

NERC LSE Standards - Classification on December 4, 2008								
				Responsible Entity				
Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Owning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
BAL-005-0	R1.	All generation, transmission, and load operating within an Interconnection must be included within the metered boundaries of a Balancing Authority Area.	LSE			X		Entity that is either DP or TO is required to do this (entity that physically attaches/connects load and determines metering)
BAL-005-0	R1.3.	Each Load-Serving Entity with load operating in an Interconnection shall ensure that those loads are included within the metered boundaries of a Balancing Authority Area.	LSE			X		Entity that is either DP or TO is required to do this (entity that physically attaches/connects load and determines metering)
CIP-001-1	R1.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	LSE			X		Need to add DP or TO instead of LSE
CIP-001-1	R2.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	LSE			X		Need to add DP or TO instead of LSE
CIP-001-1	R3.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	LSE			X		Need to add DP or TO instead of LSE
CIP-001-1	R4.	Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load-Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.	LSE			X		Need to add DP or TO instead of LSE
CIP-002-1	R1.	Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R1.2.	The risk-based assessment shall consider the following assets:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R1.2.1.	Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R1.2.2.	Transmission substations that support the reliable operation of the Bulk Electric System.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R1.2.3.	Generation resources that support the reliable operation of the Bulk Electric System.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-002-1	R1.2.5.	Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R1.2.6.	Special Protection Systems that support the reliable operation of the Bulk Electric System.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	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 interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R3.1.	The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R3.2.	The Cyber Asset uses a routable protocol within a control center; or,	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R3.3.	The Cyber Asset is dial-up accessible.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-002-1	R4.	Annual Approval — A senior manager or delegate(s) shall approve annually 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 list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	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:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R1.1.	The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R1.2.	The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-003-1	R1.3.	Annual review and approval of the cyber security policy by the senior manager assigned pursuant to R2.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R2.	Leadership — The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity’s implementation of, and adherence to, Standards CIP-002 through CIP-009	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R2.1.	The senior manager shall be identified by name, title, business phone, business address, and date of designation.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R2.2.	Changes to the senior manager must be documented within thirty calendar days of the effective date.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R2.3.	The senior manager or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R3.	Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R3.1.	Exceptions to the Responsible Entity’s cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R3.2.	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R3.3.	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R4.	Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	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, 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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R4.2.	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R5.	Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R5.1.	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-003-1	R5.1.1.	Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R5.1.2.	The list of personnel responsible for authorizing access to protected information shall be verified at least annually.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	R5.3.	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-003-1	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 vendorrelated changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	R1.	Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access 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.).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	R2.	Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	R2.1.	This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	R2.2.	Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	R2.2.1.	The proper use of Critical Cyber Assets;	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	R2.2.2.	Physical and electronic access controls to Critical Cyber Assets;	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	R2.2.3.	The proper handling of Critical Cyber Asset information; and,	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	R2.2.4.	Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-004-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	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. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	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 seven year 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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-004-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Owning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-005-1	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).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R1.5.	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R2.3.	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R2.5.	The required documentation shall, at least, identify and describe:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R2.5.1.	The processes for access request and authorization.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R2.5.2.	The authentication methods.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R2.5.3.	The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R2.5.4.	The controls used to secure dial-up accessible connections.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-005-1	R2.6.	Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R4.1.	A document identifying the vulnerability assessment process;	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R4.2.	A review to verify that only ports and services required for operations at these access points are enabled;	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R4.3.	The discovery of all access points to the Electronic Security Perimeter;	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R4.4.	A review of controls for default accounts, passwords, and network management community strings; and,	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	R5.1.	The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-005-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.	Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-006-1	R1.1.	Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also 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 the Critical Cyber Assets.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.2.	Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.3.	Processes, tools, and procedures to monitor physical access to the perimeter(s).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.4.	Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.5.	Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.6.	Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.7.	Process for updating the physical security plan within ninety calendar days 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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.8.	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R1.9.	Process for ensuring that the physical security plan is reviewed at least annually.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R2.	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:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R2.1.	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R2.2.	Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap”	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R2.3.	Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R2.4.	Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-006-1	R3.	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. One or more of the following monitoring methods shall be used:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R3.1.	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R3.2.	Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R4.	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:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R4.1.	Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R4.2.	Video Recording: Electronic capture of video images of sufficient quality to determine identity.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R4.3.	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 R2.3.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R5.	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R6.	Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R6.1.	Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R6.2.	Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-006-1	R6.3.	Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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, 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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R1.2.	The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R1.3.	The Responsible Entity shall document test results.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R2.	Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R2.1.	The Responsible Entity shall enable only those ports and services required for normal and emergency operations.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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 or an acceptance of risk.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R3.	Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document 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).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R3.1.	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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 or an acceptance of risk.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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 or an acceptance of risk.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R5.1.1.	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R5.1.3.	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R5.2.2.	The Responsible Entity shall identify those individuals with access to shared accounts.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R5.3.	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R5.3.1.	Each password shall be a minimum of six characters.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R5.3.2.	Each password shall consist of a combination of alpha, numeric, and “special” characters.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R5.3.3.	Each password shall be changed at least annually, or more frequently based on risk.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R6.2.	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-007-1	R6.4.	The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R6.5.	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R7.	Disposal or Redeployment — The Responsible Entity shall establish 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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R7.3.	The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R8.1.	A document identifying the vulnerability assessment process;	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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;	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R8.3.	A review of controls for default accounts; and,	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-007-1	R9.	Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-008-1	R1.	Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-008-1	R1.1.	Procedures to characterize and classify events as reportable Cyber Security Incidents.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-008-1	R1.2.	Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
CIP-008-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-008-1	R1.4.	Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-008-1	R1.5.	Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-008-1	R1.6.	Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-008-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-009-1	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:	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-009-1	R1.1.	Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-009-1	R1.2.	Define the roles and responsibilities of responders.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-009-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-009-1	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 ninety calendar days of the change.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-009-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
CIP-009-1	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.	LSE			X		DP and TO critical (responsible - wires/poles, scada system access); Load-side QSE has cyber access into ERCOT so could be critical if ERCOT has critical cyber assets - is the LSE for this
EOP-002-2	R9.1.	The deficient Load-Serving Entity shall request its Reliability Coordinator to initiate an Energy Emergency Alert in accordance with Attachment 1-EOP-002-0.	LSE	X				Protocol governs this standard- No "LSE" is aware of need to initiate, so noone else needs to be registered.
EOP-004-1	R2.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall promptly analyze Bulk Electric System disturbances on its system or facilities.	LSE			X		DP or TO are responsible for analyzing own facilities
EOP-004-1	R3.	A Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity experiencing a reportable incident shall provide a preliminary written report to its Regional Reliability Organization and NERC.	LSE			X		DP and TO must report if on their facilities and must submit to NERC & ERCOT - BA and RC already registered

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
EOP-004-1	R3.1.	The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load-Serving Entity shall submit within 24 hours of the disturbance or unusual occurrence either a copy of the report submitted to DOE, or, if no DOE report is required, a copy of the NERC Interconnection Reliability Operating Limit and Preliminary Disturbance Report form. Events that are not identified until some time after they occur shall be reported within 24 hours of being recognized.	LSE			X		DP and TO must report if on their facilities and must submit to NERC & ERCOT - BA and RC already registered
EOP-004-1	R3.2.	Applicable reporting forms are provided in Attachments 022-1 and 022-2.	LSE			X		DP and TO must report if on their facilities and must submit to NERC & ERCOT - BA and RC already registered
EOP-004-1	R3.3.	Under certain adverse conditions, e.g., severe weather, it may not be possible to assess the damage caused by a disturbance and issue a written Interconnection Reliability Operating Limit and Preliminary Disturbance Report within 24 hours. In such cases, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall promptly notify its Regional Reliability Organization(s) and NERC, and verbally provide as much information as is available at that time. The affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall then provide timely, periodic verbal updates until adequate information is available to issue a written Preliminary Disturbance Report.	LSE			X		DP and TO must report if on their facilities and must submit to NERC & ERCOT - BA and RC already registered
EOP-004-1	R3.4.	If, in the judgment of the Regional Reliability Organization, after consultation with the Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity in which a disturbance occurred, a final report is required, the affected Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, or Load-Serving Entity shall prepare this report within 60 days. As a minimum, the final report shall have a discussion of the events and its cause, the conclusions reached, and recommendations to prevent recurrence of this type of event. The report shall be subject to Regional Reliability Organization approval.	LSE			X		DP and TO must report if on their facilities and must submit to NERC & ERCOT - BA and RC already registered
FAC-002-0	R1.	The Generator Owner, Transmission Owner, Distribution Provider, and Load-Serving Entity seeking to integrate generation facilities, transmission facilities, and electricity end-user facilities shall each coordinate and cooperate on its assessments with its Transmission Planner and Planning Authority. The assessment shall include:	LSE			X		DPS and TOs already covered - no additional entity needed as LSE (?) Does ERCOT get any information from QSE - or just TOs DPS
FAC-002-0	R1.1.	Evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems.	LSE			X		DPS and TOs already covered - no additional entity needed as LSE (?) Does ERCOT get any information from QSE - or just TOs DPS
FAC-002-0	R1.2.	Ensurance of compliance with NERC Reliability Standards and applicable Regional, subregional, Power Pool, and individual system planning criteria and facility connection requirements.	LSE			X		DPS and TOs already covered - no additional entity needed as LSE (?) Does ERCOT get any information from QSE - or just TOs DPS
FAC-002-0	R1.3.	Evidence that the parties involved in the assessment have coordinated and cooperated on the assessment of the reliability impacts of new facilities on the interconnected transmission systems. While these studies may be performed independently, the results shall be jointly evaluated and coordinated by the entities involved.	LSE			X		DPS and TOs already covered - no additional entity needed as LSE (?) Does ERCOT get any information from QSE - or just TOs DPS
FAC-002-0	R1.4.	Evidence that the assessment included steady-state, short-circuit, and dynamics studies as necessary to evaluate system performance in accordance with Reliability Standard TPL-001-0.	LSE			X		DPS and TOs already covered - no additional entity needed as LSE (?) Does ERCOT get any information from QSE - or just TOs DPS
FAC-002-0	R1.5.	Documentation that the assessment included study assumptions, system performance, alternatives considered, and jointly coordinated recommendations.	LSE			X		DPS and TOs already covered - no additional entity needed as LSE (?) Does ERCOT get any information from QSE - or just TOs DPS

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
FAC-002-0	R2.	The Planning Authority, Transmission Planner, Generator Owner, Transmission Owner, Load-Serving Entity, and Distribution Provider shall each retain its documentation (of its evaluation of the reliability impact of the new facilities and their connections on the interconnected transmission systems) for three years and shall provide the documentation to the Regional Reliability Organization(s) Regional Reliability Organization(s) and NERC on request (within 30 calendar days).	LSE			X		DPs and TOs already covered - no additional entity needed as LSE (?) Does ERCOT get any information from QSE - or just TOs DPs
INT-001-3	R1	The Load-Serving, Purchasing-Selling Entity shall ensure that Arranged Interchange is submitted to the Interchange Authority for: R1.1. All Dynamic Schedules at the expected average MW profile for each hour.	Not LSE				PSE	Only applicable to PSEs - no other LSEs
IRO-001-1	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.	LSE		X	X	Resource entities with LAARs, REP that are LAAR, All QSE that represent LAARs	QSEs (balanced Schedule) entities should all be required to comply
IRO-004-1	R4.	Each Transmission Operator, Balancing Authority, Transmission Owner, Generator Owner, Generator Operator, and Load-Serving Entity in the Reliability Coordinator Area shall provide information required for system studies, such as critical facility status, Load, generation, operating reserve projections, and known Interchange Transactions. This information shall be available by 1200 Central Standard Time for the Eastern Interconnection and 1200 Pacific Standard Time for the Western Interconnection.	LSE		X	X	All Entities provide a piece of data for this requirement	DPs and TOs should all be required to comply
IRO-005-1	R13.	Each Reliability Coordinator shall ensure that all Transmission Operators, Balancing Authorities, Generator Operators, Transmission Service Providers, Load-Serving Entities, and Purchasing-Selling Entities operate to prevent the likelihood that a disturbance, action, or non-action in its Reliability Coordinator Area will result in a SOL or IROL violation in another area of the Interconnection. In instances where there is a difference in derived limits, the Reliability Coordinator and its 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.	LSE			X		DPs or Tos provide to ERCOT
MOD-017-0	R1.	The Load-Serving Entity, Planning Authority, and Resource Planner shall each provide the following information annually on an aggregated Regional, subregional, Power Pool, individual system, or Load-Serving Entity basis to NERC, the Regional Reliability Organizations, and any other entities specified by the documentation in Standard MOD-016-1_R 1.	LSE	X		X		Not to this degree - Regional Standard Needed
MOD-017-0	R1.1.	Integrated hourly demands in megawatts (MW) for the prior year.	LSE	X		X		DP and TO or does ERCOT have historic electronically
MOD-017-0	R1.2.	Monthly and annual peak hour actual demands in MW and Net Energy for Load in gigawatthours (GWh) for the prior year.	LSE	X		X		DP and TO or does ERCOT have historic electronically
MOD-017-0	R1.3.	Monthly peak hour forecast demands in MW and Net Energy for Load in GWh for the next two years.	LSE	X		X		DP and TO or does ERCOT have historic electronically

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
MOD-017-0	R1.4.	Annual Peak hour forecast demands (summer and winter) in MW and annual Net Energy for load in GWh for at least five years and up to ten years into the future, as requested.	LSE	X		X		Is this only ERCOT - or does ERCOT rely upon anyone else to provide data?
MOD-018-0	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner and Resource Planner's report of actual and forecast demand data (reported on either an aggregated or dispersed basis) shall:	LSE	X		X		Regional Standard needed?
MOD-018-0	R1.1.	Indicate whether the demand data of nonmember entities within an area or Regional Reliability Organization are included, and	LSE	X		X		Does ERCOT rely upon data from any entities - which ones?
MOD-018-0	R1.2.	Address assumptions, methods, and the manner in which uncertainties are treated in the forecasts of aggregated peak demands and Net Energy for Load.	LSE	X		X		Is this only ERCOT - or does ERCOT rely upon anyone else to provide data?
MOD-018-0	R1.3.	Items (MOD-018-0_R 1.1) and (MOD-018-0_R 1.2) shall be addressed as described in the reporting procedures developed for Standard MOD-016-1_R 1.	LSE	X		X		Is this only ERCOT - or does ERCOT rely upon anyone else to provide data?
MOD-018-0	R2.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each report data associated with Reliability Standard MOD-018-0_R1 to NERC, the Regional Reliability Organization, Load-Serving Entity, Planning Authority, and Resource Planner on request (within 30 calendar days).	LSE	X		X		Is this only ERCOT - or does ERCOT rely upon anyone else to provide data on LaaR? QSE representing REP with interruptable load.
MOD-019-0	R1.	The Load-Serving Entity, Planning Authority, Transmission Planner, and Resource Planner shall each provide annually its forecasts of interruptible demands and Direct Control Load Management (DCLM) data for at least five years and up to ten years into the future, as requested, for summer and winter peak system conditions to NERC, the Regional Reliability Organizations, and other entities (Load-Serving Entities, Planning Authorities, and Resource Planners) as specified by the documentation in Reliability Standard MOD-016-1_R 1.	LSE	X				LSE = QSE representing LaaR
MOD-020-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make known its amount of interruptible demands and Direct Control Load Management (DCLM) to Transmission Operators, Balancing Authorities, and Reliability Coordinators on request within 30 calendar days.	LSE	X	X			
MOD-021-0	R1.	The Load-Serving Entity, Transmission Planner, and Resource Planner's forecasts shall each clearly document how the Demand and energy effects of DSM programs (such as conservation, time-of-use rates, interruptible Demands, and Direct Control Load Management) are addressed.	LSE	X				
MOD-021-0	R2.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each include information detailing how Demand-Side Management measures are addressed in the forecasts of its Peak Demand and annual Net Energy for Load in the data reporting procedures of Standard MOD-016-0_R 1.	LSE	X				
MOD-021-0	R3.	The Load-Serving Entity, Transmission Planner, and Resource Planner shall each make documentation on the treatment of its DSM programs available to NERC on request (within 30 calendar days).	LSE	X				No additional LSE needed (DP and TO included)
PRC-007-0	R2.	The Transmission Owner, Transmission Operator, Distribution Provider, and Load-Serving Entity that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide, and annually update, its underfrequency data as necessary for its Regional Reliability Organization to maintain and update a UFLSprogram database.	LSE			X		No additional LSE needed (DP and TO included)

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
PRC-009-0	R1.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall analyze and document its UFLS program performance in accordance with its Regional Reliability Organization's UFLS program. The analysis shall address the performance of UFLS equipment and program effectiveness following system events resulting in system frequency excursions below the initializing set points of the UFLS program. The analysis shall include, but not be limited to:	LSE			X		No additional LSE needed (DP and TO included)
PRC-009-0	R1.1.	A description of the event including initiating conditions.	LSE			X		No additional LSE needed (DP and TO included)
PRC-009-0	R1.2.	A review of the UFLS set points and tripping times.	LSE			X		No additional LSE needed (DP and TO included)
PRC-009-0	R1.3.	A simulation of the event.	LSE			X		No additional LSE needed (DP and TO included)
PRC-009-0	R1.4.	A summary of the findings.	LSE			X		No additional LSE needed (DP and TO included)
PRC-009-0	R2.	The Transmission Owner, Transmission Operator, Load-Serving Entity, and Distribution Provider that owns or operates a UFLS program (as required by its Regional Reliability Organization) shall provide documentation of the analysis of the UFLS program to its Regional Reliability Organization and NERC on request 90 calendar days after the system event.	LSE			X		No additional LSE needed (DP and TO included)
PRC-010-0	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).	LSE			X		No additional LSE needed (DP and TO included)
PRC-010-0	R1.1.	This assessment shall include, but is not limited to:	LSE			X		No additional LSE needed (DP and TO included)
PRC-010-0	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.	LSE			X		No additional LSE needed (DP and TO included)
PRC-010-0	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.	LSE			X		No additional LSE needed (DP and TO included)
PRC-010-0	R1.1.3.	A review of the voltage set points and timing.	LSE			X		No additional LSE needed (DP and TO included)
PRC-010-0	R2.	The Load-Serving Entity, Transmission Owner, Transmission Operator, and Distribution Provider that owns or operates a UVLS program shall provide documentation of its current UVLS program assessment to its Regional Reliability Organization and NERC on request (30 calendar days).	LSE			X		No additional LSE needed (DP and TO included)
PRC-022-1	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:	LSE			X		No additional LSE needed (DP and TO included)
PRC-022-1	R1.1.	A description of the event including initiating conditions.	LSE			X		No additional LSE needed (DP and TO included)
PRC-022-1	R1.2.	A review of the UVLS set points and tripping times.	LSE			X		No additional LSE needed (DP and TO included)
PRC-022-1	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.	LSE			X		No additional LSE needed (DP and TO included)
PRC-022-1	R1.4.	A summary of the findings.	LSE			X		No additional LSE needed (DP and TO included)
PRC-022-1	R1.5.	For any Misoperation, a Corrective Action Plan to avoid future Misoperations of a similar nature.	LSE			X		No additional LSE needed (DP and TO included)

Standard Number	Requirement Number	Text of Requirement	LSE	Regional Standard Needed	Non-asset-owning LSE - QSE W/LAAR or EILS	Asset-Ownning LSE - TO	Comments	TRE Comments on Requirements/Responsibility
PRC-022-1	R2.	Each Transmission Operator, Load-Serving Entity, and Distribution Provider that operates a UVLS program shall provide documentation of its analysis of UVLS program performance to its Regional Reliability Organization within 90 calendar days of a request.	LSE			X		QSEs representing load
TOP-001-1	R4.	Each Distribution Provider and Load-Serving Entity shall comply with all reliability directives issued by the Transmission Operator, including shedding firm load, unless such actions would violate safety, equipment, regulatory or statutory requirements. Under these circumstances, the Distribution Provider or Load-Serving Entity shall immediately inform the Transmission Operator of the inability to perform the directive so that the Transmission Operator can implement alternate remedial actions.	LSE		X			QSEs representing load
TOP-002-2	R3.	Each Load-Serving Entity and Generator Operator shall coordinate (where confidentiality agreements allow) its current-day, next-day, and seasonal operations with its Host Balancing Authority and Transmission Service Provider. Each Balancing Authority and Transmission Service Provider shall coordinate its current-day, next-day, and seasonal operations with its Transmission Operator.	LSE		X			DP and TO
TOP-002-2	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.	LSE			X		

PSE