

13TH ANNUAL LEADERSHIP EVENT



CYBER SECURITY SUMMIT

cybersecuritysummit.org

RESILIENCE UNLOCKED

TITLE SPONSOR



Island

#cybersecuritysummit #css13



Energy Sector Cybersecurity Partnerships

Collaboration Between State Government and Critical Infrastructure Augments the Ability to Fight Cyber-Attacks Protecting the Critical Nature of Services to Minnesotans



Steen Fjalstad

Director Of Security

Midwest Reliability Organization



Christopher Watkins

Energy Security Advisor

Minnesota Dept of Commerce



Eric Peterson
Cybersecurity

Manager
Allete, Inc.



CYBER SECURITY
SUMMIT
www.cybersecuritysummit.org

13th Annual Cyber Security Summit | October 24-26, 2023

in

#cybersecuritysummit #css13

RESILIENCE
UNLOCKED

Moderator:

Bill Leifheit

Business Information Security Officer
(BISO)

Minnesota IT Services

Partnering with Transportation,
Commerce and the Public Utilities
Commission (PUC)



CYBER SECURITY
SUMMIT
www.cybersecuritysummit.org

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE
UNLOCKED

Energy Sector Cybersecurity Partnerships Panel

Goals:

1. Explore how State Government and Critical Infrastructure Providers collaborate on cyber security to protect Minnesotans.
2. Leave with resources for further learning.

Questions are welcome!

Our opening question:

- What do you think the biggest risk to the power grid is from a security standpoint?





MRO 2023 Regional Risk Assessment

Top risks to the reliable and secure operation of the North American bulk power system in MRO's regional footprint.

Territory



About Us

As part of the [ERO Enterprise](#), MRO is committed to a shared mission to identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American bulk power system in its regional footprint.

Read more at www.MRO.net

MRO Reliability Risk Matrix: Risk Rankings

Consequence / Impact (C)	Likelihood (L)					
	L1	L2	L3	L4	L5	
	Very Unlikely	Unlikely	Possible	Likely	Almost Certain	
C5 Severe						
C4 Major				4,5,6,16		
C3 Moderate		2	9,12,13	1		
C2 Minor			3,7,8,10,14,17	15		
C1 Negligible			11			

Top risks are reflected in orange above and described below. A full list of risks assessed can be found in the final report.

Assessment Overview

- Extreme weather, consumer demand, and changes in technology and generation resources continue to present a rapidly increasing number of challenges to grid planners and operators. Physical and cyber security risks also continue to evolve at an unprecedented pace.
- MRO's annual *Regional Risk Assessment* considers continent-wide risks to reliability and security of the North American bulk power system and determines which are more likely to occur and would have a higher impact in MRO's region.
- This report is focused on risk identification, prioritization and mitigation and highlights for industry the priorities needed to collaboratively address these challenges. It also serves to inform key decision makers of challenges the industry faces and the policies and regulations that will help define a variety of proposed solutions.

[READ MRO'S 2023 REGIONAL RISK ASSESSMENT](#)

Key Findings: Top Reliability and Security Risks in MRO's Territory

Model Assumptions	Planning Reserves	Energy Reliability	Generation Unavailability	Transmission Line Ratings	Insider Threats	Malware/Ransomware	Supply Chain Compromise
<p>RISK 1. Assumptions used in bulk power models to plan and operate the grid have not accounted for the rapid increase in inverter-based and distributed energy resources, challenging industry's ability to accurately assess current and future system characteristics.</p>	<p>RISK 4. Traditional methods to calculate Planning Reserve Margin are inadequate to properly plan for the generation capacity needed to meet increasingly uncertain system operations, especially during extreme weather events.</p>	<p>RISK 5. Increased uncertainty from changing energy supply and customer demand challenge the grid's ability to meet load for all hours of the year. There is no comprehensive planning that assesses assurance of available energy and fuel sources over all time periods to maintain grid reliability.</p>	<p>RISK 6. Generation unavailability assumed during cold weather, particularly in the southern U.S., has been shown to be unrealistically high due to a lack of generation winterization and natural gas curtailments.</p>	<p>RISK 12. Use of constant overhead transmission line ratings year-round (non-seasonal) limits available transmission capacity and leads to inefficient real-time decisions when system conditions deviate from assumptions that drive rating calculations, such as cooler temperatures or during emergency operations.</p>	<p>RISK 9. Employees or contractors using their knowledge and authorized access of critical systems to do harm to the bulk power system is a continued, substantial threat to organizations and the reliability of the grid.</p>	<p>RISK 13. Phishing attacks can introduce malware or ransomware to corporate IT systems, which can impact critical systems necessary for reliable bulk power system operations through direct or in-direct connections those systems have to IT networks.</p>	<p>RISK 16. A cyber security event carried out through the vendor supply chain can broadly impact bulk power system reliability, especially where the vendor is a market leader providing systems used for system operation.</p>



CYBER SECURITY
SUMMIT
www.cybersecuritysummit.org

13th Annual Cyber Security Summit | October 24-26, 2023

in f

#cybersecuritysummit #css13

RESILIENCE
UNLOCKED



15 April 2022



CYBER SECURITY
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

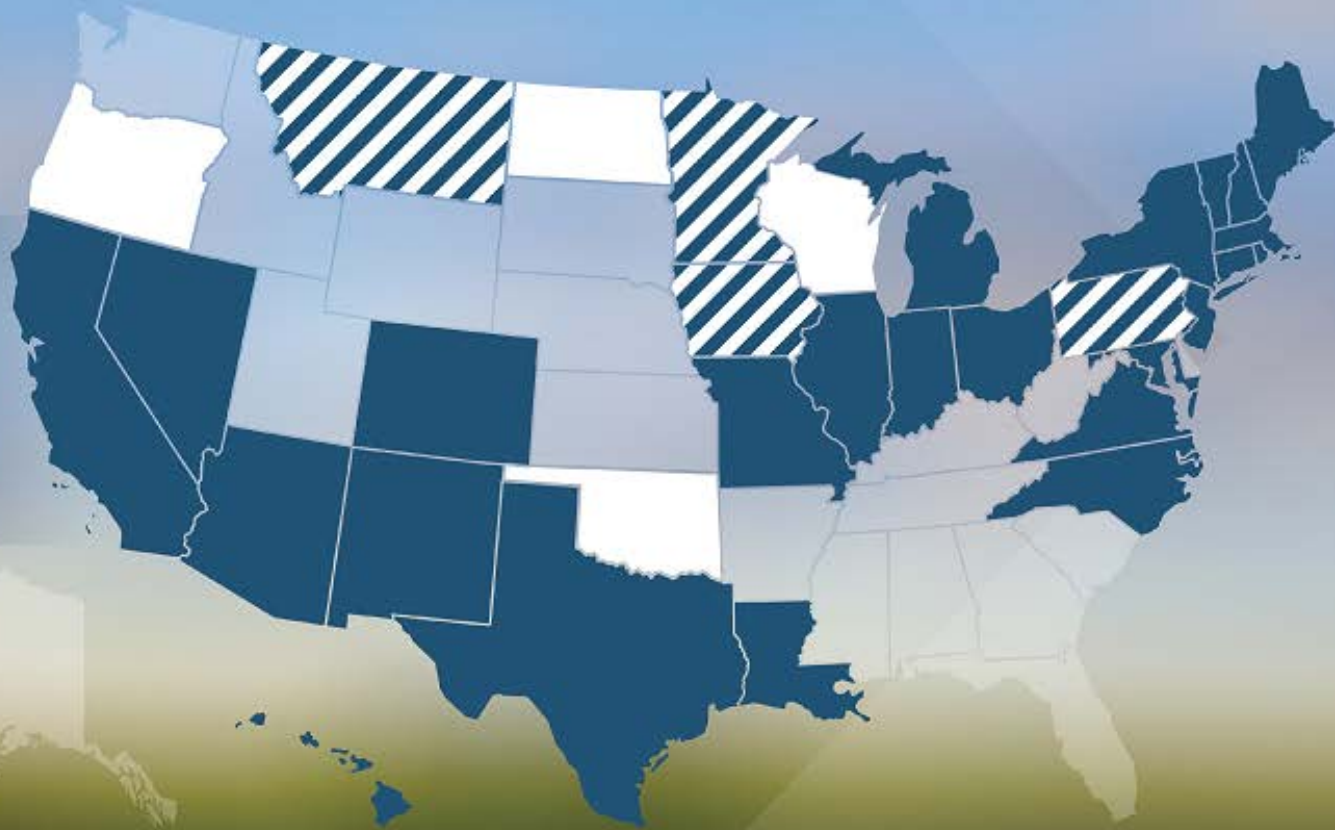
RESILIENCE
UNLOCKED





TOGETHER, we will
have a presence in
30 STATES

- ALLETE
- NEE
- ALLETE & NEE



CYBER SECURITY
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023



#cybersecuritysummit #css13

RESILIENCE
UNLOCKED

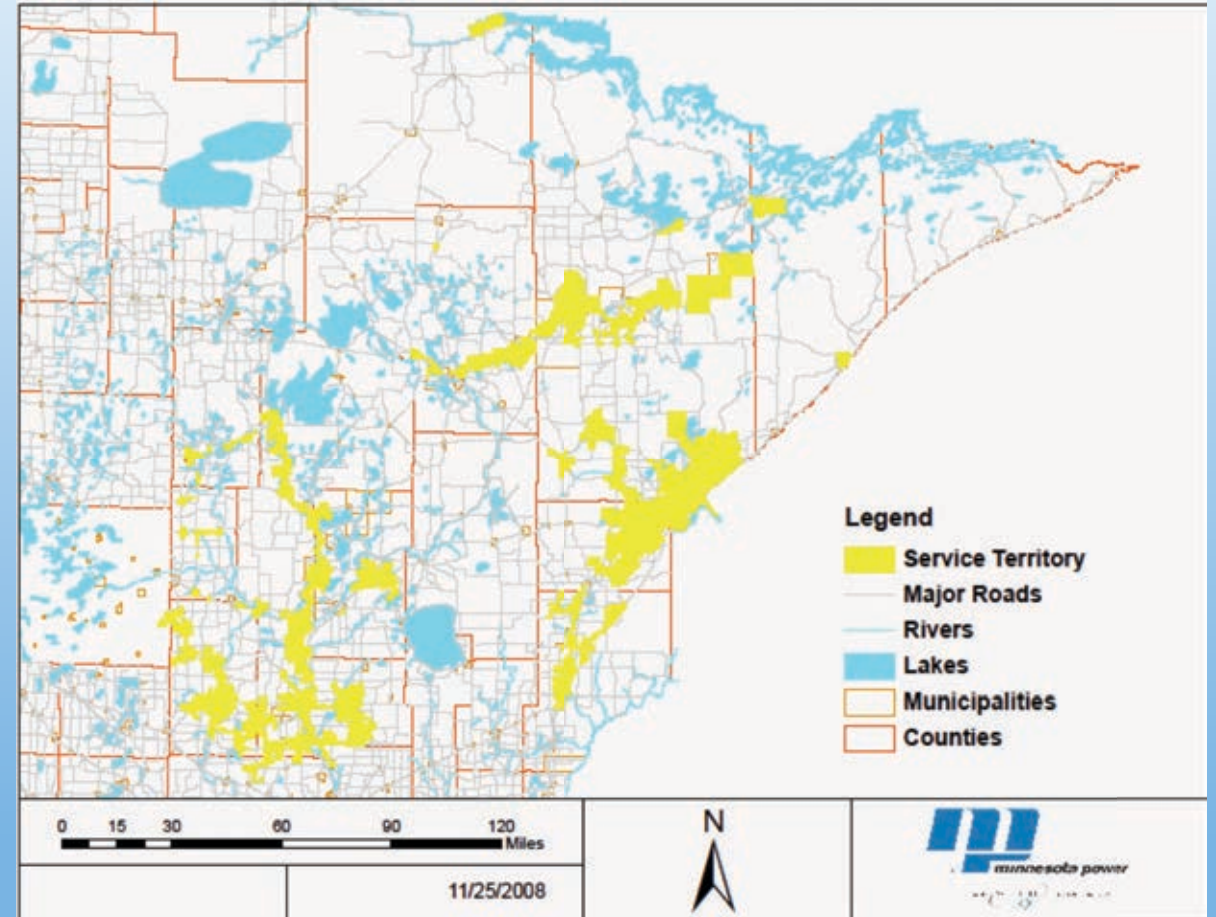
Minnesota Power

First incorporated in 1906

Service territory: We provide electricity in a 26,000-square-mile service area in northeastern Minnesota.

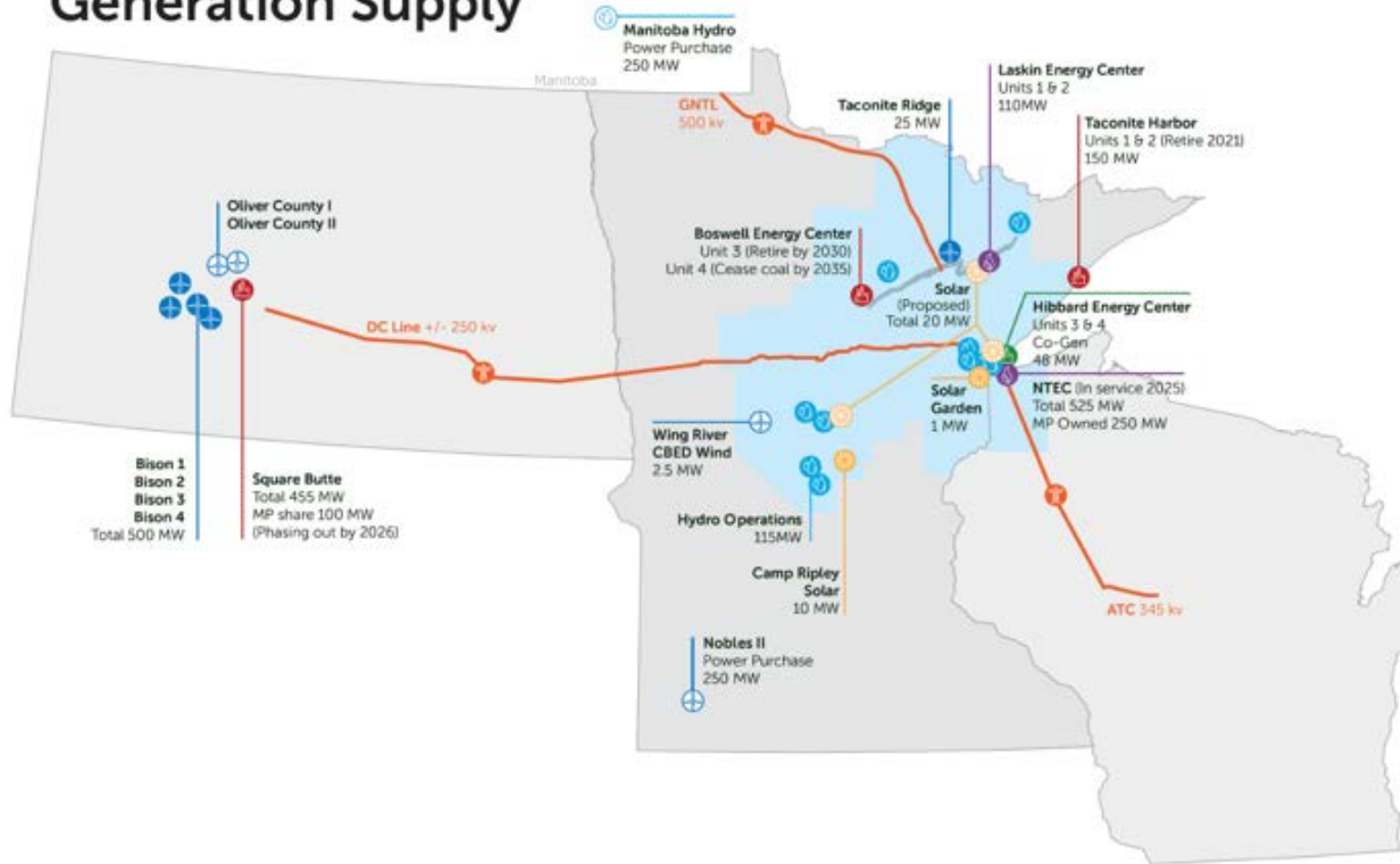
Employees: About 1200

Customers: We serve about 145,000 residential and commercial customers, 15 municipalities and some of the nation's largest industrial customers.



Minnesota Power Generation

Generation Supply



Office of Reliability and Security: Development Background

- Evolving threats to reliability and security of electric power and natural gas systems, including issues related to:
 - regional capacity shortfalls
 - extreme weather events
 - regional system interdependencies
 - cyber and physical security issues
 - other known/existing hazards
- Multiple functions within the Department that address reliability and security issues, including but not limited to:
 - Energy assurance and state energy security planning
 - Representation of Minnesota's interests at the regional and federal level
 - Emergency response pursuant to Executive Order 19-22
 - Cyber security for critical infrastructure pursuant to Executive Order 20-22
- Gaps in coordination created a potential vulnerability in serving the public's interest.

Dedicated coordination of reliability and security issues has allowed the Department to:

- Effectively respond to growing concerns and inquiries about root causes for energy reliability or security issues.
- Identify gaps and solutions where needed to ensure all reasonable measures toward a reliable and secure system are used.
- Deploy new and available tools to address issues associated with energy reliability and security.



Office of Energy Reliability and Security: Operational Objectives

Elevate

- Escalates reliability and security issues for consideration by department leadership, executive leadership, legislative committees, energy regulators, critical infrastructure providers, and other relevant stakeholders.

Coordinate

- Leads inter and intra-agency teams to ensure the Department of Commerce fulfills its planning, preparedness, and response capabilities for energy reliability and security issues.

Align

- Ensure alignment of various planning, programmatic, regulatory, and response activities to foster efficient use of limited resources to address reliability and security concerns.

Support

- Provide guidance and support to staff to develop and implement plans that are consistent across the Division business units, other state agencies, regional and national organizations, and others.



Resources and Links



- [Minnesota Fusion Center](#)
- [Multi-State Information Sharing and Analysis Center \(MS-ISAC\)](#)
- [Electricity Information Sharing and Analysis Center \(E-ISAC\)](#)
- [MRO 2023 Regional Risk Assessment](#)
- [MNIT Whole-of-State Cybersecurity Plan](#)
- [State and Local Cybersecurity Grant Program \(SLCGP\)](#)
- [Oil and Natural Gas ISAC \(ONG-ISAC\)](#)
- [Water ISAC](#)



Thank You!



CYBER SECURITY
www.cybersecuritysummit.org **SUMMIT**

13th Annual Cyber Security Summit | October 24-26, 2023

in    

#cybersecuritysummit #css13

