414 Nicollet Mall
Minneapolis, MN 55401

November 12, 2024

—Via Electronic Filing—

Will Seuffert
Executive Secretary
Minnesota Public Utilities Commission
121 7th Place East, Suite 350
St. Paul, MN 55101

RE: SUPPLEMENTAL COMMENTS
IN THE MATTER OF A COMMISSION INVESTIGATION ON GRID AND CUSTOMER SECURITY ISSUES RELATED TO PUBLIC DISPLAY OR ACCESS TO ELECTRIC DISTRIBUTION GRID DATA
DOCKET NO. E999/CI-20-800

Dear Mr. Seuffert:

Northern States Power Company, doing business as Xcel Energy, submits the enclosed Supplemental Comments in response to the Minnesota Public Utilities Commission's October 9, 2024 Notice of Supplemental Comment Period.

We have electronically filed this document with the Minnesota Public Utilities Commission, and copies have been served on the parties on the attached service list. Please contact Nathan Kostiuk at nathan.c.kostiuk@xcelenergy.com or me at brian.t.monson@xcelenergy.com if you have any questions regarding this filing.
Sincerely,

/s/

BRIAN T. MONSON
MANAGER, DISTRIBUTION REGULATORY STRATEGY

Enclosure
cc: Service List

STATE OF MINNESOTA
BEFORE THE
MINNESOTA PUBLIC UTILITIES COMMISSION

Katie J. Sieben	Chair
Hwikwon Ham	Commissioner
Valerie Means	Commissioner
Joseph K. Sullivan	Commissioner
John A. Tuma	Commissioner

IN THE MATTER OF A COMMISSION INVESTIGATION ON GRID AND CUSTOMER SECURITY ISSUES RELATED TO PUBLIC DISPLAY OR ACCESS TO ELECTRIC DISTRIBUTION GRID DATA	DOCKET NO. E999/CI-20-800 **SUPPLEMENTAL COMMENTS**

INTRODUCTION

Northern States Power Company, doing business as Xcel Energy, submits these Supplemental Comments in response to the Minnesota Public Utilities Commission's October 9, 2024 Notice of Supplemental Comment Period in the instant docket.

First, we provide a brief background on Docket No. E999/CI-20-800, highlighting the establishment of the Grid Security Workgroup by the Commission to address the increasing threats to critical infrastructure. The workgroup, which the Company participated in and includes representatives from other Minnesota utilities, state and federal agencies, and security experts – as well as two developers – convened for three meetings in 2024. The workgroup agreed that there are significant security risks to the electric grid from foreign and domestic bad actors, and that the NARUC Grid Data Sharing Playbook (NARUC Playbook) is a valuable tool for guiding data sharing discussions, balancing state goals pertaining to the clean energy transition with security.

Second, we address the three topics open for comment. In this, we include a potential roadmap for utilizing the NARUC Playbook and articulate concerns associated with the potential for grid data to be used inappropriately or, in the case of foreign or domestic adversaries, nefariously.

SUPPLEMENTAL COMMENTS

I. BACKGROUND

The history of the 20-800 docket is rooted in the ongoing need to address grid and customer security issues related to public display or access to electric distribution grid data. Recognizing the heightened geopolitical risks and increased domestic threats to critical infrastructure – and the paucity of expertise in the record from security experts at the time other than from Xcel Energy – in their June 7, 2023 Order in this docket, the Commission established a Grid Security Workgroup to develop the record more fully.

Participants in the Workgroup sessions that occurred on July 26, 2024; August 2, 2024; and September 20, 2024, agreed that the threat landscape remains serious, and that foreign actors and Domestic Violent Extremists (DVEs) pose significant risks. Nation-states such as China, Russia, and Iran continue to target U.S. critical infrastructure through cyber operations. For instance, the Office of the Director of National Intelligence (ODNI) considers China the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks.[1] Similarly, Russia and Iran also pose significant threats through their cyber capabilities and willingness to conduct aggressive operations against U.S. infrastructure.[2,3] The workgroup, comprising representatives from various utilities, state and federal agencies, and security experts, as well as two developers, agreed that the NARUC Playbook would be a useful tool for facilitating discussions on data sharing. During the workgroup meetings, participants, including representatives from the FBI, emphasized the necessity of revisiting access permissions regularly and maintaining robust security protocols.

Foreign adversaries are not the only threat to critical infrastructure, which includes our distribution grid. DVEs and criminal actors are increasingly calling for and carrying out physical attacks against critical infrastructure, particularly in the energy sector. DVEs see such attacks as a means to advance their ideologies and achieve their sociopolitical goals. DVEs, particularly Racially Motivated Violent Extremists (RMVEs) promoting accelerationism – an ideology that seeks to destabilize society and trigger a race war – have encouraged mobilization against lifeline and other critical

[1] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf
[2] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf
[3] https://home.treasury.gov/news/press-releases/jy2292

functions, including attacks against the energy, communications, and public health sectors.[4]

There have been multiple incidents of people with these ideologies and goals planning and – in some cases – executing attacks. In 2023, two men were sentenced in federal court for conspiring to attack power grids throughout the United States to promote white supremacy ideology.[5] In 2022, an individual conspired to carry out attacks against critical infrastructure, specifically electrical substations, in furtherance of racially or ethnically motivated violent extremist beliefs. The individual posted links to open-source maps of infrastructure, which included the locations of electrical substations, and described how a small number of attacks on substations could cause a "cascading failure." The individual also discussed maximizing the impact of the planned attack by hitting multiple substations at one time.[6] Additionally, just on November 2, 2024, the FBI arrested a man after he allegedly tried to attack Nashville's power grid by arming a drone with explosives and firing it into an energy facility to "further his violent white supremacist ideology."[7]

Given these very real, ongoing threats to the security of the electric grid, and thus, the safety of our customers, workgroup participants agreed that the data points in question needed to be carefully evaluated, and that the NARUC Playbook is an excellent tool to guide discussions on what data can and should be shared and how it should be shared and protected. This playbook lays out best practices and methodologies for data sharing while emphasizing the need to balance transparency with the security of critical infrastructure. By utilizing the NARUC Playbook, the workgroup believes we can develop a robust framework that not only facilitates the sharing of the minimum necessary data, but also ensures that such sharing is done with the highest security standards in mind.

The Grid Security Workgroup also reached a consensus to request that the Commission establish a permanent Grid Security Workgroup with specific guiding goals. These decisions will be discussed in the hearing scheduled for January 16, 2025, in Docket No. 20-800. The Company looks forward to participating in these conversations and finding a solution that balances support for Distributed Energy

---

[4] https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf

[5] https://www.justice.gov/usao-sdoh/pr/2-men-sentenced-prison-domestic-terrorist-plans-attack-power-grids

[6] https://www.justice.gov/usao-md/pr/maryland-woman-and-florida-man-face-federal-charges-conspiring-destroy-energy-facilities

[7] https://www.capitaliq.spglobal.com/apisv3/spg-webplatform-core/news/article?id=86114337&KeyProductLinkType=58&utm_source=MIAlerts&utm_medium=realtime-minewsresearch-newsnonfeature-electric%20utilities&utm_campaign=Alert_Email

Resources (DER) with maintaining the safety and reliability of the grid for our customers.

II. COMMENTS ON WORKGROUP RECOMMENDATIONS

From the workshop, the parties requested Commission guidance on several key items. They recommended that the Commission affirm that the minimum necessary data should be shared and that it should be shared securely. This recommendation underscores the importance of limiting data sharing to only what is essential, thereby minimizing potential security risks.

Additionally, the parties recommended authorizing the workgroup to determine the security methods to be employed via the NARUC Grid Data Sharing Framework. By leveraging this framework, the workgroup can ensure that the most effective and up-to-date security measures are implemented, providing a robust defense against potential threats.

The parties also recommended that the Commission approve the use of the NARUC Grid Data Sharing Framework in working through data sharing disagreements. This framework provides a structured approach to resolving conflicts, ensuring that all parties have a clear understanding of their roles and responsibilities. Furthermore, the parties suggested affirming the continuation of a standing workgroup that can be called by parties or the Commission to review future data sharing disagreements, similar to the Distributed Generation Workgroup (DGWG). This workgroup would provide a reliable forum for addressing ongoing data sharing issues.

Another important recommendation was the request for clarity from the Commission that federal requirements should be included in discussions, not just state requirements and priorities. This inclusion ensures that all relevant regulations and guidelines are considered, providing a comprehensive approach to data sharing and security.

While we agree with the majority of the workgroup's recommendations, we would like to provide additional comments and clarifications on certain aspects. One area of agreement is the recognition of the significant security risks posed by foreign and domestic bad actors. The workgroup has highlighted the threats from nation-states such as China, Russia, and Iran, as well as DVEs who target critical infrastructure to advance their ideologies. We concur with the workgroup's assessment and emphasize the need for robust security measures to mitigate these risks.

However, we also believe that the Commission's authority regarding data security

needs to be clearly defined. Currently, the Commission lacks the regulatory oversight to mandate that parties receiving data keep data secure. This limitation underscores the need for a more structured approach to data protection. To address this gap, we request that the Commission direct the workgroup to determine the necessary security measures for the data. These measures would serve as a baseline to ensure that all parties handling sensitive grid information adhere to a consistent level of security, thereby safeguarding critical infrastructure from potential threats.

Furthermore, we suggest that utilities should have the discretion to withhold data from parties that do not meet these established security standards. While this approach places additional responsibility on utilities to manage data access, it is a necessary measure to ensure that only qualified and secure entities can access sensitive grid information. By implementing these standards, we can create a more secure and resilient grid infrastructure, protecting both the utilities and the customers they serve.

In conclusion, we support the workgroup's recommendations and believe that they provide a solid foundation for enhancing grid security and data sharing practices. By establishing minimum security standards and creating a permanent workgroup, we can ensure that the necessary steps are being taken to protect sensitive grid information from potential threats. We look forward to participating in the ongoing discussions and finding a solution that balances support for DER with maintaining the safety and reliability of the grid for our customers.

III. UTILIZATION OF THE NARUC PLAYBOOK

The NARUC Playbook, submitted into the record on October 9th, 2024, is a comprehensive approach designed to address the complexities of data sharing and security within the energy sector. This framework is built upon the principles outlined in the NARUC Playbook, which provides valuable insights and guidelines for effective data sharing while balancing transparency with the security of critical infrastructure.

One of the key benefits of the NARUC Playbook collaborative framework is its iterative nature. This allows for continuous improvement and adaptation to the evolving security landscape. By regularly revisiting and updating the framework, stakeholders can ensure that it remains relevant and effective in addressing current and emerging threats. Additionally, the framework's flexibility makes it applicable to various data sharing use cases, accommodating the unique needs and circumstances of different stakeholders.

The framework emphasizes the importance of setting policy-based goals. This

involves establishing clear objectives that align with broader policy priorities, such as enhancing grid reliability, promoting innovation, and protecting consumer privacy. By aligning data sharing initiatives with these goals, the framework ensures that they contribute to overarching policy objectives.

Another critical aspect of the framework is the definition of party positions. By clearly outlining the roles and responsibilities of different stakeholders, the framework helps to ensure that everyone involved understands their obligations and can work together more effectively. This clarity fosters collaboration and minimizes conflicts, making it easier to achieve common goals.

The use of concrete examples, or use cases, is another strength of the framework. These use cases provide practical illustrations of how data sharing can be implemented, highlighting potential benefits and challenges. By evaluating use cases based on policy priorities, best practices, and potential impacts, the framework ensures that data sharing initiatives are grounded in real-world scenarios and designed to achieve tangible outcomes.

Finally, the framework underscores the need to assess data sharing tactics after establishing minimum security needs. This step is crucial for ensuring that data sharing practices are both effective and secure. By identifying and implementing appropriate security measures, the framework helps to protect sensitive information and mitigate potential risks.

The workgroup has already begun using the NARUC Playbook collaborative framework to guide its discussions and evaluations. This proactive approach has allowed the workgroup to make progress in addressing data sharing and security issues. Below, we provide a potential roadmap for using the NARUC Playbook to continue evaluating the question of sharing grid data. This roadmap includes steps such as identifying key stakeholders, defining data sharing objectives, developing use cases, and implementing security measures. By following this roadmap, the workgroup can ensure that data sharing initiatives are both effective and secure, ultimately enhancing the reliability and security of the grid.

In light of these benefits, we strongly support the request for the NARUC Playbook collaborative framework to be used by a standing workgroup to consider data sharing and security issues. The framework's iterative, flexible, and non-prescriptive nature, combined with the valuable insights from the NARUC Playbook, makes it a powerful tool for achieving policy-based goals, defining party positions, leveraging use cases, and assessing data sharing tactics.

A. Proposed Roadmap for Evaluating Grid Data Using the NARUC Playbook

Table 1 provides a potential roadmap for evaluating and implementing data sharing practices, using the NARUC Playbook. In the table, we also indicate any progress that has been made towards each step in the workgroup thus far.

Table 1
Roadmap for Evaluating and Implementing Data Sharing Practices

Step	Description	Details	Completeness
1. Determine the Desired Outcome	Define the desired outcomes of sharing distribution grid data.	- State Priorities: Consider state regulatory requirements, policy objectives, and public interest goals. - Utility Priorities: Identify the benefits and challenges for utility companies, including operational improvements, customer service enhancements, and compliance requirements. - Developer Priorities: Assess the needs and expectations of developers who rely on grid data for planning and developing energy projects.	Complete
2. Determine the Appropriate Use Cases for the Data	Identify specific use cases for the shared data.	- Short description of the scenario for which grid data sharing is relevant. - Use case format: "As (persona), I want (what), so that (why)." - Determine if the use case is appropriate and valid. - Determine the minimum necessary amount of data.	In Progress
3. Determine Potential Impacts of Sharing Data	Evaluate the potential impacts of sharing the minimum necessary data.	- Operational Security: Risks to grid security and integrity. - Data Privacy: Protection of customer information and compliance with privacy regulations. Data privacy issues need to be resolved before data can be shared. - Market Dynamics: Effects on competition, market efficiency,	Not Started

Step	Description	Details	Completeness
		and innovation. - Cost-Benefit Analysis: Weighing the costs of data sharing infrastructure against the anticipated benefits.	
4. Determine Appropriate Security Measures/Protections for Data	Implement robust security measures to protect the data being shared.	- Data Encryption: Ensuring that data is encrypted both in transit and at rest. - Access Controls: Defining access levels and ensuring that only authorized parties can access sensitive information. - Monitoring and Audit: Continuously monitoring data access and usage, and conducting regular audits to detect and address any security breaches. - Compliance: Adhering to relevant regulations and standards for data security and privacy. - Enforcement Responsibility: Identifying who is responsible for enforcing compliance with security measures.	Not Started
5. Reevaluate Current Data Sharing Practices	Examine and reassess the current data sharing practices to identify any gaps or areas for improvement.	- Reviewing Existing Protocols: Analyzing existing data sharing agreements, protocols, and practices. - Benchmarking: Comparing current practices with industry standards and best practices. - Stakeholder Feedback: Gathering feedback from stakeholders to understand their experiences and concerns with current practices.	Not Started
6. Determine Data Sharing Tactics	Establish concrete tactics for data sharing, ensuring alignment with the outcomes and use cases identified.	- Collaboration: Engaging stakeholders in the development and implementation of data sharing strategies. - Standardization: Developing and adopting standardized data formats, protocols, and interfaces to facilitate seamless	Not Started

Step	Description	Details	Completeness
		data exchange. - Transparency: Maintaining transparency in data sharing processes, including clear communication about what data is being shared and how it will be used. - Continuous Improvement: Regularly reviewing and updating data sharing practices to adapt to evolving needs and technologies.	

We note that privacy is an integral part of the NARUC Playbook process.[8] Per the Playbook, the workgroup needs to be cognizant of not jeopardizing the privacy expectations of utility customers when evaluating the sharing of grid data.[9] However, per the Commission's October 30, 2020, notice in this proceeding:

> *This docket focuses on electric distribution grid and customer security. Changes to customer privacy policies are not in scope. Privacy and data access issues are addressed in Docket Nos. E,G999/M-19-505 and E,G999/CI-12-1344.*

Accordingly, it is our understanding that any criteria for sharing of data in the Grid Security Workgroup need to align with current customer privacy policies. So far, this question has not been addressed by the Grid Security Workgroup. We recommend that privacy be included in the scope of the workgroup, within the context of the NARUC Playbook, to ensure that none of the potentially shared data violates privacy rules and policies. Once the workgroup works though security issues and concerns, we would evaluate the data through a privacy lens to ensure that none of the data violates the privacy of our customers per established rules.[10]

IV. INFORMATION FROM SECURITY EXPERTS AND NEW PARTIES

In the realm of grid data security, it is paramount to emphasize the importance of adopting a zero-trust model for handling data. In the workgroup, security experts, including those from the FBI and the Cybersecurity and Infrastructure Security

[8] Privacy is included in consideration of existing precedents or requirements, potential impacts of sharing data, and applicability of industry standards and data requirements as they pertain to data sharing tactics.
[9] National Association of Regulatory Utility Commissioners (NARUC), NARUC Grid Data Sharing Playbook (Washington, D.C.: NARUC, 2023), pages 15 – 17, 20 – 22.
[10] Docket No. 19-505.

Agency (CISA), stated that this model is the standard for ensuring data security. This model is built on the principle that access to grid data should be meticulously controlled and monitored. Specifically, anyone seeking access to this sensitive information must first prove their identity and demonstrate a legitimate need for the data. Furthermore, access should be granted on a view-only basis, ensuring that individuals can see the data but cannot download or manipulate it in any way.

During the workgroup, security experts, including those from the FBI and CISA, expressed significant concerns about the current state of data security. These concerns are more pronounced than what has been previously discussed in written filings in this docket. The FBI, in particular, has recommended against sharing grid data on the public internet, highlighting the potential risks and vulnerabilities associated with such practices. Given these expert opinions, it is crucial to reconsider our current data sharing practices and work towards identifying and implementing best practices that ensure the necessary level of security.

The recent Workgroup Report and the notes from Workshops 1 and 2 underscore these points. During the workgroup meetings, various parties, including representatives from the FBI, emphasized the necessity of revisiting access permissions regularly to ensure that only those with a current and legitimate need can access the data. They also highlighted the importance of maintaining robust security protocols and continuously educating those with access to data on how to safeguard it effectively.

In light of these discussions, it is clear that a zero-trust model is not just a theoretical ideal but a practical necessity. By implementing stringent access controls and continuously evaluating and updating our data sharing practices, we can better protect our grid infrastructure from potential threats and ensure that sensitive information remains secure.

A. Spreadsheet Updates

On October 8, 2024, we filed an update to the spreadsheet we filed on September 19, 2024. The updated version includes further clarifications and additional responses from developers and utilities who participated in the workgroup thus far. However, we have significant concerns regarding the potential public sharing of all data points within the spreadsheet, and we urge caution in handling these data points and emphasize the importance of maintaining confidentiality where necessary.
The risk of making this information public is twofold. Firstly, there is the concern about the ability of data recipients to protect the data. Secondly, if the data is available, a developer could use it to create a clearline map of our system, and a bad

actor or foreign adversary could do the same. This introduces significant security risks that cannot be overlooked.

We have already experienced an incident where a clearline map of a portion of our system was made, utilizing the hosting capacity data we share publicly. This information was shared with us by a third party who received the clearline map from a developer. This is an inappropriate use of our data that goes beyond its intended purpose and creates risks for our customers and our system. Such misuse of data underscores the need for stringent data access controls and the importance of anonymizing sensitive information before sharing it.

In light of these concerns, we recommend utilizing the NARUC playbook and the roadmap we outlined in Section II.A. By creating a thoughtful and thorough system of access using the guiding principles of the NARUC Playbook, we can better protect our grid infrastructure from potential threats and ensure that sensitive information remains secure.

CONCLUSION

In conclusion, we would like to extend our heartfelt gratitude to the Department of Commerce Office of Energy Reliability and Security, Commission Staff, the FBI, and all the other participants in the workgroup for their invaluable contributions and dedication to this important topic. The collective efforts have been instrumental in building a more robust record in this docket. The insights and recommendations provided by each participant have significantly enriched the discussions and have laid a strong foundation for future actions.

We respectfully ask the Commission to:

- Establish the Grid Security Working Group.
- Approve the use of the NARUC Playbook for evaluating grid data sharing.
- Direct the workgroup to determine the necessary security measures for the data.
- Grant utilities the discretion to withhold data from parties that do not meet these established security standards.
- Include privacy in the scope of the workgroup, within the context of the NARUC Playbook.

We look forward to continuing this collaborative effort to ensure the safety, reliability, and security of our grid infrastructure for the benefit of our customers and other stakeholders.

Dated: November 12, 2024

Northern States Power Company

CERTIFICATE OF SERVICE

I, Christine Schwartz, hereby certify that I have this day served copies of the foregoing document on the attached list of persons.

xx by depositing a true and correct copy thereof, properly enveloped with postage paid in the United States mail at Minneapolis, Minnesota

xx electronic filing

DOCKET NO. E999/CI-20-800

Dated this 12th day of November 2024

/s/

Christine Schwartz
Regulatory Administrator

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Ross	Abbey	ross.abbey@us-solar.com	United States Solar Corp.	100 North 6th St Ste 222C Minneapolis, MN 55403	Electronic Service	No	OFF_SL_20-800_Official
Roxanne	Achman	rachman@co.benton.mn.us		531 Dewey Street Foley, MN 56329	Electronic Service	No	OFF_SL_20-800_Official
Chad	Adams	ChadA@swmhp.org	Southwest Minnesota Housing Partnership	2401 Broadway Ave Slayton, MN 56172	Electronic Service	No	OFF_SL_20-800_Official
Michael	Ahern	ahern.michael@dorsey.com	Dorsey & Whitney, LLP	50 S 6th St Ste 1500 Minneapolis, MN 55402-1498	Electronic Service	No	OFF_SL_20-800_Official
Michael	Allen	michael.allen@allenergysolar.com	All Energy Solar	721 W 26th st Suite 211 Minneapolis, MN 55405	Electronic Service	No	OFF_SL_20-800_Official
Kristine	Anderson	kanderson@greatermngas.com	Greater Minnesota Gas, Inc.& Greater MN Transmission, LLC	1900 Cardinal Lane PO Box 798 Faribault, MN 55021	Electronic Service	No	OFF_SL_20-800_Official
Sarah	Anderson	sa@bomampls.org	Greater Minneapolis BOMA	Suite 610 121 South 8th Street Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Arnie	Anderson	ArnieAnderson@MinnCAP.org	Minnesota Community Action Partnership	MCIT Building 100 Empire Drive, Suite 202 St. Paul, MN 55103	Electronic Service	No	OFF_SL_20-800_Official
Martin S.	BeVier	bevi0022@umn.edu		4001 Grand Ave South # 3 Minneapolis, MN 55409	Electronic Service	No	OFF_SL_20-800_Official
Nichol	Beckstrand	Nichol.beckstrand@mmha.com	Minnesota Multi Housing Association	1600 W 82nd St Ste 110 Minneapolis, MN 55431	Electronic Service	No	OFF_SL_20-800_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
James J.	Bertrand	james.bertrand@stinson.com	STINSON LLP	50 S 6th St Ste 2600 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Jon	Braman	jbraman@brightpower.com	Bright Power, Inc.	11 Hanover Square, 21st floor New York, NY 10005	Electronic Service	No	OFF_SL_20-800_Official
Sheri	Brezinka	sbrezinka@usgbc.org	USGBC-Minnesota Chapter	701 Washington Ave. N Suite 200 Minneapolis, MN 55401	Electronic Service	No	OFF_SL_20-800_Official
James	Canaday	james.canaday@ag.state.mn.us	Office of the Attorney General-RUD	Suite 1400 445 Minnesota St. St. Paul, MN 55101	Electronic Service	No	OFF_SL_20-800_Official
Richard	Carter	rick.carter@lhbcorp.com	LHB	2780 Shadywood Rd Excelsior, MN 55331-9599	Electronic Service	No	OFF_SL_20-800_Official
Brent	Christensen	brentc@mnta.org	Minnesota Telecom Alliance	1000 Westgate Drive, Ste 252 St. Paul, MN 55114	Electronic Service	No	OFF_SL_20-800_Official
Andrew	Clearwater	N/A	Future of Privacy Forum	1400 I St NW Ste 450 Washington, DC 20005-6503	Paper Service	No	OFF_SL_20-800_Official
John	Coffman	john@johncoffman.net	AARP	871 Tuxedo Blvd. St, Louis, MO 63119-2044	Electronic Service	No	OFF_SL_20-800_Official
Roger	Colton	roger@fsconline.com	Fisher, Sheehan and Colton	34 Warwick Road Belmont, MA 02478	Electronic Service	No	OFF_SL_20-800_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Sheri	Comer	Sheri.comer@ftr.com	Frontier Communications Corporation	1500 MacCorkle Ave SE Charleston, WV 25396	Electronic Service	No	OFF_SL_20-800_Official
Generic Notice	Commerce Attorneys	commerce.attorneys@ag.state.mn.us	Office of the Attorney General-DOC	445 Minnesota Street Suite 1400 St. Paul, MN 55101	Electronic Service	Yes	OFF_SL_20-800_Official
George	Crocker	gwillc@nawo.org	North American Water Office	5093 Keats Avenue Lake Elmo, MN 55042	Electronic Service	No	OFF_SL_20-800_Official
Stacy	Dahl	sdahl@minnkota.com	Minnkota Power Cooperative, Inc.	5301 32nd Ave S Grand Forks, ND 58201	Electronic Service	No	OFF_SL_20-800_Official
Steve	Downer	sdowner@mmua.org	MMUA	3025 Harbor Ln N Ste 400 Plymouth, MN 55447-5142	Electronic Service	No	OFF_SL_20-800_Official
John	Farrell	jfarrell@ilsr.org	Institute for Local Self-Reliance	2720 E. 22nd St Institute for Local Self-Reliance Minneapolis, MN 55406	Electronic Service	No	OFF_SL_20-800_Official
Trent	Fellers	Trent.Fellers@windstream.com	Windstream	1440 M St Lincoln, NE 68508	Electronic Service	No	OFF_SL_20-800_Official
Sharon	Ferguson	sharon.ferguson@state.mn.us	Department of Commerce	85 7th Place E Ste 280 Saint Paul, MN 55101-2198	Electronic Service	No	OFF_SL_20-800_Official
Edward	Garvey	edward.garvey@AESLconsulting.com	AESL Consulting	32 Lawton St Saint Paul, MN 55102-2617	Electronic Service	No	OFF_SL_20-800_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Jenny	Glumack	jenny@mrea.org	Minnesota Rural Electric Association	11640 73rd Ave N Maple Grove, MN 55369	Electronic Service	No	OFF_SL_20-800_Official
Bill	Gullickson	wdgvc76@yahoo.com		1819 Colfax Avenue S Minneapolis, MN 55403	Electronic Service	No	OFF_SL_20-800_Official
Adam	Heinen	aheinen@dakotaelectric.com	Dakota Electric Association	4300 220th St W Farmington, MN 55024	Electronic Service	No	OFF_SL_20-800_Official
Michael	Hoppe	lu23@ibew23.org	Local Union 23, I.B.E.W.	445 Etna Street Ste. 61 St. Paul, MN 55106	Electronic Service	No	OFF_SL_20-800_Official
Caroline	Horton	chorton@aeonmn.org	Aeon	901 N 3rd St Ste 150 Minneapolis, MN 55401	Electronic Service	No	OFF_SL_20-800_Official
Alan	Jenkins	aj@jenkinsatlaw.com	Jenkins at Law	2950 Yellowtail Ave. Marathon, FL 33050	Electronic Service	No	OFF_SL_20-800_Official
Craig	Johnson	cjohnson@lmc.org	League of Minnesota Cities	145 University Ave. W. Saint Paul, MN 55103-2044	Electronic Service	No	OFF_SL_20-800_Official
Richard	Johnson	Rick.Johnson@lawmoss.com	Moss & Barnett	150 S. 5th Street Suite 1200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Sarah	Johnson Phillips	sarah.phillips@stoel.com	Stoel Rives LLP	33 South Sixth Street Suite 4200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Nicolle	Kupser	nkupser@greatermngas.com	Greater Minnesota Gas, Inc. & Greater MN Transmission, LLC	1900 Cardinal Ln PO Box 798 Faribault, MN 55021	Electronic Service	No	OFF_SL_20-800_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Brenda	Kyle	bkyle@stpaulchamber.com	St. Paul Area Chamber of Commerce	401 N Robert Street Suite 150 St Paul, MN 55101	Electronic Service	No	OFF_SL_20-800_Official
Peder	Larson	plarson@larkinhoffman.com	Larkin Hoffman Daly & Lindgren, Ltd.	8300 Norman Center Drive Suite 1000 Bloomington, MN 55437	Electronic Service	No	OFF_SL_20-800_Official
Annie	Levenson Falk	annielf@cubminnesota.org	Citizens Utility Board of Minnesota	332 Minnesota Street, Suite W1360 St. Paul, MN 55101	Electronic Service	No	OFF_SL_20-800_Official
Todd	Liljenquist	todd.liljenquist@mmha.com	Minnesota Multi Housing Association (MHA)	1600 West 82nd Street, Suite 110 Minneapolis, MN 55431	Electronic Service	No	OFF_SL_20-800_Official
Kavita	Maini	kmaini@wi.rr.com	KM Energy Consulting, LLC	961 N Lost Woods Rd Oconomowoc, WI 53066	Electronic Service	No	OFF_SL_20-800_Official
Sarah	Marquardt	smarquardt@mcknight.org	The McKnight Foundation	710 S 2nd St Minneapolis, MN 55401	Electronic Service	No	OFF_SL_20-800_Official
J.B.	Matthews	N/A	Cushman & Wakefield/NorthMarq	3500 American Blvd W - #200 Minneapolis, MN 55431	Paper Service	No	OFF_SL_20-800_Official
Craig	McDonnell	Craig.McDonnell@state.mn.us	MN Pollution Control Agency	520 Lafayette Road St. Paul, MN 55101	Electronic Service	No	OFF_SL_20-800_Official
Matthew	Melewski	matthew@nokomisenergy.com	Nokomis Energy LLC & Ole Solar LLC	2639 Nicollet Ave Ste 200 Minneapolis, MN 55408	Electronic Service	No	OFF_SL_20-800_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Joseph	Meyer	joseph.meyer@ag.state.mn.us	Office of the Attorney General-RUD	Bremer Tower, Suite 1400 445 Minnesota Street St Paul, MN 55101-2131	Electronic Service	No	OFF_SL_20-800_Official
Stacy	Miller	stacy.miller@minneapolismn.gov	City of Minneapolis	350 S. 5th Street Room M 301 Minneapolis, MN 55415	Electronic Service	No	OFF_SL_20-800_Official
David	Moeller	dmoeller@allete.com	Minnesota Power	30 W Superior St Duluth, MN 55802-2093	Electronic Service	No	OFF_SL_20-800_Official
Andrew	Moratzka	andrew.moratzka@stoel.com	Stoel Rives LLP	33 South Sixth St Ste 4200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Ted	Nedwick	tnedwick@nhtinc.org	National Housing Trust	1101 30th Street NW Ste 100A Washington, DC 20007	Electronic Service	No	OFF_SL_20-800_Official
David	Niles	david.niles@avantenergy.com	Minnesota Municipal Power Agency	220 South Sixth Street Suite 1300 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Samantha	Norris	samanthanorris@alliantenergy.com	Interstate Power and Light Company	200 1st Street SE PO Box 351 Cedar Rapids, IA 52406-0351	Electronic Service	No	OFF_SL_20-800_Official
Carol A.	Overland	overland@legalectric.org	Legalectric - Overland Law Office	1110 West Avenue Red Wing, MN 55066	Electronic Service	No	OFF_SL_20-800_Official
Greg	Palmer	gpalmer@greatermngas.com	Greater Minnesota Gas, Inc. & Greater MN Transmission, LLC	1900 Cardinal Ln PO Box 798 Faribault, MN 55021	Electronic Service	No	OFF_SL_20-800_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Eric	Pasi	ericp@ips-solar.com	IPS Solar	2670 Patton Rd Roseville, MN 55113	Electronic Service	No	OFF_SL_20-800_Official
Jennifer	Peterson	jjpeterson@mnpower.com	Minnesota Power	30 West Superior Street Duluth, MN 55802	Electronic Service	No	OFF_SL_20-800_Official
Kristen	Peterson	kristenp@ips-solar.com	New Energy Equity	2670 Patton Road Roseville, MN 55113	Electronic Service	No	OFF_SL_20-800_Official
Gordon	Pietsch	gpietsch@grenergy.com	Great River Energy	12300 Elm Creek Blvd. Maple Grove, MN 55369-4718	Electronic Service	No	OFF_SL_20-800_Official
Phyllis	Reha	phyllisreha@gmail.com		3656 Woodland Trail Eagan, MN 55123	Electronic Service	No	OFF_SL_20-800_Official
Generic Notice	Residential Utilities Division	residential.utilities@ag.state.mn.us	Office of the Attorney General-RUD	1400 BRM Tower 445 Minnesota St St. Paul, MN 55101-2131	Electronic Service	Yes	OFF_SL_20-800_Official
Kevin	Reuther	kreuther@mncenter.org	MN Center for Environmental Advocacy	26 E Exchange St, Ste 206 St. Paul, MN 55101-1667	Electronic Service	No	OFF_SL_20-800_Official
Christine	Schwartz	Regulatory.records@xcelenergy.com	Xcel Energy	414 Nicollet Mall FL 7 Minneapolis, MN 55401-1993	Electronic Service	No	OFF_SL_20-800_Official
Will	Seuffert	Will.Seuffert@state.mn.us	Public Utilities Commission	121 7th Pl E Ste 350 Saint Paul, MN 55101	Electronic Service	Yes	OFF_SL_20-800_Official
Janet	Shaddix Elling	jshaddix@janetshaddix.com	Shaddix And Associates	7400 Lyndale Ave S Ste 190 Richfield, MN 55423	Electronic Service	No	OFF_SL_20-800_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Bria	Shea	bria.e.shea@xcelenergy.com	Xcel Energy	414 Nicollet Mall Minneapolis, MN 55401	Electronic Service	No	OFF_SL_20-800_Official
Brendon	Slotterback	bslotterback@mcknight.org	The McKnight Foundation	710 S 2nd St Minneapolis, MN 55401	Electronic Service	No	OFF_SL_20-800_Official
Ken	Smith	ken.smith@districtenergy.com	District Energy St. Paul Inc.	76 W Kellogg Blvd St. Paul, MN 55102	Electronic Service	No	OFF_SL_20-800_Official
Peggy	Sorum	peggy.sorum@centerpointenergy.com	CenterPoint Energy	505 Nicollet Mall Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Sky	Stanfield	stanfield@smwlaw.com	Shute, Mihaly & Weinberger	396 Hayes Street San Francisco, CA 94102	Electronic Service	No	OFF_SL_20-800_Official
Byron E.	Starns	byron.starns@stinson.com	STINSON LLP	50 S 6th St Ste 2600 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Richard	Stasik	richard.stasik@wecenergygroup.com	Minnesota Energy Resources Corporation (HOLDING)	231 West Michigan St - P321 Milwaukee, WI 53203	Electronic Service	No	OFF_SL_20-800_Official
Kristin	Stastny	kstastny@taftlaw.com	Taft Stettinius & Hollister LLP	2200 IDS Center 80 South 8th St Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Cary	Stephenson	cStephenson@otpco.com	Otter Tail Power Company	215 South Cascade Street Fergus Falls, MN 56537	Electronic Service	No	OFF_SL_20-800_Official
James M	Strommen	jstrommen@kennedy-graven.com	Kennedy & Graven, Chartered	150 S 5th St Ste 700 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Eric	Swanson	eswanson@winthrop.com	Winthrop & Weinstine	225 S 6th St Ste 3500 Capella Tower Minneapolis, MN 55402-4629	Electronic Service	No	OFF_SL_20-800_Official
Jason	Topp	jason.topp@lumen.com	CenturyLink Communications, LLC	200 S 5th St Ste 2200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Jenna	Warmuth	jwarmuth@mnpower.com	Minnesota Power	30 W Superior St Duluth, MN 55802-2093	Electronic Service	No	OFF_SL_20-800_Official
Patricia	Whitney	patricia@pwhitneylaw.com	St. Paul Assn of Responsible Landlords	627 Snelling Avenue South St. Paul, MN 55116	Electronic Service	No	OFF_SL_20-800_Official
Joseph	Windler	jwindler@winthrop.com	Winthrop & Weinstine	225 South Sixth Street, Suite 3500 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official
Robyn	Woeste	robynwoeste@alliantenergy.com	Interstate Power and Light Company	200 First St SE Cedar Rapids, IA 52401	Electronic Service	No	OFF_SL_20-800_Official
Yochi	Zakai	yzakai@smwlaw.com	SHUTE, MIHALY & WEINBERGER LLP	396 Hayes Street San Francisco, CA 94102	Electronic Service	No	OFF_SL_20-800_Official
Kurt	Zimmerman	kwz@ibew160.org	Local Union #160, IBEW	2909 Anthony Ln St Anthony Village, MN 55418-3238	Electronic Service	No	OFF_SL_20-800_Official
Patrick	Zomer	Pat.Zomer@lawmoss.com	Moss & Barnett PA	150 S 5th St #1200 Minneapolis, MN 55402	Electronic Service	No	OFF_SL_20-800_Official