

Risk Dashboard

November 2025

For more details on each risk, see the [WECC Risk Register](#).

Changing Resource Mix

Name	Description	Links to Resources & Related Documents
Generation Resource Mix Impacts to Future Transmission Congestion	Building new transmission takes years to complete due to many factors leading to WECC studies showing current transmission paths with higher utilization in the future, and in some cases, exceeding their rating.	SOTI— Transmission

Cybersecurity

Name	Description	Links to Resources & Related Documents
Artificial Intelligence	Public development of AI is a rapidly growing online sector and is out of entity control, leading to reconnaissance of entity information becoming much easier for a threat actor to exploit, and weaponization and delivery becoming easier to generate.	SOTI— Security
Compromised Supply Chain	Compromised vendors can be a source of cyber-attacks on critical infrastructure, which could include the loss of confidential information stored by the vendor, the delivery of malware, or a compromised vendor	

	connected to a customer's critical systems being used as a conduit for unauthorized disclosure.	
Cybersecurity in Transmission Planning	Traditional transmission planning processes do not include cyber-informed transmission planning approaches that incorporate cybersecurity risks, which can prevent industry from more effectively mitigating the reliability impacts of cyberattacks.	
Insider Threat	A trusted insider uses their authorized access to deliberately or accidentally harm assets, which can lead to unauthorized operation of cyber assets.	SOTI— Security
Internet of Things (IoT)	Malicious threat actors could compromise many high-wattage IoT devices (such as air conditioners, heaters, charging stations, Distributed Energy Resources (DER) that are connected to the grid's distribution network and turn them into a botnet. They could then use the botnet to launch a coordinated attack to manipulate demand across distribution grids.	
Malware	Software from any source on an entity's corporate system that seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control of a device's operations.	SOTI— Security
Perimeter Breach	Unauthorized actions on digital assets within an organizational network. Upon infiltration, malicious parties may exploit other hacking activities, such as malware and endpoint attacks, to attack the entity network.	
Perimeterless Operational Technology	Systems and software used to peripherally interact or transmit into cyber assets that are not within an enterprise-owned network boundary. This may lead to unintended misoperation of cyber assets. Integrating BYOD, IoT, or other external operational technology assets as extensions of the	

	electric grid is a growing trend and potentially necessary for future operation.	
Phishing and Social Engineering	When a threat actor exploits trusted single insider access to harm critical cyber assets.	SOTI— Security
Physical Attacks on Cyber Assets	Insufficient physical controls to protect against unauthorized physical access to cyber assets, which could allow threat actors to exploit hardware and software to which they can gain physical access.	
Public Cloud/Cloud Computing	Using cloud-based services to maintain or control Western Interconnection (WI) BPS resources can introduce a new threat vector for threat actors to exploit that is outside the ownership of Registered Entities.	
Third-Party Operations	Unvetted and unmonitored third parties with unverified security controls can lead to unintended misoperation of cyber assets.	
Unauthorized Software & Hardware	Unauthorized use, including authorized software and hardware that is end-of-life or unmaintained to the point of vulnerability, can allow threat actors to exploit the unknown/vulnerable software or hardware leading to attack on the entity network.	
Zero-Day Exploit	The existence of a computer-software vulnerability previously unknown to those interested in its mitigation can allow hackers to adversely affect programs, data, additional computers or a network until the vulnerability is mitigated.	
Technology Availability Risk	Out-of-date systems (electro-mechanical) being functionally unusable to current staff because of the difference between new and old technology. Systems or data are unavailable to the right people at the right time.	

Extreme Natural Events

Name	Description	Links to Resources & Related Documents
Drought (Aridification)	Severe and extended drought conditions can cause reduction of availability of some hydro resources in the West and limit the cooling capacity of thermal generation.	SOTI— Extreme Natural Events
Large and Prolonged Heat Waves	Prolonged heat waves cause stress on the interconnection as BAs work to ensure there is enough generation to meet the demand and transmission available to transfer it. The impact can also be more significant depending on the magnitude of the heat wave. As the ambient temperature rises, derates will occur for transmission and generation thermal ratings, causing a lack of transmission and generation availability.	SOTI— Extreme Natural Events August 2020 Heatwave Event Analysis Report
Wildfire	Wildfires can cause service disruptions to transmission and generation assets by affecting the equipment directly (e.g., fire burning equipment) and indirectly (e.g., smoke causing transmission line arcing, sediment on insulators). Depending on factors like the magnitude or location, the disruptions and loss of load can be prolonged (e.g., remote areas). In addition, extreme wildfires can create their own climates, which can cause unsafe mitigation conditions, slowing restoration or exacerbating its impact and the damage it causes.	Wildfire Weekly Update Wildfire Dashboard SOTI— Extreme Natural Events
Cold Weather Preparedness	Applicable Western Interconnection entities may not be implementing best practices learned from recent cold weather events or have adequate plans for winter preparedness. Generation assets are affected by cold weather and will trip offline if they are not prepared for cold ambient	SOTI— Extreme Natural Events Extreme Weather Preparedness Assurance Program

	temperatures. Transmission assets can also be affected due to icing on the lines, which will eventually cause them to be derated or forced out of service (e.g., arcing, line sagging).	
Geomagnetic Disturbance	GMD events can adversely affect the operation of interconnected transmission systems. During a GMD, geomagnetic-induced currents (GIC) may cause transformer hot-spot heating or damage, loss of reactive power sources, increased reactive power demand, and protection system malfunction, the combination of which may result in voltage collapse and potential blackouts. Extremely strong GMDs, though rare, can induce strong quasi-dc currents in the electric grid that could affect system voltages, relay and protection system performance, and the operation and health of some large power transformers. Geomagnetic storms can disrupt/delay the communication of critical data.	TPL-007-4 Controls Guidance and Compliance Failure Points Western Electricity Coordinating Council
Haboobs (Extreme Dust Storm)	Haboobs and debris flows are expected to increase annually, with more frequency due to changing climate. Large dust storms can take down trees and power lines, bury equipment, fill reservoirs and rivers with dirt, damage buildings, and cause extreme health issues in livestock and people. A secondary effect of haboobs is the dust after the storms preventing or reducing the output of both utility-scale and rooftop solar panels. This output reduction could last several days beyond the storms as owners work to clean the panels. Delays can be extended during drought conditions with local governmental programs limiting water usage. Dust storm contamination of the line insulators and subsequent high humidity can cause lines to flash and fault.	
Atmospheric Rivers	Atmospheric rivers are the most significant transport mechanisms of freshwater on Earth. This moisture transport occurs under certain wind, temperature, and pressure conditions. Atmospheric rivers can lead to record-breaking rainfall, snowfall, and floods, which then cause	

	catastrophic mud and debris flows where wildfires may have created burn scar areas. Mud and debris flows can clog rivers and dams, disrupt travel, and cause damage to life and property, which also slows recovery efforts.	
Rising Oceans and Coastal Erosion	Rising water causes beaches to recede and makes structures (including coastal power plants and transmission lines) near them much more vulnerable to storm damage.	
Extreme Winds	Extreme winds of various types can damage utility equipment or disrupt regional or local utility operations.	SOTI— Extreme Natural Events
Earthquakes	Critical infrastructure in an earthquake-damaged area will be out of service for an extended period. A major earthquake (7.0 – 7.9) or greater will damage well-designed infrastructure. Oceanic earthquakes can generate tsunamis, causing extensive damage along the coastal regions where generation is located.	
Tsunamis	With the 600-mile Cascadia Subduction Zone—running from Vancouver Island, Canada, to northern California—and the threat of a major earthquake creating tsunamis bringing colossal waves, significant coastal damage and disruption to critical infrastructure, communities, homes, structures, and lives is possible.	
Volcanic Eruptions	Significant volcanic eruptions near critical infrastructure will render it inoperable, and terrain changes may make replacement take months to years.	

Inverter-Based Resources

Name	Description	Links to Resources & Related Documents
Performance and Validation Issues	Lack of studying the actual performance of inverter-based resources and validation not being performed by applicable entities can result in large-scale disturbances on the bulk power system with the potential to cause widespread outages.	SOTI— Resources
Inadequate Interconnection Requirements and Commissioning	Active interconnection and commissioning requirements set and enforced by applicable entities may not adequately provide clarity and consistency for inverter-based resources.	Inverter-Based Resource Disturbances in the Western Interconnection
Modeling Quality Issues	Model simulations do not adequately represent how inverter-based resources will respond during transients and fault studies, which causes a lack of confidence in planning studies and can lead to unforeseen actions in real-time operations, such as loss of generating resources or load shedding.	
Applicability of GO Registration and NERC Reliability Standards	As generating facilities using inverter-based resources may not follow some or any of NERC's applicable standards, the effects experienced by these devices will increase as the number of facilities grows.	SOTI— Resources
System Restoration	With the continued retirement of thermal plants and the increase of IBRs, system restoration will be more dependent on IBRs. Current guidelines and standards do not or may not fully address the integration of IBRs into restoration plans (as blackstart resources or as destination plants).	NERC and Regional Entity Staff Study - Availability and Readiness in the Eastern and Western Interconnections

Increasing Number of Long-Term Frequency Deviations	The Western Interconnection is experiencing an increase in the number of frequency deviation events in which the interconnection frequency gradually declines and is not corrected for several minutes (mostly noticeable during periods of large solar generation changes). As these events lower the interconnection frequency for several minutes, there is an increased risk of activating Underfrequency Load Shed relays if a large generator loss or credible double-contingency occurs at the same time.	
Forced Oscillations from Battery Energy Storage Systems	As more IBRs are added to the Western Interconnection, the industry is seeing them generate oscillations, some that resonate at or near the known natural modes of the system. If the system is stressed, a forced oscillation could cause instability of the grid. Forced oscillations can cause transmission facility overloads, generator instability, and other problems that could lead to facility damage, islanding, and other extreme reliability issues.	

Resource Adequacy

Name	Description	Links to Resources & Related Documents
Energy Policy	The implementation of policy decisions can significantly affect the reliability and resilience of the BPS. Decarbonization, decentralization, and electrification have been active policy areas. Implementing policies in these areas is accelerating, and, with changes in the resource mix, extreme weather events, and physical security and cybersecurity challenges, reliability implications are emerging.	Western Assessment

Resource Adequacy Forecast Planning	Existing approaches to resource adequacy may not account for a broader range of possibilities and may cause resource adequacy studies to lead to a misperception of the future. This misperception can include inadequate capacity requirements during peak times. This can lead to energy emergency alerts and ultimately the shedding of firm load.	Western Assessment SOTI– Load
Electrification: Electric Vehicle and Residential and Commercial Heating	Electric power is being driven to replace natural gas and fuel oil used for building heat and petroleum energy sources for transportation, mainly automotive and trucking, which will lead to a higher demand on both energy and capacity as well as the delivery infrastructure. Traditional forecasts of energy demands will be inadequate if advanced planning of production and delivery of electricity does not consider the large increase in demand in all seasons and, more significantly, in the winter months when heating loads increase.	Western Assessment

Infrastructure

Name	Description	Links to Resources & Related Documents
Supply Chain Constraints	The implementation of policy decisions can significantly affect the reliability and resilience of the BPS. Decarbonization, decentralization, and electrification have been active policy areas. Implementing policies in these areas is accelerating, and, with changes in the resource mix, extreme weather events, and physical security and cybersecurity challenges, reliability implications are emerging.	Western Assessment
Energy Adequacy Concerns/Energy Efficiency	The system is moving toward new types of generation, including rapidly growing inverter-based variable generation and energy-limited storage, with retirement of traditional synchronous resources. Changes to the	

	types and locations of resources and the loads they serve are altering the operational characteristics and dynamics for planning and operating the grid. Energy availability has become as important as capacity, if not more so, causing extensive reconsideration of system adequacy metrics. Further, many new resources are more sensitive to changing weather patterns, and increasing extreme weather events are affecting all resources and loads in various ways.	
Misconfiguration	Incorrect settings, design errors, and knowledge-based errors lead to misoperations that affect BPS reliability.	
Facility Rating—Ambient Temperature Effects on Transmission Capacity	Most utilities publish seasonal facility ratings to guide the use of the transmission system, but new regulations under FERC 881 require hourly evaluations of these ratings over a 240-hour window. Extreme weather forecasting errors could lead to energy shortages and differences between real-time and planning models, complicating the responsibilities of Transmission Owners. The rigorous computations needed may necessitate new personnel or technology and could further strain the processing of interconnection requests and Ambient Adjusted Ratings.	SOTI— Transmission
Facility Rating—Inconsistent Development and Application of Facility Ratings Methodologies	When facilities are jointly owned, each owner could establish its own methods for facility ratings, leading to a piece of equipment having different facility ratings depending on which owner is asked. Each owner may also establish different emergency ratings and durations, creating the need to coordinate the most limiting and next-most limiting element to establish a single rating for the facility. Otherwise, real-time operations can be affected, especially across tie lines.	Western Assessment

TO/TOP Registration Gaps with BES-Level Generation Tie-lines	BES-level transmission equipment (transformers, lines, switchyards) that serve as generation tie-lines are owned and operated without a NERC-registered TO/TOP are not compelled to comply with applicable NERC reliability standard requirements, which limits the authority and ability of interconnected NERC-registered entities to ensure reliable operations.	
Default Temperature Ratings	Some facilities have default temperature ratings instead of actual ratings for their location. Improper rating could cause the facilities to operate outside of plan if the ambient temperature exceeds the default.	

Other

Name	Description	Links to Resources & Related Documents
Planning Case Accuracy	As two types of organizations originate transmission projects (current Transmission Owners and Operators, and independent transmission developers), information about transmission projects originated by independent developers may not be submitted to WECC to be included in future studies. If the transmission planners are not informed about transmission projects in an appropriate time frame, they are not able to determine and coordinate any impacts these projects have on their transmission planning assessments and any impacts outside of the interconnecting entity.	
Congested Radio Spectrum	The radio frequency spectrum is one of the most critical and limited resources utilities use to operate and maintain a reliable power transmission system. Radio spectrum is used for various services that ensure reliable control, protection, restoration, generation, and marketing of electric power for the Bulk Electric System (BES). Most of these	

	services are carried out by utility-owned and operated high-capacity microwave radio networks. Radio spectrum is required to operate electric power systems; fiber optic networks cannot replace many radio systems and, in many situations, can't provide the reliability electric utilities need. Potential interference levels have been proven substantial in the field. This has two effects: the increased interference to existing utility networks decreases reliability for both protection and control, and will directly affect the regulatory compliance and operation of the BES. Additionally, the increased congestion prevents growth to meet demands for incorporating wind and solar generation, electric vehicle charging networks, and other increasing demands on the grid.	
--	---	--

Personnel

Name	Description	Links to Resources & Related Documents
Workforce Skillset Shortage	Entities in the West have a workforce that is close to retirement and they are finding it difficult to hire personnel with technical skillsets (entry level and expert) to replace open positions. This is symptomatic across the industry and can affect an organization's ability to design, construct, operate, and maintain the physical assets needed for reliability and prevent, detect, and respond to physical security and cybersecurity events.	
Future Pandemics	"In the future, it is predicted that pandemics will emerge more often, spread more rapidly, cause more damage to the global economy, and lead to greater global morbidity and mortality." –World Health Organization. This could lead to workforce unavailability or sudden shifts in load.	

Physical Security

Name	Description	Links to Resources & Related Documents
Substation Sabotage	Physical attacks on substations, primarily unattended, are increasing, leading to more damage to facilities. Although primarily financial loss, there is potential for increasing attack severity to stop operation of a substation for more than X (consider time or cascading as a potential threshold. i.e. 4+ hours is unacceptable).	SOTI— Security
Drones or Unmanned Aircraft	The use of drones has increased exponentially in North America. This is a problem because they can easily bypass traditional security perimeters for surveillance and negative publicity, cause injury to personnel, lead to attacks on infrastructure, or exploit cybersecurity vulnerabilities.	