transmitters defines scope of IESO-controlled grid	
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R5.	Each Transmission Operator shall inform its Reliability Coordinator and any other potentially affected Transmission Operators of real-time or anticipated emergency conditions, and take actions to avoid, when possible, or mitigate the emergency.	✓			
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R6.	Each Transmission Operator, Balancing Authority, and Generator Operator shall render all available emergency assistance to others as requested, provided that the requesting entity has implemented its comparable emergency procedures, unless such actions would violate safety, equipment, or regulatory or statutory requirements.	✓		Interconnection Agreements. Facilities agreement, market rules, Hydro One-IESO Operating Agreement	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R7.	Each Transmission Operator and Generator Operator shall not remove Bulk Electric System facilities from service if removing those facilities would burden neighboring systems unless:	✓			
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R7.1.	For a generator outage, the Generator Operator shall notify and coordinate with the Transmission Operator. The Transmission Operator shall notify the Reliability Coordinator and other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	✓		Generator Operator must notify and obtain approval for outage from IESO. (MR. Ch.5, S. 6.2) IESO has ability to and is obligated to notify and coordinate with neighbouring Areas (Interconnection agreements and MR. Ch.5, S. 6.5.3) Market Rule Chapter 5 section 6	
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R7.2.	For a transmission facility, the Transmission Operator shall notify and coordinate with its Reliability Coordinator. The Transmission Operator shall notify other affected Transmission Operators, and coordinate the impact of removing the Bulk Electric System facility.	✓		MP obligated to notify and seek IESO approval for transmission facility outages. IESO has ability to and is obligated to notify and coordinate with neighboring Area operators (MR. Ch.5, S. 6.5.3, NPCC C-13 and applicable Interconnection agreements)	
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R7.3.	When time does not permit such notifications and coordination, or when immediate action is required to prevent a hazard to the public, lengthy customer service interruption, or damage to facilities, the Generator Operator shall notify the Transmission Operator, and the Transmission Operator shall notify its Reliability Coordinator and adjacent Transmission Operators, at the earliest possible time.	✓			
TOP-001-1a	Reliability Responsibilities and Authorities	Effective	R8.	During a system emergency, the Balancing Authority and Transmission Operator shall immediately take action to restore the Real and Reactive Power Balance. If the Balancing Authority or Transmission Operator is unable to restore Real and Reactive Power Balance it shall request emergency assistance from the Reliability Coordinator. If corrective action or emergency assistance is not adequate to mitigate the Real and Reactive Power Balance, then the Reliability Coordinator, Balancing Authority, and Transmission Operator shall implement firm load shedding.	✓			
TOP-001-3	Transmission Operations	Future Effective	R1.	Each Transmission Operator shall act to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions. [Violation Risk Factor: High][Time Horizon: Same-Day Operations, Real-time Operations]	✓	✓	Hydro One actively maintains its area	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-001-3	Transmission Operations	Future Effective	R5.	Each Transmission Operator, Generator Operator, and Distribution Provider shall comply with each Operating Instruction issued by its Balancing Authority, unless such action cannot be physically implemented or it would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk Factor: High] [Time Horizon: Same-Day Operations, Real-Time Operations]	✓	✓	Hydro One recieves direction from the BA	
TOP-001-3	Transmission Operations	Future Effective	R6.	Each Transmission Operator, Generator Operator, and Distribution Provider shall inform its Balancing Authority of its inability to comply with an Operating Instruction issued by its Balancing Authority. [Violation Risk Factor: High] [Time Horizon: Same- Day Operations, Real-Time Operations]	✓	✓	Hydro One recieves direction from the BA	
TOP-001-3	Transmission Operations	Future Effective	R7.	Each Transmission Operator shall assist other Transmission Operators within its Reliability Coordinator Area, if requested and able, provided that the requesting Transmission Operator has implemented its comparable Emergency procedures, unless such assistance cannot be physically implemented or would violate safety, equipment, regulatory, or statutory requirements. [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	✓	✓	Hydro One assists IESO, IESO assist Hydro One	
TOP-001-3	Transmission Operations	Future Effective	R8.	Each Transmission Operator shall inform its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-Time Operations]	✓	✓	Hydro One does studies which are also verfied by IESO. So I would go either way, but keeping it a joint responsibility with Hydro One keeps consistancy with rest of TOP-001	
TOP-001-3	Transmission Operations	Future Effective	R9.	Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between the affected entities. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-Time Operations]	✓	✓	OGCC is first line knowledge of unplanned outages in Hydro One system	
TOP-001-3	Transmission Operations	Future Effective	R10.	Each Transmission Operator shall perform the following as necessary for determining System Operating Limit (SOL) exceedances within its Transmission Operator Area: [Violation Risk Factor: High] [Time Horizon: Real-Time Operations]	✓	✓	Hydro One is the only one to monitor its RASs	
TOP-001-3	Transmission Operations	Future Effective	R10.1.	Within its Transmission Operator Area, monitor Facilities and the status of Special Protection Systems, and	✓	✓	Hydro One is the only one to monitor its RASs	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-001-3	Transmission Operations	Future Effective	R10.2.	Outside its Transmission Operator Area, obtain and utilize status, voltages, and flow data for Facilities and the status of Special Protection Systems.	✓	✓		
TOP-001-3	Transmission Operations	Future Effective	R12.	Each Transmission Operator shall not operate outside any identified Interconnection Reliability Operating Limit (IROL) for a continuous duration exceeding its associated IROL Tv. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	✓		IROLs set by IESO	
TOP-001-3	Transmission Operations	Future Effective	R13.	Each Transmission Operator shall ensure that a Real-time Assessment is performed at least once every 30 minutes. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	✓	✓	Hydro One has own state estimation tool used to compare with IESO.	
TOP-001-3	Transmission Operations	Future Effective	R14.	Each Transmission Operator shall initiate its Operating Plan to mitigate a SOL exceedance identified as part of its Real-time monitoring or Real-time Assessment. [Violation Risk Factor: High] [Time Horizon: Real-time Operations]	✓	✓	we have an operating plan as per EOP-11-1	
TOP-001-3	Transmission Operations	Future Effective	R15.	Each Transmission Operator shall inform its Reliability Coordinator of actions taken to return the System to within limits when a SOL has been exceeded. [Violation Risk Factor: Medium] [Time Horizon: Real-Time Operations]	✓	✓	This is aligne with EOP-011	
TOP-001-3	Transmission Operations	Future Effective	R16.	Each Transmission Operator shall provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	✓	✓	OGCC approves NOMs outages	
TOP-001-3	Transmission Operations	Future Effective	R18.	Each Transmission Operator shall operate to the most limiting parameter in instances where there is a difference in SOLs. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	✓	✓	OGCC follows LTAs	
TOP-001-3	Transmission Operations	Future Effective	R19.	Each Transmission Operator shall have data exchange capabilities with the entities that it has identified that it needs data from in order to maintain reliability in its Transmission Operator Area. [Violation Risk Factor: High] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	✓	✓	OGCC shares info with Clarkson. Hydro One has RTUs that directly communicate with Clarkson	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-002-2.1b	Normal Operations Planning	Effective	R1.	Each Balancing Authority and Transmission Operator shall maintain a set of current plans that are designed to evaluate options and set procedures for reliable operation through a reasonable future time period. In addition, each Balancing Authority and Transmission Operator shall be responsible for using available personnel and system equipment to implement these plans to ensure that interconnected system reliability will be maintained.	✓	✓		
TOP-002-2.1b	Normal Operations Planning	Effective	R2.	Each Balancing Authority and Transmission Operator shall ensure its operating personnel participate in the system planning and design study processes, so that these studies contain the operating personnel perspective and system operating personnel are aware of the planning purpose.	✓	✓		
TOP-002-2.1b	Normal Operations Planning	Effective	R4.	Each Balancing Authority and Transmission Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal planning and operations with neighboring Balancing Authorities and Transmission Operators and with its Reliability Coordinator, so that normal Interconnection operation will proceed in an orderly and consistent manner.	✓			
TOP-002-2.1b	Normal Operations Planning	Effective	R5.	Each Balancing Authority and Transmission Operator shall plan to meet scheduled system configuration, generation dispatch, interchange scheduling and demand patterns.	✓			
TOP-002-2.1b	Normal Operations Planning	Effective	R6.	Each Balancing Authority and Transmission Operator shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional, and local reliability requirements.	✓			
TOP-002-2.1b	Normal Operations Planning	Effective	R10.	Each Balancing Authority and Transmission Operator shall plan to meet all System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs).	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-002-2.1b	Normal Operations Planning	Effective	R11.	The Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs. Neighboring Transmission Operators shall utilize identical SOLs for common facilities. The Transmission Operator shall update these Bulk Electric System studies as necessary to reflect current system conditions; and shall make the results of Bulk Electric System studies available to the Transmission Operators, Balancing Authorities (subject to confidentiality requirements), and to its Reliability Coordinator.	✓			
TOP-002-2.1b	Normal Operations Planning	Effective	R16.	Subject to standards of conduct and confidentiality agreements, Transmission Operators shall, without any intentional time delay, notify their Reliability Coordinator and Balancing Authority of changes in capabilities and characteristics including but not limited to:	✓	✓		
TOP-002-2.1b	Normal Operations Planning	Effective	R16.1.	Changes in transmission facility status.	✓	✓		
TOP-002-2.1b	Normal Operations Planning	Effective	R16.2.	Changes in transmission facility rating.	✓	✓		
TOP-002-2.1b	Normal Operations Planning	Effective	R17.	Balancing Authorities and Transmission Operators shall, without any intentional time delay, communicate the information described in the requirements R1 to R16 above to their Reliability Coordinator.	✓	✓		
TOP-002-2.1b	Normal Operations Planning	Effective	R18.	Neighboring Balancing Authorities, Transmission Operators, Generator Operators, Transmission Service Providers and Load Serving Entities shall use uniform line identifiers when referring to transmission facilities of an interconnected network.	✓	✓		
TOP-002-2.1b	Normal Operations Planning	Effective	R19.	Each Balancing Authority and Transmission Operator shall maintain accurate computer models utilized for analyzing and planning system operations.	✓	✓		
TOP-002-4	Operations Planning	Future Effective	R1.	Each Transmission Operator shall have an Operational Planning Analysis that will allow it to assess whether its planned operations for the next day within its Transmission Operator Area will exceed any of its System Operating Limits (SOLs). [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	✓	✓	shared between hydro and ieso	
TOP-002-4	Operations Planning	Future Effective	R2.	Each Transmission Operator shall have an Operating Plan(s) for next-day operations to address potential System Operating Limit (SOL) exceedances identified as a result of its Operational Planning Analysis as required in Requirement R1. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	✓	✓	OGCC has outage planning department and NMS modelling to accommodate	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-002-4	Operations Planning	Future Effective	R3.	Each Transmission Operator shall notify entities identified in the Operating Plan(s) cited in Requirement R2 as to their role in those plan(s). [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	✓	✓	Hydro Coordinates its own outages with relevant entities	
TOP-002-4	Operations Planning	Future Effective	R6.	Each Transmission Operator shall provide its Operating Plan(s) for next-day operations identified in Requirement R2 to its Reliability Coordinator. [Violation Risk Factor: Medium] [Time Horizon: Operations Planning]	✓	✓	HydroOne provide plans to IESOs RC	
TOP-003-1	Planned Outage Coordination	Effective	R1.	Generator Operators and Transmission Operators shall provide planned outage information.	✓			
TOP-003-1	Planned Outage Coordination	Effective	R1.2.	Each Transmission Operator shall provide outage information daily to affected Balancing Authorities and Transmission Operators for scheduled generator and bulk transmission outages planned for the next day (any foreseen outage of a transmission line or transformer greater than 100 kV or generator greater than 50 MW) that may collectively cause or contribute to an SOL or IROL violation or a regional operating area limitation.	✓			
TOP-003-1	Planned Outage Coordination	Effective	R1.3.	Such information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.	✓			
TOP-003-1	Planned Outage Coordination	Effective	R2.	Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of system voltage regulating equipment, such as automatic voltage regulators on generators, supplementary excitation control, synchronous condensers, shunt and series capacitors, reactors, etc., among affected Balancing Authorities and Transmission Operators as required.	✓			
TOP-003-1	Planned Outage Coordination	Effective	R3.	Each Transmission Operator, Balancing Authority, and Generator Operator shall plan and coordinate scheduled outages of telemetering and control equipment and associated communication channels between the affected areas.	✓			
TOP-003-3	Operational Reliability Data	Future Effective	R1.	Each Transmission Operator shall maintain a documented specification for the data necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The data specification shall include, but not be limited to: [Violation Risk Factor: Low] [Time Horizon: Operations Planning]	✓	✓	Hydro One owns and maintains system data	
TOP-003-3	Operational Reliability Data	Future Effective	R1.1.	A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Realtime Assessments including non-BES data and external network data as deemed necessary by the Transmission Operator.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-003-3	Operational Reliability Data	Future Effective	R1.2.	Provisions for notification of current Protection System and Special Protection System status or degradation that impacts System reliability.	✓	✓		
TOP-003-3	Operational Reliability Data	Future Effective	R1.3.	A periodicity for providing data.	✓	✓		
TOP-003-3	Operational Reliability Data	Future Effective	R1.4.	The deadline by which the respondent is to provide the indicated data.	✓	✓		
TOP-003-3	Operational Reliability Data	Future Effective	R3.	Each Transmission Operator shall distribute its data specification to entities that have data required by the Transmission Operator's Operational Planning Analyses, Realtime monitoring, and Real-time Assessment. [Violation Risk Factor: Low] [Time Horizon: Operations Planning]	✓	✓	as per R1	
TOP-003-3	Operational Reliability Data	Future Effective	R5.	Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Load-Serving Entity, Transmission Owner, and Distribution Provider receiving a data specification in Requirement R3 or R4 shall satisfy the obligations of the documented specifications using: [Violation Risk Factor: Medium] [Time Horizon: Operations Planning, Same-Day Operations, Real-time Operations]	✓	✓	as both operator and owner	
TOP-003-3	Operational Reliability Data	Future Effective	R5.1.	A mutually agreeable format	✓	✓		
TOP-003-3	Operational Reliability Data	Future Effective	R5.2.	A mutually agreeable process for resolving data conflicts	✓	✓		
TOP-003-3	Operational Reliability Data	Future Effective	R5.3.	A mutually agreeable security protocol	✓	✓		
TOP-004-2	Transmission Operations	Effective	R1.	Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).	✓		NPCC Document A-2 & A-3 and Market Rules Chapter 5 define the requirements for Transmission Operations and further defined in the Operating Limits SCOs	
TOP-004-2	Transmission Operations	Effective	R2.	Each Transmission Operator shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.	✓		NPCC Document A-2 & A-3 and Market Rules Chapter 5 define the requirements for Transmission Operations and further defined in the Operating Limits SCOs	
TOP-004-2	Transmission Operations	Effective	R3.	Each Transmission Operator shall operate to protect against instability, uncontrolled separation, or cascading outages resulting from multiple outages, as specified by its Reliability Coordinator.	✓		NPCC Document A-2 & A-3 and Market Rules Chapter 5 define the requirements for Transmission Operations and further defined in the Operating Limits SCOs	
TOP-004-2	Transmission Operations	Effective	R4.	If a Transmission Operator enters an unknown operating state (i.e. any state for which valid operating limits have not been determined), it will be considered to be in an emergency and shall restore operations to respect proven reliable power system limits within 30 minutes.	✓		NPCC Region Reliability Plan, Section 4.6.1 & MM 7.4	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-004-2	Transmission Operations	Effective	R5.	Each Transmission Operator shall make every effort to remain connected to the Interconnection. If the Transmission Operator determines that by remaining interconnected, it is in imminent danger of violating an IROL or SOL, the Transmission Operator may take such actions, as it deems necessary, to protect its area.	✓		IESO's operating agreements and interconnection agreements	
TOP-004-2	Transmission Operations	Effective	R6.	Transmission Operators, individually and jointly with other Transmission Operators, shall develop, maintain, and implement formal policies and procedures to provide for transmission reliability. These policies and procedures shall address the execution and coordination of activities that impact inter- and intra-Regional reliability, including:	✓			
TOP-004-2	Transmission Operations	Effective	R6.1.	Monitoring and controlling voltage levels and real and reactive power flows.	✓			
TOP-004-2	Transmission Operations	Effective	R6.2.	Switching transmission elements.	✓			
TOP-004-2	Transmission Operations	Effective	R6.3.	Planned outages of transmission elements.	✓			
TOP-004-2	Transmission Operations	Effective	R6.4.	Responding to IROL and SOL violations.	✓		NPCC Document C-20' Section 4.2, MM7.43 and various SCOs	
TOP-005-2a	Operational Reliability Information	Effective	R2.	Upon request, each Balancing Authority and Transmission Operator shall provide to other Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability, the operating data that are necessary to allow these Balancing Authorities and Transmission Operators to perform operational reliability assessments and to coordinate reliable operations. Balancing Authorities and Transmission Operators shall provide the types of data as listed in Attachment 1-TOP-005 "Electric System Reliability Data," unless otherwise agreed to by the Balancing Authorities and Transmission Operators with immediate responsibility for operational reliability.	✓			
TOP-006-2	Monitoring System Conditions	Effective	R1.	Each Transmission Operator and Balancing Authority shall know the status of all generation and transmission resources available for use.	✓		MR. Ch.5, S. 3.2.1 places obligation on the IESO to monitor and direct the operation of the ICG facilities.	
TOP-006-2	Monitoring System Conditions	Effective	R1.2.	Each Transmission Operator and Balancing Authority shall inform the Reliability Coordinator and other affected Balancing Authorities and Transmission Operators of all generation and transmission resources available for use.	✓		Hydro One-IESO Operating Agreement	
TOP-006-2	Monitoring System Conditions	Effective	R2.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor applicable transmission line status, real and reactive power flows, voltage, load-tap-changer settings, and status of rotating and static reactive resources.	✓	✓		

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-006-2	Monitoring System Conditions	Effective	R3.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall provide appropriate technical information concerning protective relays to their operating personnel.	✓	✓	Protection Standards MM 2.10 CAA Procedure	
TOP-006-2	Monitoring System Conditions	Effective	R4.	Each Transmission Operator, and Balancing Authority shall have information, including weather forecasts and past load patterns, available to predict the system's near-term load pattern.	✓		Weather Data Services MM 2.8, 2.11 and 7.2 describe the various load forecast outlooks from next day to 10 years out (IESO no longer produces the annual 10-year outlook)	
TOP-006-2	Monitoring System Conditions	Effective	R5.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall use monitoring equipment to bring to the attention of operating personnel important deviations in operating conditions and to indicate, if appropriate, the need for corrective action.	✓	✓		
TOP-006-2	Monitoring System Conditions	Effective	R6.	Each Balancing Authority and Transmission Operator shall use sufficient metering of suitable range, accuracy and sampling rate (if applicable) to ensure accurate and timely monitoring of operating conditions under both normal and emergency situations.	✓	✓	CEA/SCC metering standards Participant Technical Reference Manual S. 4- Operational Metering Equipment	
TOP-006-2	Monitoring System Conditions	Effective	R7.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall monitor system frequency.	✓	✓	MR. Ch 4, App 4.15 and 4.16 specifies the obligation of MP to install as directed by the IESO.	
TOP-007-0	Reporting System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) Violations	Effective	R1.	A Transmission Operator shall inform its Reliability Coordinator when an IROL or SOL has been exceeded and the actions being taken to return the system to within limits.	✓		MR. Ch.5, S 5 specifies IESO's mandate to establish and manage security limits of the ICG	
TOP-007-0	Reporting System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) Violations	Effective	R2.	Following a Contingency or other event that results in an IROL violation, the Transmission Operator shall return its transmission system to within IROL as soon as possible, but not longer than 30 minutes.	✓		Hydro One-IESO Operating Agreement	
TOP-007-0	Reporting System Operating Limit (SOL) and Interconnection Reliability Operating Limit (IROL) Violations	Effective	R3.	A Transmission Operator shall take all appropriate actions up to and including shedding firm load, or directing the shedding of firm load, in order to comply with Requirement R 2.	✓		Hydro One-IESO Operating Agreement	
TOP-008-1	Response to Transmission Limit Violations	Effective	R1.	The Transmission Operator experiencing or contributing to an IROL or SOL violation shall take immediate steps to relieve the condition, which may include shedding firm load.	✓		Hydro One NMI 0123 - "Accountabilities for Controlled Rotational and Emergency Load Shedding" outlines procedures SCO - Controlled Rotational and Emergency Load Shedding	
TOP-008-1	Response to Transmission Limit Violations	Effective	R2.	Each Transmission Operator shall operate to prevent the likelihood that a disturbance, action, or inaction will result in an IROL or SOL violation in its area or another area of the Interconnection. In instances where there is a difference in derived operating limits, the Transmission Operator shall always operate the Bulk Electric System to the most limiting parameter.	✓		Hydro One-IESO Operating Agreement The various SCO's and the interconnection agreements establish the operating parameters of the ICG and each of the interconnections.	

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
TOP-008-1	Response to Transmission Limit Violations	Effective	R3.	The Transmission Operator shall disconnect the affected facility if the overload on a transmission facility or abnormal voltage or reactive condition persists and equipment is endangered. In doing so, the Transmission Operator shall notify its Reliability Coordinator and all neighboring Transmission Operators impacted by the disconnection prior to switching, if time permits, otherwise, immediately thereafter.	✓	✓		
TOP-008-1	Response to Transmission Limit Violations	Effective	R4.	The Transmission Operator shall have sufficient information and analysis tools to determine the cause(s) of SOL violations. This analysis shall be conducted in all operating timeframes. The Transmission Operator shall use the results of these analyses to immediately mitigate the SOL violation.	✓		IESO's EMS, OSL and Power Flow tools	
VAR-001-4	Voltage and Reactive Control	Effective	R1	Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.	✓			
VAR-001-4	Voltage and Reactive Control	Effective	R1.1	Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.	✓			
VAR-001-4	Voltage and Reactive Control	Effective	R2	Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various	✓			
VAR-001-4	Voltage and Reactive Control	Effective	R3	Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary.	✓	✓		
VAR-001-4	Voltage and Reactive Control	Effective	R4	The Transmission Operator shall specify the criteria that will exempt generators from: 1) following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications.	✓			
VAR-001-4	Voltage and Reactive Control	Effective	R4.1	If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.	✓			
VAR-001-4	Voltage and Reactive Control	Effective	R5	Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the generator step-up transformer at the Transmission Operator's discretion.	✓			

					Responsibility			
Standard Number	**Standard Name**	**Requirement**	**Requirement No.**	**Text of Requirement**	**IESO**	**Transmitter**	**Comments/Details**	**IESO Comments**
VAR-001-4	Voltage and Reactive Control	Effective	R5.1	The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).	✓			
VAR-001-4	Voltage and Reactive Control	Effective	R5.2	The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).	✓			
VAR-001-4	Voltage and Reactive Control	Effective	R5.3	The Transmission Operator shall provide the criteria used to develop voltage schedules Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator within 30 days of receiving a request.	✓			
VAR-001-4	Voltage and Reactive Control	Effective	R6	After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.	✓			

Job Step/Work Operation:

STRINGING CONDUCTOR AND / OR SHIELDWIRE

HO 4191 **Stringing System Strength Requirements**
PR 0164 **Line Stringing Over 50 kV – Safety Basics**

Before starting work, visual barriers must be installed to identify clearly the *safe work area(s)* for the worker, and/or to identify hazardous area(s) for people not involved in the work (HOSR 224)

Activity/Hazards	Barriers
❑ **Setting up stringing compounds** • slips and trips • underground • unplanned Outages	❑ Call Ontario One Call for locates of all underground utilities ❑ Refer to drawings (if applicable) ❑ Prior to working within 30 metres or crossing high pressure pipe lines notify the proper authorities. ❑ Proper bonding mats ❑ HO 1987 Tension Stringing of Shield wire ❑ Work Protection Manual ❑ **SP 0089** Grounding Transport and Work Equipment in Stations ❑ **HO 1950** Installing Helper Cables and Tie-Downs on Conductors ❑ **HO 2678** Grounding Procedure for Handling Conductor on the Ground
❑ **Install anchors** • under ground utilities • overhead Electrical contacts • unplanned Outages	❑ **HO 0501** Installing Log Anchors and Peg Anchors ❑ **HO 0483** Rock Anchors ❑ Dedicated Observer required ❑ Maintain safe limits of approach **EUSR 129** ❑ **See** Installing Anchors, Screw, Slug & Rock supplement
❑ **Setting up equipment** • personal Injuries • crushing hazards • overhead Electrical contacts	❑ Signal person required, signaller shall wear high Vis clothing **OHSA Reg 213/91 Section 106 (1.2&.3&.4)** ❑ Qualified Operator ❑ Maintain safe limits of approach **EUSR 129** ❑ Keep hands and feet clear of all moving parts
❑ **Loading Equipment & material** • transporting material • personal Injuries • prushing hazards • overhead Electrical contacts	❑ Craning and Rigging Handbook ❑ Make sure reels are tightened in and all safe guards are used ❑ Load security handbook ❑ Signal person required, signaller shall wear high Vis clothingt **OHSA Reg 213/91 Section 106 (1.2&.3&.4)** ❑ Maintain safe limits of approach **EUSR 129** ❑ **HO4087** Securing Loads
❑ **Stringing Conductor / Shieldwire** • overhead electrical contacts • personal Injuries • crushing hazards	❑ **HO 4053** Mesh Grip Installation on Conductor and Synthetic Rope ❑ **HO 0696** Installing Compression Connectors and Jumper terminals ❑ Conductors or stringing ropes are free of obstructions. ❑ Personnel are aware of pulling angles and are to stay out of

	the **BITE** of any cables or ropes ❑ Rider Poles and Observers at all road & rail crossings ❑ **PR 0164** Line Stringing Over 50 kV – Safety Basics
❑ **Sagging / Working aloft** • falling while working aloft	❑ **HO 2036** Taking Sags with a Transit or Theodolite (A) in the same Span or (B) from an Adjacent Span ❑ **HO 0308** Checking Conductor Sag on Towers and Wood Poles using a telescope ❑ Approved PPE and Fall Protection (worn properly) ❑ Fall protection required, equipment options available i.e. French Hook, Retracta Lock, White rope etc. Options reviewed and discussed.
❑ **Clamp in & Un-clamp Conductor** • falling • falling tools & material • electrical Contact • altering strain on structure • equipment / rigging failure	❑ **HO 3010** Pulley Block Handline assemblies ❑ Raising and Lowering of Tools and Material ❑ **HO 2689** Jib Attachment and Adapters ❑ **HO 4016** Temporary Support of Wood Poles ❑ **SP 0089** Temporary Grounding and Bonding ❑ Fall protection required, equipment options available i.e. French Hook, Retracta Lock, White rope etc. Options reviewed and discussed. ❑ Maintain safe limits of approach **EUSR 129** ❑ Temporary Fall Protection ❑ **HO 4102** Ampact Tool Maintenance ❑ **HO 4038** Aerial Bucket Device ❑ **HO 4173** All Terrain Vehicle Operation ❑ **HO 0809** The Use of Manbaskets on Cranes While Lifting Loads ❑ **HOSR 403** Overhead Protection ❑ Identify safe work zone i.e.: tape/fencing /flags/signs barricades ❑ **HOSR 325** ❑ Daily Inspection of rigging. Refer to Craning and Rigging Hand Book ❑ Rigging & Equipment Tested & up to date
❑ **Additional Hazards**	❑

Version #	Date	Brief Description of Revisions
Rev 01	Jan 2012	Added Ontario One Call and referenced the requirement to notify the proper authorities when working with in 30 metres or crossing high pressure pipe lines

Document Number: **PR 0164 R0**

Document Name: **Line Stringing Over 50 kV - Safety Basics**

Issue Date: **July 2002**

Any variance from this practice must be documented in the Job Plan.

Purpose

This document deals with transmission line stringing operations (single or multi conductors) over 50 kV.

The scope of this document includes:

- a typical stringing operation.
- specific responsibilities of key individuals involved in line stringing operation.
- identification of common critical hazards associated with transmission lines stringing operations.

Revision

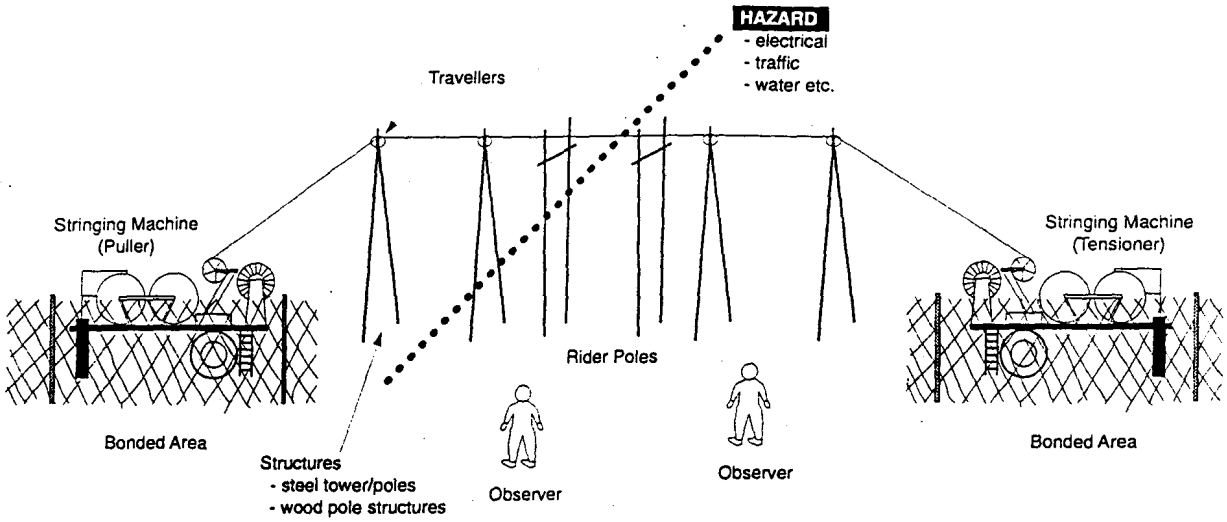
This is a new document.

Contents

1.0 Overview of the Line Stringing Operation

The following block diagram illustrates the various components of a typical line stringing operation. Not all of the components illustrated are present in all stringing operations. The number, size, type and shape of the stringing components, operating conditions, etc., depends on the type of operation and the combination of hazards that are present.

Figure 1: Typical Stringing Operation



1.1 Stringing Methods

There are basically two methods of stringing, slack and tension, and variations of the two methods i.e. bonded tension stringing and unbonded tension stringing. The type of method used depends on factors such as the hazards present, the equipment used, need for conductor cleanliness etc.

1.1.1 Tension Stringing

Tension stringing is a method for stringing conductors where there is continuous control of conductor sag to keep the conductor clear of the ground, obstacles, and energized circuits. A puller with fine and/or automatic controls is positioned at one end and is used to prevent over-pull and while a tensioner at the other end of the pull is used to continuously restrain and control the sag on the conductor.

The tension method of stringing is used where it is necessary to keep the conductor off the ground to minimize surface damage or in areas where frequent crossings are encountered.

Tension stringing is mandatory:

- when slack stringing procedures would endanger the public;

- when conditions call for a bonded stringing system (exceptions are by approval only);
- when other conditions exist which call for precise control of conductor sag; or
- on corridors where induction may be of concern.

1.1.2 Conventional / Slack Stringing

Slack stringing is a method of stringing conductor slack without the use of a tensioner. The conductor is pulled off the reel by a pulling vehicle and dragged along the ground, or the reel is carried along the line on a vehicle and the conductor deposited on the ground. As the conductor is dragged to, or past, each supporting structure, the conductor is placed in the travellers, normally with the aid of finger fines.

Using this method the hazard of uncontrolled loss of tension of the conductor must be adequately considered.

1.2 Bonded vs. Unbonded Stringing

1.2.1 Bonded Tension Stringing

Bonded tension stringing is used in areas where the hazard of electrically energizing the pull due to contact with or induction from energized circuits exists. It is a method that provides a low resistance, high current carrying capacity path around the workers in each stage of the job.

A bonded system is mandatory:

- on most HV and EHV stringing operations;
- when conductors must be strung on one portion of multi-circuit structures with a live circuit on the other portion of the structure;
- when stringing adjacent to, parallel to or crossing live lines;
- When other conditions exist which call for special precautions.

1.2.2 Unbonded Tension Stringing

Unbonded tension stringing is a stringing method that uses temporary grounds to drain off naturally occurring and induced charges and guard against high current hazards by physical barriers or by distance from sources of high currents.

1.3 Induction Hazards

When tension stringing in inductive corridors, electrostatic and electromagnetic charges will be present. The level of induction will depend upon geometry of existing lines and the electrical conditions of line circuits.

To measure the level of induction a computer program is available from Work Methods, called "Tesla". This program will calculate the max. level of induction that may be encountered. To obtain voltage and current levels, circuit configuration, dimension etc. must be established. The calculated values can be analyzed and referenced against previous encounters of high level induction. Therefore, the effective method used previously to handle similar situations could be used again with some modification, if required.

There are special tools and aids which have been developed and tested to effectively handle high induction levels. Listed below are some of these tools and aids:

- induction drainers;
- traveller insulators;
- tie-down insulators bonding devices;
- insulative links- this may be required depending during various activities;
- In-line ground circuit interrupter.

Refer to PR 0078: Definitions and Acronyms for definitions required to understand the most appropriate Grounding and Bonding arrangement for the job at hand.

1.3.1 Removing Grounds

When working in line sections with a known history of excessive arc lengths when removing grounds (i.e. multi-circuit corridors) additional precautions are required. In these situations, the following steps should be taken prior to removing grounds:

- Measure current in temporary ground using an ammeter.
- Calculate voltage (using TESLA program, contact Work Methods & Training dept.) or measure voltage using an approved tool.
- Determine the estimated arc gap.

For personnel safety reasons, temporary grounds should only be used in lines applications to break inductive or capacitive currents if the calculated are gap is 300 mm (12") or less. For gaps calculated to be greater than 300 mm (12"), use alternate methods such as sequential ground removal, portable ground interrupter etc.

Refer to SP 0100: Transmission Lines Grounding and Bonding-Removal of Grounds.

1.3.2 Induction and Synthetic Ropes

When fly ropes and uniline are pulled during stringing they are subject to electrostatic charges. This voltage can be high and can result in an electrostatic current flow in the rope where a path to ground is found. This current can cause a "pecking" over time and will seriously affect the physical and dielectric strength of the rope or can cause localized

burning. Insulators are used between tower steel and stringing travellers to reduce the chance of current flow through the traveller to the tower.

In bonded tie down areas, ropes can be insulated from the grips using polymeric insulators. This practice is used for severe induction corridors and should be decided early in the planning stage of stringing.

A concentrated area for current flow can develop where the synthetic pulling rope connects to the conductor or other conductive line. Because the conductor is conductive and a path to ground exists at the compound area, an insulated link must be used between the two lines to limit the possibility of burning.

As the conductor or other conductive line is pulled into the compound by the synthetic pulling rope (with the single ground located at the puller end) an electromagnetic Ferranti voltage develops and increases with the length of parallel circuit. This voltage can reach into hundreds of volts at the point where the bull line enters the tensioner compound. When the second ground is attached to the conductor or bull line at this location, the Ferranti voltage drives a circulating current and voltage on the bull line essentially disappears. The circulating current that is established due to two or more grounds being on the conductive bull line or conductor, remains present throughout the stringing activity.

1.3.3 Gradient Mats

The bonded mat allows work to proceed when lethal Ferranti voltage and circulating current are present because these hazards are then adequately controlled. The bonded mat and other associated bonding, permits workers to handle conductor because a low resistance path permits the flow of current to ground, bypassing the worker. Bonded mats also protect workers from potential voltage and current rise by creating an equal potential area.

At no time during tension stringing or other activities should grounds be removed by hand. Grip all sticks must be used even while in the bonded area. Lethal circulating and fault current could be present.

2.0 Key Responsibilities

2.1 Supervisor of Stringing Operation (SSO)

The Supervisor of the Stringing Operation is in charge of the overall stringing operation and his/her responsibilities include:

- preparing a detailed Job Plan and reviewing the plan with each member of the crew;
- ensuring an adequate communications system is in place to maintain a safe operation;

- developing an emergency shut down procedure and periodically practicing this procedure with the crew;
- ensuring all rigging is inspected regularly and to ensure it is free from defects;
- ensuring all equipment used in the stringing operation is of adequate strength and in safe working order;
- controlling personnel entering and exiting the stringing compounds;
- ensuring the proper grounding and bonding procedures are used on and around the Stringing Compound. (Boom Truck, Fuel Truck, Lube Truck, Personnel)
- ensuring stringing equipment is adequately anchored;
- conducting regular Tailboard Meetings with the crew;
- assigning specific responsibilities to each member of the crew;
- authorizing start up and shut down of the stringing operation;
- ensuring operators are trained/qualified to operate the equipment assigned; and
- excluding unauthorized personnel from the work zone.

2.2 Puller Operator (P.O.)/ Tensioner Operator (T.O.)

The Puller / Tensioner Operator is in charge of his/her assigned equipment and is responsible for the safe operation of the equipment. Specific responsibilities include:

- controlling personnel movement around his/her assigned stringing machine at all times, i.e. no one enters the compound, or works on the equipment without permission from the operator. Note: the operator is not responsible for the work methods of anyone working on or around the stringing equipment,
- using the communications system as per the plan;
- ensuring the emergency shut down procedure is in place before pulling and for shutting down the operation as per the procedure in the event of an emergency;
- operating the equipment in accordance with the manufacturers instructions;
- inspecting his/her assigned equipment before use each day that it is operated and taking the necessary actions when deficiencies are found;
- ensuring defective equipment is not operated;
- ensuring good housekeeping is maintained (cab, windows, mirrors, etc.) in the immediate vicinity of their equipment i.e. stringing compound;
- ensuring the stringing equipment is securely anchored before operating;

- ensuring grips are applied to the conductor in the event the operation is put on hold for any unknown period of time i.e. while work is being performed on the conductor or when work is going to be performed on the stringing machine. Note: once the grip is applied it is very important to let the conductor off into the grip;
- ensuring the bonded areas barriers are not violated e.g. passing material over the fence barriers is not allowed;
- ensuring their assigned stringing equipment is fueled safely. Refer to SP 0090: Temporary Grounding and Bonding Systems: Grounding and Bonding for Fuelling Operations.

2.3 Mechanic

The Mechanic is responsible for the maintenance to the equipment as required. Specific responsibilities include:

- obtaining permission from the operator before making any adjustments to the equipment;
- ensuring his / her work methods are safe;
- using Work Protection tags to lock out equipment, where the operation of the equipment is not under the immediate control of the mechanic.

2.4 Observer

The Observer is responsible for observing the portion of the stringing operation he/she is assigned. Specific responsibilities include:

- advising the Puller/Tensioner Operators and / or the supervisor of the stringing operation of conditions that may be hazardous to the workers, the operation and /or the public as they occur;
- remaining clear of all moving parts and, where possible, remaining in full view of the Operator during the stringing operations;
- knowing the emergency plan at their work location.

2.5 Additional Workers

At the discretion of the Stringing Operation Supervisor, Additional workers may be assigned various tasks in addition to the skills identified above i.e. assisting with fueling operation, grounding conductor, following the running board. Additional responsibilities assigned should be clearly defined by the Supervisor and communicated in the Tailboard Meeting before the operation begins.

3.0 Job Planning

Plan the operation using the job Planning folder. Include any necessary documentation i.e. Work Protection Permits, applicable stringing procedures etc.

When preplanning the job, conduct a site visit considering the following items:

- Vicinity of live circuits.
- Induction hazards.
- Road/rail crossings and notification.
- Public safety and notification
- Need for barriers i.e. rider poles, observers etc.
- Condition/terrain.
- Length of the pull.
- Length of spans, knolls, corners and hills.
- Condition of existing pole, hardware and conductor.
- Height of existing line.
- The number location of deadends, corners and their angles.
- Existing guying and anchors.
- Equipment accessibility.
- Open points (temporary and permanent).
- Size of conductor and length of reels to be used.
- Type of travellers to be used.
- Type of pulling rope / condition of existing conductor when part of the pull.
- Specific training requirements / qualifications of crew members.
- Number of observation points / number of observers required.
- Type of communication equipment required.
- Details of the emergency shut down plan.

Refer to TD1000: Job Planning and SP 0140: Job Planning - Construction Services.

3.1 Notifying Outside Authorities

The Superintendent/GF or delegate must insure contact has been made to outside authorities fully explaining the details of the stringing operation and the impact those activities may have to personal, property and equipment.

Table 1: Outside Authorities

Authority	*Actions*
Hydro One Lines	Inform Provincial Lines Zones of construction activities.
Public Utilities	Notify the appropriate lines customers and foreign organization official sufficiently in advance for making necessary arrangements. for making necessary
Provincial Highways	Obtain approval of the District Engineer before working adjacent to roadways
County and Township	Inform the appropriate Engineer of roads construction activities.
Railways	Inform the designated officials at least 4 weeks prior stringing.
Public & Public Officials	Personal contacts, mail notices, answer inquiries.
Police	Call the Ontario Provincial Police or the local police to control traffic at busy road crossings.
Underground Utilities (Electric, Water, Gas, Bell)	Consult the local authorities before excavating poles avoid damaging buried services.
Private property	Obtain owner approval before any work begins.

3.2 Public Protection

When conductors are to be strung through built-up areas and particularly in the vicinity of schools, playground and garden plots, it is imperative that the safest possible methods be selected in order to protect the public and property. Depending on local conditions, the following precautions should be kept in mind:

- use rider pole structures or equivalent to safe guard pathways, roads and live lines.
- place observers at road and walkway crossings.

If there is a school, golf course, playground, i.e. soccer field nearby, provide extra observers in the area, particularly in the school area. It may be necessary to work during school hours so be prepared to suspend operation immediately before and after school hours. Also, request the school principal to warn the children to keep clear of the work area.

Even when conductors are to be tension strung and kept clear of the ground, sometimes the initial pulling line needs to be slack strung. During this operation, if the workers are having difficulty controlling the actions of bystanders, local police should be called in to clear the right of way.

Once the pulling line is in position, an absolute minimum clearance of 5 metres (16.4 feet) from the ground should be maintained while pulling line or conductor. If difficulty is being experienced in holding a steady tension while stringing, minimum clearance should be increased.

Refer to HO 4079: Warning Barriers.

3.3 Radio Communications

When the stringing operation is in progress, the radio channel that is being used is an exclusive channel. Only the personnel directly associated with the pull may use this channel (puller / tensioner operators, stringing operation supervisor, lineman following running board and observers). Anyone else who keys into this channel will have to be authorized to do so, unless they have a reason for stopping the pull. **All communications should be clear, short and to the point.**

Because of the variety of stringing machines available, selection of the right type of communication systems is very important, i.e.: hand held sets vs. head sets to enable the operators to have both hands free at all times.

3.4 Emergency Plans

The emergency plan should provide clear instructions on how to shut down the stringing operation in the event of an emergency and provide the necessary aid to rescue workers and / or attend to injuries e.g. first aid, phone numbers of local ambulance etc.

When a pull has to be stopped, it is crucial that the puller end and the tension end are in communication. First the puller end should stop while the tension end keeps the sag maintained (depending upon the types of equipment being used).

3.5 Rescuing Workers

Project-specific procedures for emergency response must be established before work can begin. The rescue plan should also provide first aid and where practical, communications with the local ambulance service.

3.6 Selection of Stringing Equipment

The main consideration when choosing tension stringing equipment is the expected line tensions that will be used to properly control the conductor. The line must be surveyed and sag selected which represents the maximum sag that is acceptable during stringing. This sag should ensure that the shieldwire is maintained at an acceptable clearance from all underbuilds, conductors, riders etc. This sag can then be used to calculate the pulling line tension.

To calculate line tension and size of pulling rope, you must first determine the following:

- Single or multi conductor pull
- W - weight (size) of conductor (lb./ft.)
- L - Average Span (ft.)
- N - Number of travellers (structures)

- S - Mid-span sag (ft.) during stringing.

$$T = \frac{W \times L^2}{8 \times S}$$

T = Line Tension
W = Weight of Conductor in lbs./ft.
L = Length of Span in ft.
S = Sag in ft.

When the conductor or shieldwire is pulled over the travellers it takes energy to bend and unbend the wire and turn the traveller. This energy results in a higher stringing tension than calculated above. A reasonable estimate is 0.5% of the line tension for each traveller. A pull of 8 km would result in 20% to 25% more tension at the puller end than the tensioner end. To allow for unforeseen requirements an additional 25% should be included. Therefore for an 8 km pull the puller should be rated approximately 50% greater than the line tension calculated.

To calculate the pull required at puller, use this formula:

$$P = \frac{T}{(.98)N}$$

T = Tension required at tensioner (above)
N - Number of travellers
(.98) = efficiency of each traveller (98%)

This formula assumes the efficiency of each traveller is 98 per cent. This takes into account the energy used to deflect the conductor over the block and around corners.

3.7 Selection of Travellers

The traveller must be capable of handling the vertical and horizontal loads which will be imposed on it. If the traveller is used on a tangent structure with level spans on either side then it will experience a vertical load equal to the weight of conductor from mid span to mid span. If there is an elevation difference between structures then the higher traveller will carry a larger proportion of the load. These loads can easily be calculated.

The travellers used on the last structures before the puller or tensioner usually experience the greatest working loads due to the large conductor departure angle from the structure down to the machines. The working load on travellers is also higher on angle structures. The crew should be prepared to use larger travellers at these locations. This loading and expected angle can be calculated.

The use of a traveller with the proper sheave diameter will ease the stringing operation and prevent damage to the conductor/shieldwire because of a high bearing pressure. If too small a traveller is used the wire will not move through it easily to balance spans during

sagging. Small travellers cause a high bearing pressure between the wire and sheave which could cause damage to the wire.

When stringing shieldwire, travellers with hardened steel sheaves are to be used when stringing steel wire and urethane lined or aluminum sheave travelers should be used when stringing alumoweld and ACSR shieldwire. Refer to HO 1987: Tension Stringing of Shieldwire.

4.0 Stringing Compound Set-Up

This section discusses criteria for selection of suitable stringing equipment sites. Past experience has shown that pulls up to 20 kilometres without any abnormal conditions are usually easy to manage. A pull can be longer or shorter depending on the conditions.

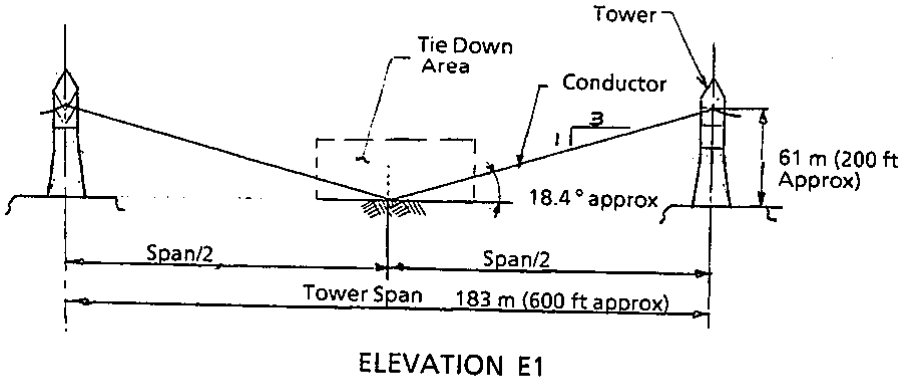
One of the consequences of a longer pull is that the front to back ratio of stringing tension greatly increases when the length of pull increases. The increase is mainly due to friction in the travellers and the energy it takes to bend and unbend the wire as it rolls over the travellers.

4.1 Site Preparation

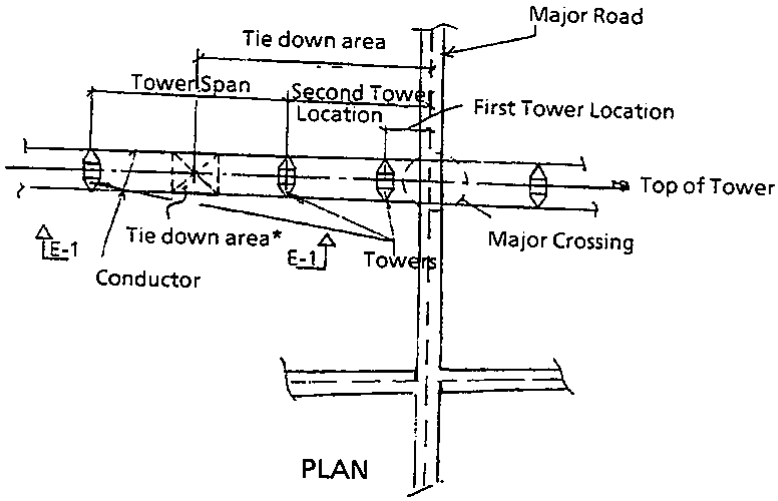
The area may be any size and shape to contain machine and men. Typically puller / tensioners are located 3:1 ratio (distance : height) from the nearest tower. There should be space in front and back of the tensioner for tying down conductor, jointing, and room for changing reels if necessary.

Figure 2: Tie Down Area Position

Figure 6-1a- Schematic of Preferred set up location



ELEVATION E1



PLAN

* All efforts must be made to locate "tiedown area" at least two towers in from major crossing

Check the area to ensure that the ground gradient mats will not be lying on old fence wire, counterpoise wire, buried cables, etc., which could form an electrical connection between the ground gradient mat system and any adjacent fences or wires.

4.2 Anchors

Anchor the machines as required. In some cases, if the tensions are heavy, the machines must be anchored in three positions (to prevent them from overturning) as indicated on the chart attached to the tensioners. If the machines are positioned on solid dry ground and all the jacks are down, additional wheel chocks could eliminate the necessity to install anchors.

All anchors or guys installed inside the ground gradient mat enclosure, must be connected electrically to the mat.

If the anchor is outside the gradient matted area, an insulator of adequate mechanical and electrical strength must be installed. Place the insulator between the machine and the anchor sling where it passes over the edge of the ground gradient control mat.

Refer to HO 0267: Determining Soil Conditions Using a Chance Probe and Installing Screw Anchors and HO 1950: Installing Helper Cables and Tie-Downs on Conductors.

Refer to HO 4084: Working in the Vicinity of Underground Services and SP 0106: Excavation in the Vicinity of Gas Lines.

4.3 Setting Up Ground Gradient Mats

Bonded areas vary in size and shape depending on the type and the conditions of the operation. Their function is to provide an equi-potential surface to prevent the hazard of a potential difference across the worker i.e. step and touch potential . It is important to ensure the area is well bonded and once set up that the electrical barriers are not violated. Where practical it is preferred that the machine is sitting directly on the gradient mat. This provides the maximum protection for workers in the event that the machines need service or repair.

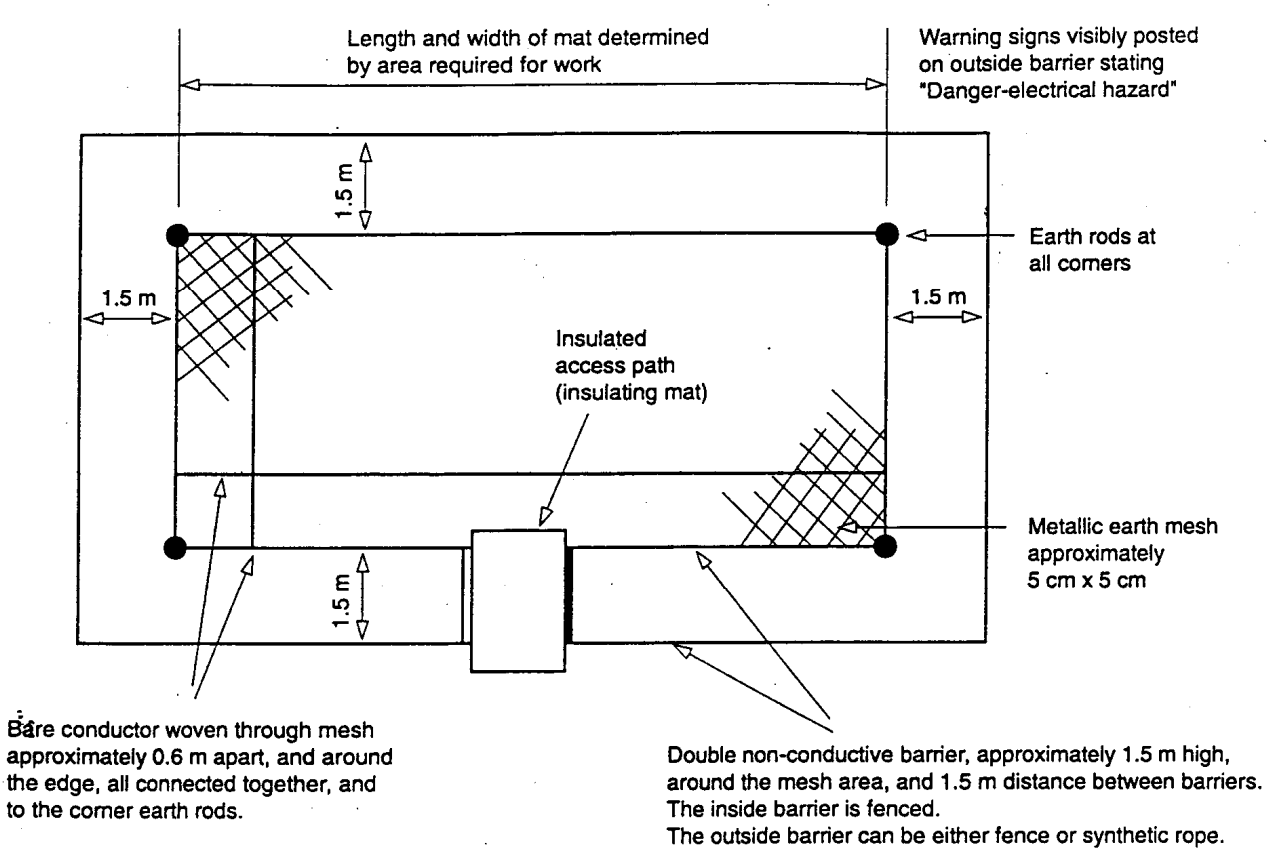
After the machine locations are chosen, the work should proceed as follows:

- Lay sufficient ground gradient mat and connect pieces together with the proper electrical connectors. Each connection should be clean and tight. If more than one machine (tensioner) is required, the mat system should be installed between each machine so that the entire system becomes one. There should be no gaps between the mats at a machine location. Workers must be able to move about and stay on the ground gradient control mat while stringing is in progress.
- Connect the ground mat to the system neutral with adequate size conductor and suitable connectors. If a system neutral is not available, ground rods or earth anchors can be driven at each end and connected to the ground gradient mat.
- In some locations, it will be impossible to drive ground rods, therefore, it may be necessary to run a conductor to a remote ground and tie the mat system to it.

Note: If it is impractical to run a conductor to a remote ground a new site should be selected where grounding can be accomplished.

- Megger the ground gradient mat system. The reading should be 25 ohms or less.

Figure 3: Grounded Compound for Stringing Operation



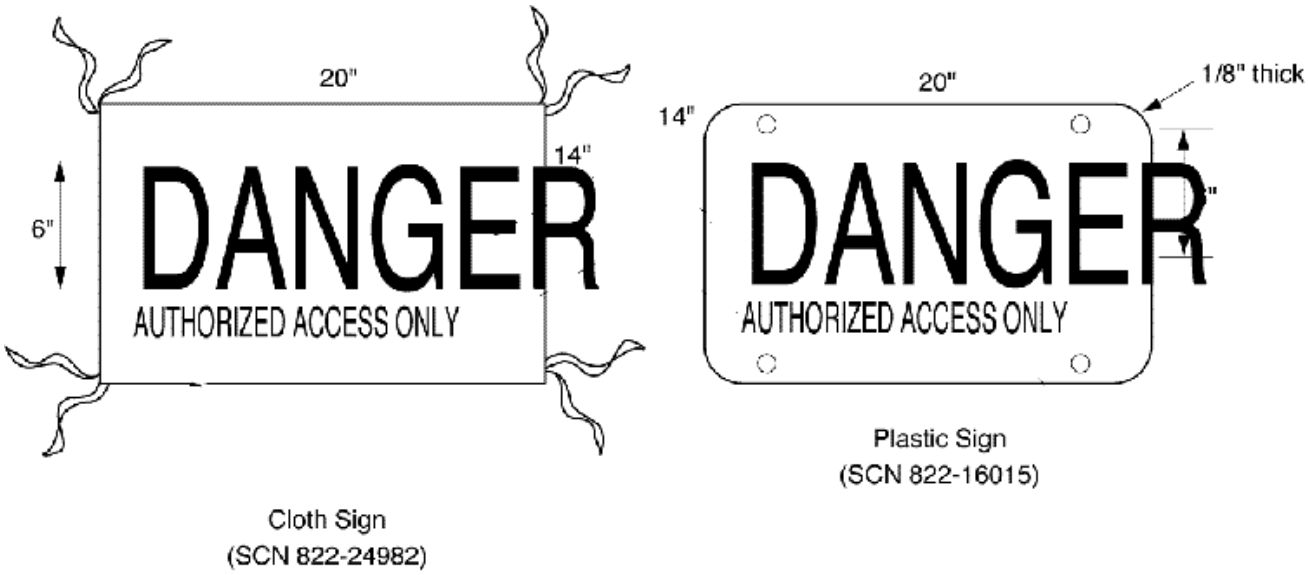
4.4 Compound Barriers

A plastic barrier fence (non-conductive) must be erected around the perimeter of the ground gradient control mat area to separate workers inside the compound from workers outside the compound. A small opening of 1 m (3 feet) is left for a passage way for workers. An additional barrier is strung around the enclosure 1.5 m (five feet) away from the first barrier. On this fence "Danger Live Apparatus" signs are hung to warn workers and public. This barrier may be another suitable non-conductive barrier such as polypropylene rope netting or synthetic rope.

Refer to HO 4079: Warning Barriers.

Note: The fence barrier is to protect against electrical hazards and should not be violated for example by passing tools or material over the barrier. The designated entrance must be used.

Figure 4: Danger Signs



5.0 Fuelling Operation

When fueling stringing equipment that is not on a ground gradient mat a bond must be made between the fuel truck and the stringing machine. The fuel truck may not be used when the stringing equipment is in place on the ground gradient mat.

For fuelling Stringing Equipment located in a bonded compound, ensure the equipment is refueled prior to bringing the conductor into the compound. After the conductor has been bonded to the compound, use a) an insulated link to lower 45 gallon drum into the compound and transfer or b) 5 gallon cans walked into the compound. Refer to SP 0090: Temporary Grounding and Bonding Systems: Grounding and Bonding for Fuelling Operations.

6.0 Grips

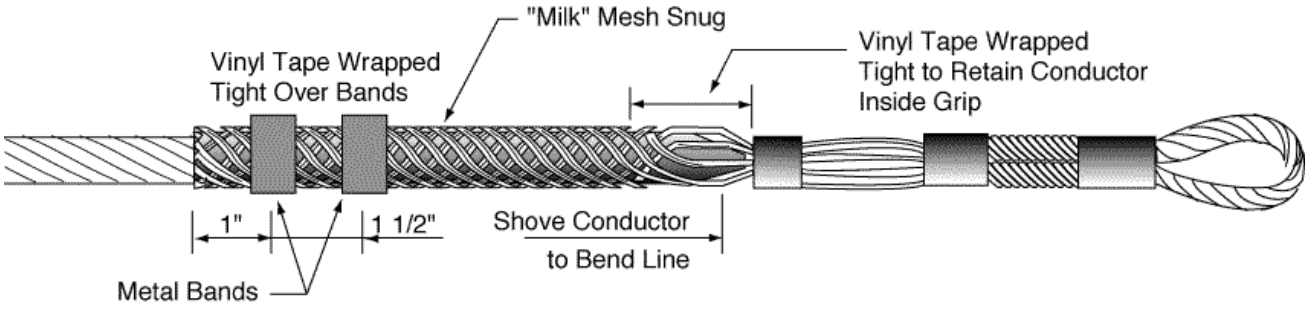
6.1 Kellem Grips

Kellem grips are a fast and easy method of joining pull lines to conductor. They are only slightly larger than the conductor and allow smooth passage of the connections of the pulling line and conductor through the traveller.

The Kellem grip presently recommended for line work is the 'Multiple Strength Conductor Pulling Grip' which may be easily identified by its construction of a single weave section at the open end of the grip, double weave in the center portion and triple weave at the metal shoulder of the grips. The metal shoulders on the grip protect the end of the conductor and equalize strand loading. The grip comes with a flexible wire rope

pulling eye. Refer to PR 0057: Grips and Compression Tools - Wire Mesh Grips for sizing information.

Figure 5: Kellem Grip



6.2 Preform Grips

Swivels must be used when preformed dead ends are utilized as a pulling grip in a running operation. A swivel must be placed between the preform and the pulling line or between two preforms when they are joined back to back, in order to prevent the building up of torque. If torque is not released, it can cause the preform to unravel. Consideration should be given to the use of mesh grips wherever possible. Only the preform grip sizes listed in Table 2 have been tested to establish their efficiency when used on a pulling line in a stringing operation.

Table 2: Preform Grip Properties

Cable	Type (Stranding)	Conductor Dia. (in)	Rated Tensile Strength (RTS) **New**	Grip (Cat Id)	Efficiency of Preform Assembly* (% of RTS)	Safe Working Load @ 3.5:1 **New**
5/16	Steel 160 (7)	.327	9900 lbs.	Black (0909)	100%	2828 lbs.
3/8	Steel 160 (7)	.360	12000 lbs.	Orange (0914)	85%	2914 lbs.
4/0	ACSR (6/1)	.563	8420 lbs.	Red (11107)	70%	1684 lbs.

*Have been determined through tests of preform assemblies joined back to back with a swivel. See WM&T file MU-PR-004-00 "Preforms for Stringing".

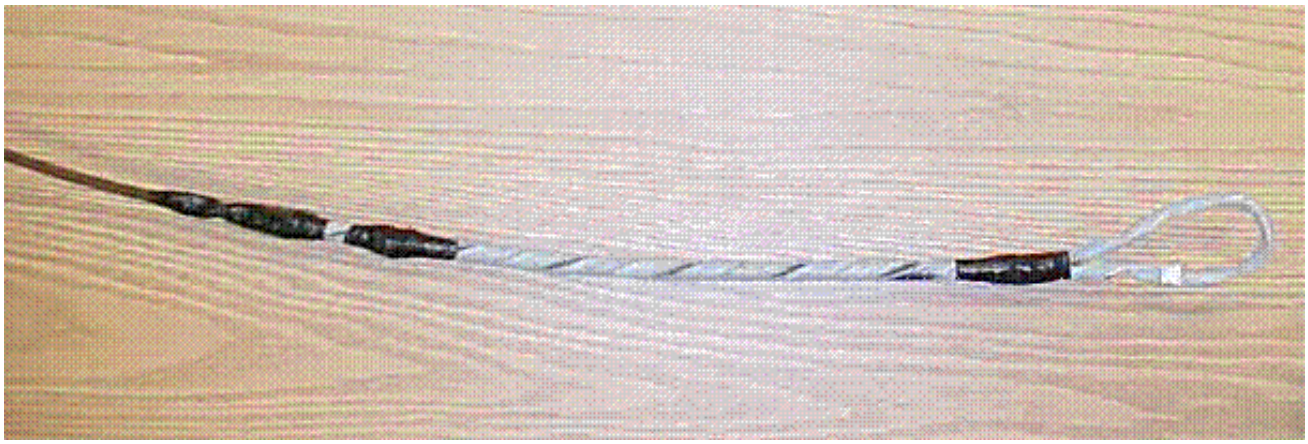
In addition when using preformed grips in a stringing operation the following points must be followed:

- Care should be taken to limit the length of the tail protruding through the eye of the preform as it could become caught during the pulling operation.
- Preforms must be banded.

- Preforms used for stringing purposes are for single use only and must be disposed of after use.

Refer to SP 0150 Preform Grip Installation for Conductor Stringing.

Figure 6: Preform Grip



6.3 Jaw and Bolted Grips

In the larger cable sizes, more common to HV lines, the range of cable size is limited due to the higher tensions. It is very important to match the groove diameter of the grip accurately to the O.D. of the cable.

Ultimate strength tests of grip and conductor assemblies have demonstrated that:

- A single jaw grip, properly installed on ACSR conductor, usually achieves 60% of the conductor RTS (rated tensile strength).
- A tandem jaw grip arrangement, properly installed on ACSR conductor, usually achieves 78% of the conductor RTS. This strength is a 30% increase over a single jaw grip. Tandem grips must **always** be installed with a minimum of **3 feet of clear conductor between jaws**, and must utilize an equalizing sheave and wire rope sling.

The minimum acceptable Factor of Safety (FOS) for a grip/conductor combination is 2:1.

Refer to PR 0056: Grips and Compression Tools - Jaw Grips and PR 0058: Grips and Compression Tools - Bolted Grips.

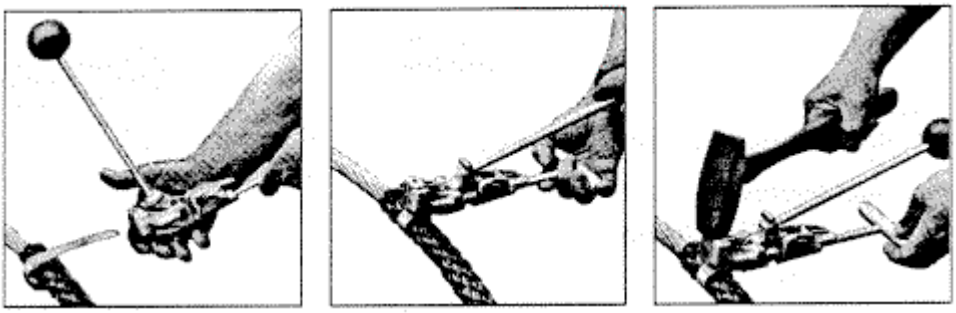
6.4 Punch-Lok Bands

Punch-lok bands must be installed on the open end of all Kellem grips 25 mm (1 inch) from the end. This is to prevent the edges of the grip from catching on the edge of the traveler and thereby pulling the grip off. It is strongly recommended that the front (pulling end) of the grip be taped so the conductor strands will not come through the aluminum shoulders on the grip.

When using Preform grips for stringing install one band approx. 6" below looped eye at first cross over mark. Install a second and third band approx. 3" & 6" from the end of the preform.

Refer to HO 4053: Mesh Grip Installation on Conductor and Synthetic Rope.

Figure 7: Punch-Lok Installation



7.0 Swivels

Swivels are necessary to join the Kellem or Preform grip on the pulling line and the conductor to prevent the build up of excessive torque. When pulling conductor, the torque builds up rapidly as a result of the pull on the stranded rope by the pulling equipment.

This rotational force is increased by the pull resistance of the conductor and by the resistance of the tension equipment controlling the line sag. Swivels are available in various load ratings for different stringing tension. These swivels pass easily through the travellers.

- Swivels are necessary to make all connections of the pulling line and conductor in tension stringing.
- Swivels are available in various load ratings and should be purchased to suit individual needs.
- In a multi-conductor pull the lead swivel on the running board will be larger than the individual swivels on the conductor.
- Swivels should be discarded whenever a thin dime, approximately 1 mm, will slip between the crown bearings.

Caution: Make sure the set screws in the swivels are tightened.

Figure 8: Swivel

8.0 Operating Tensioners and Pullers

8.1 Pulling Procedure

The following is the recommended procedure for pulling:

Table 3: Pulling Procedure

Step	*Action*
1	Start to pull slowly to remove the slack and elongation out of the pulling line, then stop.
2	Check the length before the pull of to ensure that everything is in the clear and the pulling line is not caught anywhere.
3	Resume pulling when the Supervisor of the Stringing Operation gives the all clear.
4	Bring the stringing operation up to speed gradually. This is intended to keep the conductor from surging. A change of stringing speed may also call for a change in tensioner setting.
5	Increase pulling speed only as directed by the Supervisor of the Stringing Operation.

Note: During tension stringing operations, no worker shall be aloft on any structure while the conductor or pulling rope is in motion.

If it is necessary to pass equipment, such as a running board, through the stringing sheave at a structure, the pull shall be stopped until the worker is in position on the structure. Only the necessary movement to pass the equipment through the stringing sheave shall be allowed. The worker shall descend before tension stringing is resumed. This restriction is not intended when the work is being performed from an aerial device which is safely positioned.

8.2 Changing Reels

As sleeves and conductor are passed around the bull wheels, there are bending stress, as well as tensile stress. When the two are combined, a large stress build up occurs, which could cause damage to the sleeve or in extreme cases it to fail, allowing it to drop uncontrolled to the ground. Accidents have occurred in the past where sleeves have broken and released the conductor, causing damage to equipment and tower/pole structures, as well as causing unplanned outages to underbuilt circuits.

New sleeves must never be passed around the bullwheels.

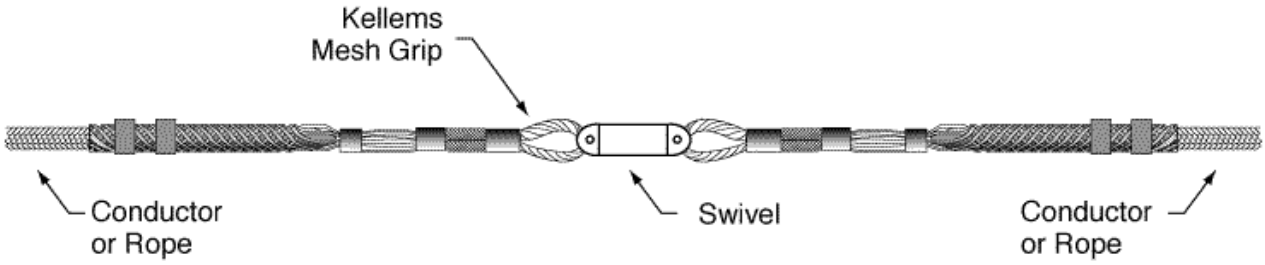
When pulls are longer than one reel in length, splicing will be required using the method outlined in Table 4.

Table 4: Procedure for changing reels

Step	*Action*
1	When the telltale appears indicating that there are three layers left on the reel, notify the puller operator.
2	Run off the conductor until there are four to six turns left on the reel. Stop, apply temporary grounds to the conductor and secure the conductor with a grip. Tell the puller operator to install his grip on the pulling line. This will ensure that the conductor remains up to tension. Where practical, inspect the setting to make sure that adequate clearance from energized apparatus, road crossing, etc., is being maintained over the entire length of the pull. **Note:** The temporary grounds shall be connected to the ground mat enclosure and shall be installed on the conductor(s) with an operating stick.
3	Remove the empty reel, load the new reel of conductor and secure electrical connections to the tensioner.
4	Install a kellem grip to the tail on the new reel.
5	Install a second kellem grip to the tail of the conductor from the old reel that has yet to be run through the bull wheel.
6	Connect the kellems together with a swivel.
7	Take tension on the tensioner until the grip is slack Remove safety grips and temporary grounds.
8	Pull kellem grip assembly through the bull wheels until it is far enough in front of the machine to join with a sleeve
9	Re-apply grounds to tails and secure conductor with a grip.
10	Clean, cut and splice conductor .

11	Take tension on the tensioner until the grip is slack. Remove the grip and temporary ground from the conductor; the machine is ready to string the next reel of conductor.

Figure 9: Connecting Mesh Grips



8.3 Stringing Using Existing Conductor or Shieldwire

Old conductor, particularly OHGW (shieldwire) may be very brittle and can break easily during stringing. Exercise extreme caution; refer to existing test results or consider taking samples for testing to confirm residual strength.

In the majority of situations the new conductor/shieldwire will be pulled into place using the old wire. If the old conductor/shieldwire is not strong enough to pull in the new shieldwire then a rope should be pulled in first and then the new shieldwire. Short stringing setups should also be considered. Refer to HO 1987: Tension Stringing of Shieldwire.

Typically compression sleeves should not be passed around the small radius of the bull wheel. An exception to this is during re-conductoring where the old conductor used to pull in new conductor is passed over the bullwheels and onto the split reel at the puller end. A random inspection of compression sleeves should be carried out. If sleeves are suspect, have samples taken and tested.

In the past several methods have been used in an attempt to prevent the conductor from breaking free. Use the example in Table 5.

Table 5: Passing sleeves through the bull wheel

Step	*Action*
1	Stop the pull when the sleeve is approximately 5ft from the puller fairlead.
2	Place a conductor grip approximately 200 feet in front of the puller fairlead.
3	Connect the grip to a suitable length of Uniline or other non-conductive rope of sufficient strength.
4	Run the Uniline through a block located at the pulling machine.
5	Attached the free end of the Uniline to a bulldozer or suitable sized truck.
6	Pull up tension on the Uniline with the truck.

7	Restart the pull having the puller slowly bring the sleeve through the bull wheels.
8	Maintain tension on the Uniline with the truck until the sleeve has passed fully through the bullwheels and wrapped onto the split reel a minimum of 3 wraps.

9.0 Splicing Conductor and Shieldwire

When splicing conductor high circulating current and Ferranti voltages may be present. For this reason bonding both conductors to the bonded mat is essential prior to performing splicing or when handling. The same principle applies to splicing conductors in the air. Placing a jumper between the two conductors to be cut or sleeved and bonding the crane boom to the conductor, bypasses the worker with a low resistance path. Refer to: SP 0089: Temporary Grounding and Bonding Systems - Transport and Work Equipment.

For information on compression connectors refer to HO 0696: Installing Compression Connectors and Jumper Terminals and PR 0055: Grips and Compression Tools - Fittings and Dies.

Implosive connectors are compressed by means of an implosive charge, which is initiated by a non-electric detonator. All employees must successfully complete a training course and be proven competent before handling implosive connectors.

The user must comply with any pertinent regulations relating to transportation, handling, storage and use of detonators and implosive sleeves. A responsible person must ensure that all safety regulations are adhered to. For additional information on implosive connectors refer to HO 2827: The Use of Implosive Connectors Circuit De-Energized.

10.0 Sagging Conductor and Shieldwire

During the stringing of transmission lines the conductors are strung to a predetermined sag. If the actual sag is less than the predetermined sag, vibrations resulting from the increased tension may result in damage to the structure hardware and the conductor. If the actual sag is greater than the predetermined sag, electrical clearances may not be sufficient.

Conductors are sagged in progressive order from the let up point toward the unsagged end. The conductors must be sagged within tolerances stated in the specification which is usually ± (4 in) 100 mm.

Sagging may be done aloft from an aerial device or from the gradient mat. During the sagging operation from the gradient mat, conductor must not be touched from outside the bonded area. Exercise caution if the conductor is within 3.6m (12 ft) of the ground. For additional safety, the work area of the sagging equipment employed in the sagging operation should be roped off with "danger" signs.

For additional information on sagging refer to HO 2036: Taking Sags with a Transit or Theodolite (A) in the Same Span or (B) from an Adjacent Span and HO 0308: Checking Conductor Sag on Towers and Wood Pole Structures using a Telescope

11.0 Use of Helicopters During Stringing Operations

When helicopters are involved, pre-planning the job is the most important factor in providing the safest working environment possible and minimizing needless expense.

For additional information refer to TD 2544: Job Planning when using Helicopters.

One advantage of using helicopters is to minimize the damage to the environment.

Helicopters can be used to pull out the pilot rope used during the stringing operation. Typically the rope, which is fed from the flyrope carrier stationed at the pulled end, is flown toward the tensioner end. Starting with the bottom conductor position, the pilot flies the helicopter along the stringing section while maneuvering the machine to install the rope into each traveller. Travellers are fitted with special arms to assist the pilot with this operation however it may be necessary to provide some assistance from the structure.

Refer to HO 2301: Stringing Pilot Rope on Emergency Restoration Structures (ERS) Using a Helicopter.

Helicopters may also be used when accessing transmission line structures or for patrolling the line section during the stringing operation. Refer to PR 0137: Accessing Transmission Line Structures using the Helicopter AirStair and HO 0770: Physical Clearances for Helicopters

12.0 Job Aids - Stringing Forms

- Instruction for Tension Stringing (click here to view Form)
- Tension Stringing Observer's Duties (click here to view Form)
- Tension Stringing Procedure and Planning Checklist (click here to view Checklist)
- Tension Stringing Strength Requirements "Defining the Weakest Link" (click here to view Checklist)

13.0 HODS Document reference

TD 1000	Job Planning
HO 0050	Notification of Work at Road and Railway Crossings
HO 0064	Work Under a Hold-Off on Transmission/Distribution Lines
HO 0100	Tension Stringing Using Wooden Reels
HO 0267	Determining Soil Conditions Using a Chance Probe and Installing Screw Anchors
HO 0308	Checking Conductor Sag on Towers and Wood Pole Structures using a Telescope

HO 0696	Installing Compression Connectors and Jumper Terminals
HO 0770	Physical Clearances for Helicopters
HO 1049	Installation of Conductor Travellers on 115 kV and 230 kV Suspension Towers Circuit De-Energized
HO 1900	Installation of Rider Poles and Rider Arms
HO 1950	Installing Helper Cables and Tie-downs on Conductors
HO 1987	Tension Stringing of Shieldwire
HO 2036	Taking Sags with a Transit or Theodolite (A) in the Same Span or (B) from an Adjacent Span
HO 2301	Stringing Pilot Rope on Emergency Restoration Structures (ERS) Using a Helicopter
HO 2827	The Use of Implosive Connectors Circuit De-Energized
HO 2829	Overhead Protection

HO 4014	Splicing and Eye Termination Methods for Uniline Synthetic Fibre Rope
HO 4051	Installation Care and Use of Shieldwire Riders
HO 4053	Mesh Grip Installation on Conductor and Synthetic Rope
HO 4079	Warning Barriers
HO 4084	Working in the Vicinity of Underground Services
HO 4191	Stringing System Strength Requirements
PR 0001	Craning and Rigging Handbook - Contents, Definitions and Appendices
PR 0055	Grips and Compression Tools - Fittings and Dies
PR 0056	Grips and Compression Tools - Jaw Grips
PR 0057	Grips and Compression Tools - Wire Mesh Grips
PR 0058	Grips and Compression Tools - Bolted Grips
PR 0075	Preparation for De-energized Work Over 50 kV
PR 0078	Temporary Grounding and Bonding Systems Handbook: Introduction; Contents; Definitions; Explanations
PR 0098	Transmission Lines Grounding and Bonding - General
PR 0137	Accessing Transmission Line Structures using the Helicopter AirStair
SP 0089	Temporary Grounding and Bonding Systems - Transport and Work Equipment
SP 0090	Temporary Grounding and Bonding Systems - Fuel Operations
SP 0099	Transmission Lines Grounding and Bonding Arrangements
SP 0100	Transmission Lines Grounding and Bonding - Removal of Grounds
SP 0106	Excavation in the Vicinity of Gas Lines
SP 0140	Job Planning - Construction Services
SP 0143	Requirements for Development of Traffic Protection Plans
SP 0150	Preform Grip Installation for Conductor Stringing

TD 2544	Job Planning when using Helicopters

14.0 Definitions

Bonded
Conductive parts of equipment metallically interconnected to maintain a common electrical potential.

Breaking Strength
The unit stress in psi (kpa) at which a material actually breaks.

Bull line
The steel cable used to pull in conductor.

Bundle
A set of sub-conductors (usually four) strung and connected to act as a single conductor.

Circuit
A closed path for electric current. In transmission lines, the conductors forming 3 alternating current electrical phases (red, white, blue).

Deadending
A procedure which results in the termination of conductors at an anchor tower.

Decking
The act of raising insulators, hardware, etc. into position.

De-Energized
A circuit that is isolated and grounded.

Effective span
The term used to designate the portion of the conductor which is supported by a structure. If the supports for the conductor at each end of a span are at the same elevation, the low point of the conductor is at the middle of the span and each structure will support one half of the conductor. In this case, the effective span is equal to the actual span. If one support is higher than the other, the low point of the conductor will be closer to the lower support and each structure will then support that portion of the conductor between the structure and the low point.

Factor of Safety (Rigging)
The ratio of breaking strength to the maximum anticipated applied force. (Normally 5:1 for rigging)

Fall Arrest System
A safety system designed to minimize injury due to a fall, by either restricting the worker's movements to prevent a fall, or by arresting an accidental fall (FAS).

Fault
Accidental electrical connection between an electrically energized component and earth or some extended conducting body, that achieves the same purpose as earth.

Finger Line
The Finger Line is a rope used to pull in the pilot line. Its length is usually twice the ground to traveller distance and it is installed when the traveller is installed.

Flyrope
Initial pilot line used to pull uniline or bull line.

Grip-all Stick
An electrically insulated handle fitted with a remotely controlled grip for holding tools.

Ground
An intentional electrical connection between an electrically energized component and earth or some extended conducting body, that achieves the same purpose as earth.

Hold-off
A procedure which limits operation of apparatus in the event of an accidental contact

Implosive
An inwardly directed explosive energy for conductor splice compression as an alternative to hydraulic compression.

Initiation
Setting off an explosive charge.

Isolated
Known sources of electrical potential are disconnected but there is no guarantee that circuit is de-energized until it is grounded.

Penetrox
A chemical inhibitor that prevents the buildup of oxides on (Anti-oxidant paste) aluminum and copper conductors.

Pilot Line
The Pilot Line (fly rope) is a non-rotating rope used to pull in the larger pulling rope under tension. It is installed by hand using the previously installed finger line.

Phase
One of the three conductors that form a transmission line.

Ruling Span
The ruling span may be defined as that span length in which the tension in the conductor, under changes in temperature and loading, will most nearly agree with the average tension in a series of spans of varying lengths between dead ends. A more common definition is that the ruling span is the span length used as a basis for calculating the conductor sags and tensions, constructing the sag template, and preparing the stringing tables.

The ruling span for any section of transmission line having n spans of lengths L1, L_2 L_3...Ln between dead ends may be calculated from the following equation:

$$\text{Ruling span} = \sqrt{\frac{L_1^3 + L_2^3 + L_3^3 + \ldots L_n^3}{L_1 + L_2 + L_3 + \ldots L_n}}$$

Running board
A pulling device designed to permit stringing more than one sub-conductor simultaneously with a single pulling line.

Safe Working Load
The maximum allowable working load established by the manufacturer or an engineer.

Sag
The vertical distance that the lowest part of a conductor hangs below a straight line between end supports. Sag controls line tension and ground clearance.

Setting
The distance between the selected locations of puller and tensioner usually limited by bull line length.

Sub-conductor
One cable of a bundle; 2,3,4,5 sub-conductors make up a bundle.

Tension Stringing
The process of installing overhead line conductors in which there is continuous control of conductor sag.

Ultimate Strength
The greatest unit stress in psi (kpa) a material can withstand without fracture or excessive distortion.

Uniline
A brand of rope that has many parallel filaments of synthetic plastic enclosed in a braided jacket and is used for pulling in the bull line.

Intro Page Home Page Top of Document Document Listing E-Mail

Document Number: **HO 4191 R3**

Document Name: **Stringing System Strength Requirements**

Issue Date: **February 2001**

Any variance from this practice must be documented in the Job Plan.

Purpose

This practice provides a process for every supervisor to follow before starting a stringing operation.

The scope of this document is limited to the components of the actual 'pull' and does not include dead ending work or stringing machines.

Revision

This document replaces HO 4191 R2. Format and/or contents have changed.

This revision includes an updated "Defining the Weakest Link" table, with information on determining the working load limit of wire mesh and jaw grips on old conductor.

Contents

1.0 Need To Know

Essential to every conductor stringing operation is the assurance that each system component has adequate strength and adequate design factor (factor of safety) for the loading to be applied.

1.1 Component Strength Requirements

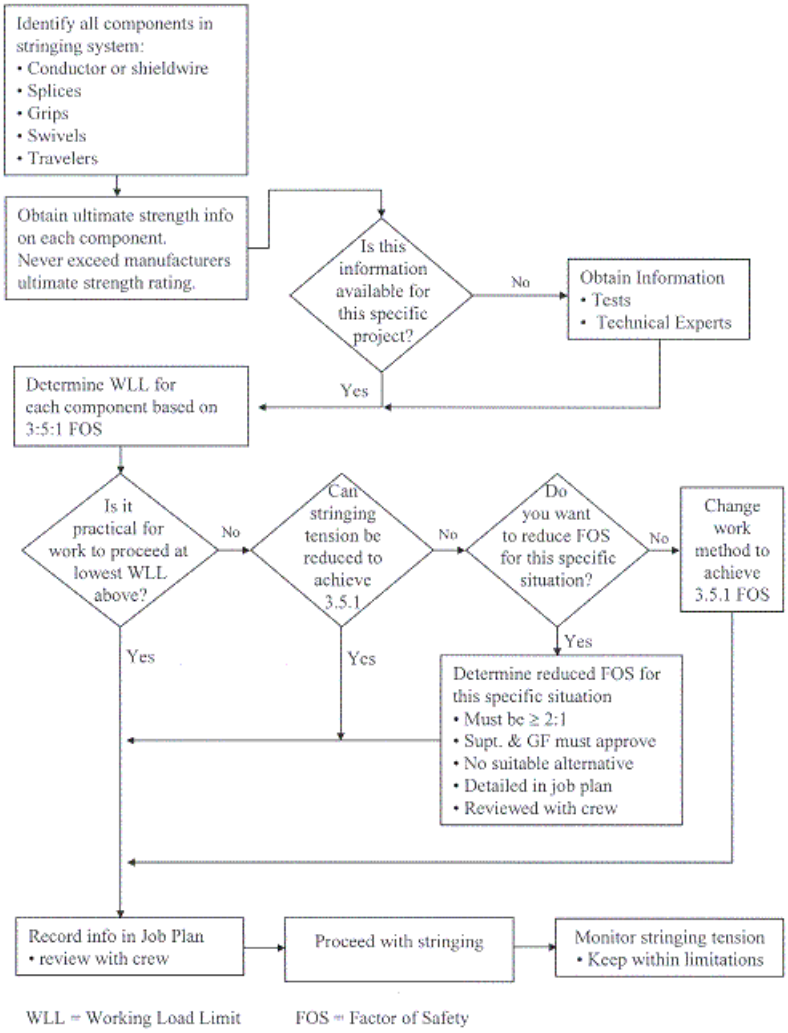
Identify the ultimate strength of each component by referring to manufacturer's information, technical information or test reports. A relatively complete 'quick pick list' is included in the section Tools and Equipment. Follow the process in the flow chart Stringing System – Component Strength and Factor of Safety (See Figure 1). For a convenient method of organizing your information see the table defining the Weakest Links (See Figure 2).

The desired Factor of Safety of 3.5:1 is based on the Occupational Health and Safety Act for Construction.

A Factor of Safety of less than 3.5:1 but never less than 2:1 may be used in specific situations as described in this document. This minimum Factor of Safety must be based on good engineering practice.

Figure 1: Stringing System - Component Strength and Factor Safety

View Version



2.0 Tools and Equipment Required

This information is current at the time of document issue. You should always check to determine if information has been revised.

7/8" Uniline® Synthetic Fibre Rope

The information in this table is based on new rope with average breaking strength of 32,800 lbs. Uniline deteriorates with age and exposure. You should ensure that regular strength tests are conducted. See HODS document SP 0004 (Rigging - Fiber Rope) for further information on Uniline®.

Splice or Termination Method	% Efficiency of Splice or Termination	Ultimate Strength of Splice or Termination	Working Load Limits at 3.5 FOS (lbs.)
Eye - Cable Clip with Thimble	90%	29,520	8,430
Eye - Cable Clip with no Thimble and connected to Hammerlok or Swivel	50%	6,400	4,680
Eye - Mesh Grip (Kellems 1040)	100%	32,800	*6,120
Eye - 'Woven' with Thimble	100%	32,800	9,371
Eye - 'Woven' with no Thimble and connected to Hammerlok or Swivel	50%	16,400	4,680
Splice - 'Woven'	100%	32,800	9,371
Splice - Mesh Grips (Kellems 1040)	100%	32,800	*6,120

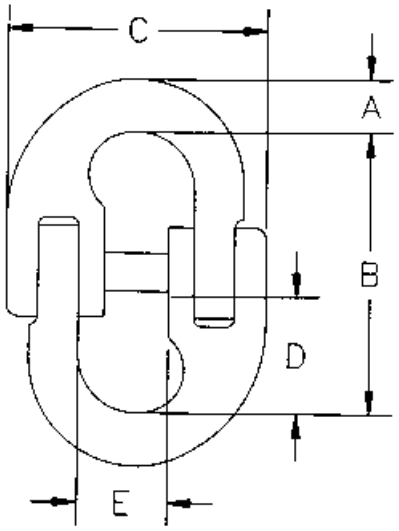
* Working load limited by Kellems grip rating.

3/4" Flyrope

Most Flyrope in use today is Herzog 'Combi-12'; a single braid construction made of polyester and olefin fibers. This construction results in a high strength, low elongation, abrasion resistant, non-rotational and hand spliceable rope.

Average breaking strength (new) = 14,400 lbs.

Connecting Links (Hammerlocks)



CROSBY 'LOK-A-LOY 6' Connecting Links

Chain Size (in)	Minimum Ultimate Strength (lbs.)	Working Load Limit* (lbs.)	Dimensions (in)				
			A	B	B	D	E
1/4	13000	3250	.31	2.06	1.69	.78	.78
3/8	26400	6600	.45	2.72	2.31	1.06	1.09
1/2	45000	11250	.58	3.34	3.16	1.28	1.41
5/8	66000	16500	.78	3.91	3.94	1.56	1.69
3/4	92000	23000	.89	4.84	4.44	1.97	2.00
7/8	115000	28750	1.00	5.81	5.31	2.38	2.12
1	155000	38750	1.08	6.48	6.07	2.84	2.55
1 1/4	230000	57500	1.38	8.48	7.65	3.77	3.77

* Ultimate Strength is 4 times the Working Load Limit.

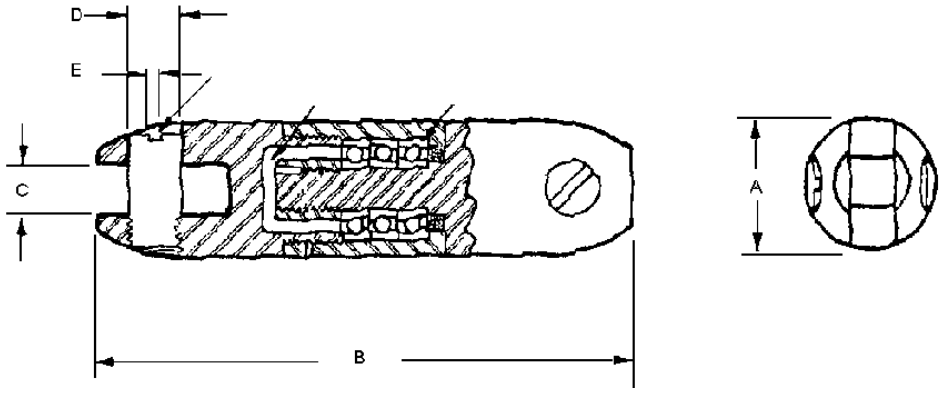
CROSBY 'LOK-A-LOY 8' Connecting Links

Chain Size (in)	Minimum Ultimate Strength (lbs.)	Working Load Limit* (lbs.)	Dimensions (in)				
			A	B	B	D	E
9/32 (1/4)	14000	3500	.36	1.88	1.75	.78	.66
5/16	18000	4500	.39	2.13	1.97	.88	.69
3/8	28400	7100	.52	2.50	2.50	1.03	.88
1/2	48000	12000	.64	3.44	3.22	1.44	1.13
5/8	72400	18100	.75	4.13	3.78	1.73	1.41
3/4	113200	28300	.97	4.94	4.66	2.06	1.63
7/8	136800	34200	1.06	5.50	5.53	2.31	2.00
1	190800	47700	1.22	6.00	6.19	2.50	2.25
1 1/4	289200	72300	1.50	7.43	7.63	3.06	2.56

* Ultimate Strength is 4 times the Working Load Limit.

Swivels

The following information is for 'Bethea' swivels only.



Catalog Number	Ultimate Strength (lbs.)	Working Load Limit (lbs.)*	Overall Diameter A	Overall Length B	Opening Width C	Pin Diameter D	Screw Slot E	Weight Pounds Each
A-1.8	5400	1,800	7/8	3-1/16	5/16	5/16	3/32	.32
BB-4	12000	4,000	1-1/4	4-17/32	9/32	3/8	3/32	.93
B-8	24000	8,000	1-1/2	5-1/8	19/32	7/16	3/32	1.46
C-10	30000	10,000	1-7/8	7	3/4	5/8	5/32	3.49
D-16	48000	16,000	2-7/16	10-15/32	1	7/8	5/32	8.66
D-30	90000	30,000	2-1/2	11-1/16	1	7/8	5/32	10.09

* Ultimate Strength is 3 times the Working Load Limit.

3.0 Defining the Weakest Links

Figure 2: Tension Stringing Strength Requirements

Component	**Manufacture Or Type**	**Working Load Limit** (manufacturer's)	**Ultimate Strength** (New or based on Test)	**Stringing Tension** (see Note 2)	**Actual FOS** (Ultimate Strength) (Stringing Tension)
Fly Rope					
Uniline					
Connecting Link (Hammerlock)					
Swivel					
Mesh Grip					
(Old) Conductor & Mesh Grip Assembly (see Note 1)					
(New) Conductor & Mesh Grip Assembly (from GCTM)					
(Old) Conductor & Jaw Grip Assembly (see Note 1; check "H" number)					
(New) Conductor & Jaw Grip Assembly (from GCTM; check "H" number)					
Puller					
Tensioner					
Travellers					
Special Tools (i.e. running board, antirotation device, insulated link, etc.)				Max. applied load =	

Notes:

1. Calculation of :
   (Old) Cond. & Grip Assembly Ult. Strength = (Old) Cond. Tensile Strength x Ult. Strength for New Assembly

(New)Cond. Tensile Strength

2. Stringing Tension must never exceed manufacturers WLL.

Caution:

- **For all components that will be exposed to sag tension, verify that component has required strength.**
- **Old conductor, particularly OHGW (shieldwire) may be very brittle and can break easily during stringing. Exercise extreme caution; refer to existing test results or consider taking samples for testing to confirm residual strength.**
- **A random inspection of compression sleeves should be carried out. If sleeves are suspect, have samples taken and tested.**