414 Nicollet Mall
Minneapolis, MN 55401

April 30, 2026

—Via Electronic Filing—

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

RE: 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 Ms. Bergman:

Northern States Power Company, doing business as Xcel Energy, submits the enclosed Comments to the Minnesota Public Utilities Commission in response to its March 31, 2026 Notice of Comment Period in the above-referenced docket.

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 contact me at jody.l.londo@xclenergy.com if you have any questions regarding this filing.

Sincerely,

/s/

JODY LONDO
DIRECTOR, REGULATORY AND STRATEGIC ANALYSIS

Enclosure
cc: Service List

STATE OF MINNESOTA
BEFORE THE
MINNESOTA PUBLIC UTILITIES COMMISSION

Katie J. Sieben	Chair
Hwikwon Ham	Commissioner
Audrey C. Partridge	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 **COMMENTS**

INTRODUCTION

Northern States Power Company, doing business as Xcel Energy (Xcel Energy or Company), submits these Comments to the Minnesota Public Utilities Commission (Commission) in response to its Notice of Comment Period issued on March 31, 2026[1] (Notice) in the above-referenced docket.

The Notice seeks responses to the following questions:

(1) Should the Commission accept, modify, or reject the Grid Data Sharing Framework Report submitted into the record on March 4, 2026?
(2) Should the Commission accept, modify, or reject the Framework's appeals process? Specifically, should the Commission accept, modify, or reject the use of the Grid Security Working Group to address informal complaints to minimize submittal to CAO?
(3) Should the Commission accept, modify, or reject the framework's evaluation recommendations?
(4) Are there other issues or concerns related to this matter?

Xcel Energy supports the development of renewable energy and the ability of our customers to access distributed energy resources (DER) and understands that developers have a legitimate interest in accessing grid data to further DER in the public interest. At the same time, we take our responsibility to ensure reliable and safe

[1] *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, NOTICE OF COMMENT (March 31, 2026).

service very seriously. To date, we make significant amounts of data necessary for DER siting publicly available through various tools published on our website.[2] This docket examines utility provision of a limited amount of non-public or highly sensitive information that implicates the physical and cyber security of the grid and of our customers, which raises important national security and grid security questions. We continue to support a measured approach that ensures individuals with legitimate interests in sensitive grid information will have access to it – but with appropriate guardrails that ensures the sensitive information will not fall into the hands of potential bad actors.

After hosting a number of workgroups, Converge Strategies developed its *Recommendations for a Grid Data Sharing Framework* report (Report) that proposes a framework (Framework) to navigate these competing imperatives.[3] There are many aspects of the Report we support, as elaborated in Section II below. But we disagree with a number of recommendations in the Report, and believe there are a number of recommendations that require further record development before Commission decision. We summarize our positions here.

Our concerns:

- *Cost recovery*: The Report does not acknowledge utility costs to implement a grid data sharing Framework, which is a critical gap. It is essential that the Commission explicitly acknowledge that all costs associated with grid data sharing, including administrative and technology related costs, are eligible for cost recovery. As discussed in these comments, we believe a secure portal and other software development costs associated with implementation of this framework be recoverable from all customers, and costs related to program administration be recovered through participant fees, consistent with the cost causation principle.
- *Clarifying the background check proposal*. We agree with and support the requirement that requestors undergo a background check as part of the pre-application process. However, we strongly recommend that the Commission require requestors to provide proof of completed background screenings conducted by a verified third-party reporting agency, rather than requiring utilities to conduct their own reviews using publicly available information.
- *Empowering utilities to maintain discretion to deny requests*. Utilities must be granted the ability to use their discretion to deny certain requests, and to remove or

[2] https://mn.my.xcelenergy.com/s/renewable/developers/interconnection.

[3] *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, RECOMMENDATIONS FOR A GRID DATA SHARING FRAMEWORK (March 4, 2026) ("Converge Strategies Report").

revoke access for individuals or entities as may be appropriate. The Report should explicitly state this necessary condition.

- *Timelines for implementing new business processes.* The Report does not address the time it will take to implement this Framework. Until we know the specific requirements for the portal and data release framework, we cannot know the implementation timeline. We therefore recommend that the Commission expect that the Company will require a minimum of 12 months after the Commission issues its final framework Order to develop our internal processes and necessary technology solutions.
- *Timelines for responding to data requests.* The Report presents an overly prescriptive and unreasonable timeline for responding to data requests. We recommend the Commission articulate a target timeframe of two months for responding to data requests, while expressly allowing utilities additional flexibility to extend that timeframe when warranted.

Issues that need further record development:

- *What data can be requested.* The current Report does not specify which data can be requested and how that ties to legitimate uses pertaining to siting DER. Without these parameters, overly broad or inappropriate requests will strain the request and dispute resolution processes. This issue must be addressed before a workable Framework is established.
- *Developing a clearly defined dispute resolution process.* Before the proposed framework is implemented, we recommend the Commission direct the Grid Security Working Group (GSWG) to develop a clearly defined dispute resolution process, addressing such topics as which parties will be involved in reviewing disputes, procedural details, and steps for elevating unresolved matters. Lack of clarity in this regard will likely lead to contentious disputes regarding the process itself.

We propose the Commission accept the Report but require modifications related to the above topics before implementation begins. We address these positions in more detail below.

COMMENTS

I. BEFORE ACCEPTING THE REPORT, THE COMMISSION SHOULD MODIFY THE PROPOSED CONVERGE STRATEGIES GRID DATA SHARING FRAMEWORK

The Converge Strategies' Report was developed after three intensive workgroup

sessions that provided stakeholders an opportunity to discuss the most pressing issues related to developing a process to request and securely share sensitive distribution grid data in line with the NARUC Grid Data Sharing Framework and Playbook.[4] We believe there are critical gaps that must be addressed, and therefore, recommend the Commission modify the Report as discussed in this section. These substantive concerns need to be addressed before implementation begins.

A. Cost Recovery Must Be Addressed

The Report does not acknowledge utility costs to implement a grid data sharing framework, which is a critical gap. For Xcel Energy, we propose that costs to develop the secure portal and any other technology solutions necessary to implement the approved framework be recoverable, like other recent incremental new hosting capacity costs that have been recovered through the Transmission Cost Recovery (TCR) Rider. Minn. Stat. § 216B. 2425, subd. 8 requires distribution studies to identify interconnection points on its distribution system for small-scale distributed generation resources. And Minn. Stat. § 216B.16, subd. 7b(4) allows "the utility to recover costs associated with distribution planning required under section 216B.2425."

We have recovered distribution planning costs through the TCR rider for other incremental, technology-driven investments required to produce hosting capacity data. Similarly, to provide the requested data considered in this docket, our system planners must conduct additional distribution studies; the results of which will be used by requestors to identify potential DER interconnection points. These studies represent net-new work beyond routine distribution planning activities. Consistent with Minn. Stat. § 216B.16, subd. 7b(4), the software development and implementation costs for this data-sharing framework are necessary to securely share data used to assess distribution-level interconnection capability.

We further propose that ongoing program administration costs related to the Company's support of the data sharing process be recovered through a user fee structure, which we base on the cost causation principle. These costs are expected to include, at a minimum:

- Time to create and maintain new business processes;
- Time to respond to data requests;
- Time to compile reporting data; and
- Other Program administration activities.

[4] https://pubs.naruc.org/pub/E2E50FD7-CD1B-62D5-1071-8D8362AD1E6D?_gl=1*fr1nv0*_ga*MTA0MjU3MzAwOC4xNzcwNzQwMTE3*_ga_QLH1N3Q1NF*czE3NzYwOTIzMTYkbzEwJGcwJHQxNzc2MDkyMzE2JGo2MCRsMCRoMA.. (November 2023).

A fee-based cost causer approach is appropriate, so that utility electric service customers do not subsidize DER developers.

Precedent for this approach exists in the Commission's Open Data Access Standards (ODAS). The ODAS are "intended to set standards for the collection and sharing of customer energy use data (CEUD) for use by third parties,"[5] including both aggregated and anonymized CEUD. In that case, the ODAS protections are primarily driven by customer privacy concerns, rather than grid physical security and cybersecurity as in this Framework. Nonetheless, some of the same logic – balancing the interests of data requesters with those of utility customers as a whole, protecting privacy and safety, and ensuring utility customers do not bear costs while benefits flow primarily to data requesters – apply in both cases.

In the ODAS, Section VI stipulates that:

> *A. A utility may charge the requester a fee to prepare and supply CEUD. A utility charging a data access fee authorized by this section must:*
> *(1) base the fee amount on the actual costs incurred by the utility to create and deliver the requested data;*
> *(2) consider the reasonable value of the data prepared to the utility and, if appropriate, reduce the fee assessed to the requesting person;*
> *(3) provide the requesting person with an estimate and explanation of the fee; and*
> *(4) collect the fee before preparing or supplying the requested data.*[6]

Principles from this section of the ODAS that may also be appropriate for the Framework are that any fees should reflect actual costs to prepare and provide data to requesters, not more or less; that in cases where compiling the data has demonstrated value to the utility as well, the fee may be reduced accordingly to reflect that value; and that if the value is primarily to the requester, charging a fee ensures that the costs of fulfilling such requests are not simply passed on to the utility's customers as a whole.

The ODAS fee structure also allows for a distinction between "start-up" costs to create the infrastructure to meet future data requests, which should not necessarily be

---

[5] Open Data Access Standards at I.A. See *In the Matter of a Petition by the Citizens Utility Board of Minnesota to Adopt Open Data Access Standards,* Docket No. E,G-999/M-19-505, ORDER REFINING OPEN DATA ACCESS STANDARDS (July 5, 2024), and *In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities,* Docket No. E,G-999/CI-12-1344.

[6] Open Data Access Standards at VI.A. See Commission's July 5, 2024 ORDER REFINING OPEN DATA ACCESS STANDARDS.

borne entirely by the first requester; and costs that are specific to fulfilling a given request, which should be borne by the requester, unless a case can be made under VI.A.(2) to reduce those fees in consideration of value to the utility or its customers.

B. Areas of Concern

1. Background Checks Must Be Conducted by Qualified and Verified Third Parties

The Report recommends that requestors undergo a background check prior to submitting an application, including both the individual making the request and any ancillary personnel who may handle the data, such as contractors, student workers, and other third-party organizations, as well as the organization the individual is making the request on behalf of.[7] To implement this recommendation, the Report identifies two potential approaches: (1) background checks conducted by a verified third-party provider, or (2) reviews conducted in-house by utilities using publicly available resources.

We believe background screenings must be conducted by qualified and verified third-parties and presented to the utility at the time a data request is made. A public records search is unlikely to yield information that would adequately inform a potential security risk for an individual. Further, utilities do not maintain in-house resources or the expertise necessary to conduct comprehensive background checks commensurate with the sensitivity of grid data. For example, background screenings for utility employees are typically performed by Fair Credit Reporting Act (FCRA) compliant third-party reporting agencies. Conducting similar screenings internally would introduce significant operational, compliance, and security risks. Background checks require the collection and handling of protected personal information, which would in turn obligate utilities to assume additional data protection, reporting, and regulatory compliance responsibilities. These activities would also impose meaningful financial and staffing burdens on utilities beyond their existing operational scope. While the Report characterizes background checks that use some publicly available resources as without fees, it is important to clarify that these options still require costs related to the use of the utility's internal resources.[8]

The requestor should be responsible for engaging a qualified third-party background screening agency. When a data request is made by an individual on behalf of an organization, we believe the background screening should be conducted on both the individual and the organization. We agree with the Report that, at minimum, the

[7] Converge Strategies Report at p11.
[8] Converge Strategies Report at p12.

screening for individuals should include identity verification and a criminal history check; we further believe that the screening should cover at least the prior seven years. For organizations, the screening should include any ties to foreign entities of concern, poor financial history (e.g., bankruptcy), and cybersecurity incidents. Requestors may reference existing background checks conducted in the last one year for new data requests. All costs associated with background checks should be borne by the requestor, not utility electric service customers.

In the Report, Converge Strategies recommends that the Commission choose one of the two methods for background checks: Verified Third Parties, or Publicly Available Resources.[9] We support this approach and recommend that the Commission choose the Verified Third Parties method for background checks in the Framework, and remove the Publicly Available Resources option.

2. Utilities Must Maintain Discretion Over Requests to Appropriately Manage Risk

We recommend the Commission modify the proposed Framework by clearly acknowledging the utility's authority to deny data requests and revoke access to data. The Report appropriately recognizes that all data sharing carries some level of risk. But the Report appears to assume that all data requests utilities receive will be valid, because it does not explicitly address circumstances under which a utility may deny a request. It also does not address utilities' ability to remove or revoke access for individuals or entities for any reason other than time. For example, given frequent interaction with federal and state agencies, we are aware of information that would inform our assessment of whether certain entities or individuals should have access to certain data, given the importance of the data. Recognition that utilities will integrate security concerns into its decisions on when to withhold certain information is reasonable and appropriate; utilities must have authority to deny requests and/or remove access for individuals or entities.

The ODAS again provides some useful precedent here. While the protections in the ODAS are mostly for reasons of customer privacy, some of the same principles apply equally to grid security. The ODAS has several safeguards to balance the benefits of disclosure against risks:

- Precisely defining the types of data – in that case, Aggregated CEUD and Anonymized CEUD – that may be requested;
- Prohibiting access to personally identifiable information;
- Setting minimum thresholds to protect privacy (e.g., the 4/50 standard for

[9] Converge Strategies Report at p12.

Aggregated CEUD and the 15/15 standard for Anonymized CEUD);

- Stipulating that only certain types of entities are authorized requesters: in the case of Anonymized CEUD, authorized requesters include 501(c)3 nonprofit organizations, federal/state/local/Tribal governments, entities seeking to provide demand response or energy efficiency services, and researchers affiliated with an accredited college or university;
- Allowing utilities to refuse to provide CEUD if the requester does not sign a contract (in effect, a Non-Disclosure Agreement) with specific protections around broader access to the data, data retention and destruction, and specifying the intended use of the data; and
- Requiring customer consent to disclose CEUD for any large industrial or commercial customer with peak demand of 5 MW or more.[10]

In addition to those specific protections, the ODAS provides broadly that "a utility may refuse to provide aggregated or anonymized CEUD when it reasonably believes the data release would create a security risk for the utility, its customer(s), or the public, or that the release would allow the third party to re-identify customers, violate the terms of the contract in 2(v) above, or otherwise use the data in violation of these standards."[11]

While not all the specifics above will be relevant in the case of the Framework, the general principle – and the caution the Commission has exercised to balance the benefits of data disclosure against risks and costs – do apply. The ODAS may provide a starting point for developing specific guidelines and protections in the Framework, including the ability for utilities to exercise some degree of discretion to refuse to provide data if the benefits of disclosure are outweighed by security risks for the utility, its customer(s), or the public.

Although the Report acknowledges that low or medium risk data can be elevated to a higher risk level based on data aggregation, it sets a three-year window as the appropriate benchmark for determining risk level.[12] We do not believe that capping data aggregation risk to a three-year window is sufficient. While some data becomes stale over time, there are many aspects of our distribution system that do not change as rapidly. For example, requests for data from five years ago may still introduce the risk that the requestor can still develop a very detailed view of our distribution grid as

[10] Open Data Access Standards at III.B. See Commission's July 5, 2024 ORDER REFINING OPEN DATA ACCESS STANDARDS and *In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities,* Docket No. E,G-999/CI-12-1344.

[11] Open Data Access Standards at III.C. See Commission's July 5, 2024 ORDER REFINING OPEN DATA ACCESS STANDARDS.

[12] Converge Strategies Report at p15-16.

it is today. Especially given recent advances in publicly available Artificial Intelligence capabilities to scrape insights from vast data sets, low or medium risk in aggregate can result in insights that create unforeseen security risks based on detailed visibility into large portions of the electric grid.

To address these concerns, the Commission could consider the following revisions to the Framework: (Revisions in redline)

> ***Medium-Risk***
> ***Definition.*** *Medium-risk data carries the risk of limited potential impacts to the system and people (e.g. short duration or localized disruptions). It may offer some visibility into system vulnerabilities but not a level that could result in significant harm to the distribution grid and society. It can also be the result of specific points or types of aggregated data that would be normally categorized as low-risk, either in the single request or in a series of requests from an individual or organization ~~over a period of at least three years~~.*[13]
>
> …
>
> ***High-Risk***
> ***Definition.*** *High-risk data is anything that could result in the grid being harmed, significantly degraded, or destroyed, resulting in operations being disrupted on a societal-level. Data in this category reveal specific physical or cyber vulnerabilities of assets or information about individual customers that is critical to security, economic security, public health or safety, or any combination thereof. In Minnesota, these are referred to as Priority End Users, which can include law enforcement, firefighting units, and emergency medical services. It can also be the result of specific points or types of aggregated data that would be normally categorized as medium-risk, either in the single request or in a series of requests from an individual or organization ~~over a period of at least three years~~.*[14]
>
> …
>
> ***Mitigations and Release Criteria***
> *Mitigations and release criteria are flexible, scalable, and can be layered, appropriate to the risk level of the specific request. The list below outlines the appropriate options for protecting shared distribution grid data. Utilities can decide which of these measures are appropriate, given the risk level of a specific use case.*
>
> - *Non-disclosure Agreements (NDA)*

[13] Converge Strategies Report at p15.
[14] Converge Strategies Report at p15-16.

- *Attestations*
- *Business Agreement*
- *Data Sharing Agreement*
- *Data Access Time Limits*
- *View-Only Capabilities (e.g., non-downloadable, secured portals)*
- *Data Sanitization*
- *Data Aggregation*
- *Data Handling Training*
- *Cybersecurity Guidelines/Training*

If this list needs to be amended in the future to respond to shifts in the security landscape, or to account for changes in authority, policy, or technology, we recommend that the new or amended measures be developed and agreed upon by the Grid Security Working Group (GSWG), discussed in detail in Section 4, Application Appeals Process. This ensures the data sharing environment in the state remains procedurally equal for all stakeholders involved. Utilities may reject a data request or remove access to shared data if an acceptable mitigation or release criteria cannot be identified, or if necessary for other security, legal, or operational reasons.[15]

3. Timelines for Implementing New Business Processes and Responding to Data Requests Must Be Addressed

The Report does not adequately address the amount of time utilities will need to establish processes and tools following the issuance of a Commission order.

We recommend the Commission establish at least a 12-month implementation goal following issuance of the order containing the final framework. This time is necessary for utilities to establish internal processes, develop or modify necessary technology solutions, and address staffing and training needs. Stating the timeline as a goal will provide motivation for utilities to implement the framework swiftly, however, also allowing for necessary flexibility to adequately address complexities and unknowns – which is particularly important given the stakes of erroneous or inadvertent disclosure of non-public grid data. The implementation timeline could also be further addressed by requiring utilities to submit a compliance filing within 90 days of the Commission's order that outlines their implementation timelines.

In addition, the Report suggests that utilities process data-sharing requests within two months.[16] We do not support a fixed deadline for processing requests given a number

[15] Converge Strategies Report at p16.
[16] Converge Strategies Report at p19.

of circumstances that may warrant additional time. While a two-month timeframe may be reasonable for most requests, complex requests, or concurrent requests could make strict adherence to a fixed timeline impracticable.

We therefore recommend the Commission modify this aspect of the framework as follows: (Revisions in Redline)

> ***5.0 Timeline.***
> *Utilities shall use at least a 12-month implementation goal following issuance of the Commission's Order containing the final framework to establish internal processes, develop or modify necessary technology solutions, and address staffing and training needs.*
>
> *Establishing a clear, realistic timeline for the overall Grid Data Sharing Process and the individual steps within it is important for effective implementation.*
> *A reasonable overall timeline for completion of a request—from background check initiation to fulfillment of data request—is two months. ~~Within those two months, the response to the Pre-Application should take no more than two weeks; the initial review of the application and scheduling of the scoping meeting should take less than two weeks; and the Risk Assessment and fulfillment of the request should take no more than 30 days. Figure 2: Process Timeline below depicts this~~.*
>
> *While utilities should make every good-faith effort to resolve requests in an efficient and timely manner, we recognize that some requests may take longer due to their complexity or the need to facilitate engagements with the Commission. Additionally, normal activities (e.g., utility employees taking PTO, medical, or family leave, and natural staff turnover) and fluctuating volumes of requests, could impact the timeline. These circumstances should be clearly communicated to the requester, along with a reasonable estimated time of completion.*[17]

C. Areas Requiring Further Record Development

1. *The Report Does Not Adequately Identify What Data Can be Requested and the Data Minimization Principle is Missing*

The Report does not articulate what data sets requestors have a valid need to know in order to site DER that is not already shared – especially in light of the extensive information that is already made available to developers both publicly and subject to NDAs. The Report scopes out a number of datasets (e.g. federally protected non-shareable data, data that is already public, and Personally Identifiable Information),[18]

[17] Converge Strategies Report at p19.
[18] Converge Strategies Report at p7.

but it does not identify what non-public data sets requestors have a valid need to know, and for what purpose. Although requestors are required to specify the data sought and how they intend to use it, the Report does not establish clear guardrails on the types of non-public data requests that may be considered permissible. As a result, utilities are left without clear guidance on the boundaries of acceptable requests. This could lead to an increased volume of overly broad or inappropriate requests that are not in the public interest and, in turn, place unnecessary strain on the application and dispute resolution process.

Absent clarity within the Framework, requestors may seek access to data that is not necessary to evaluate potential locations for DER and would carry high risk if shared publicly. For example, we strongly believe that data reflecting the exact locations of our distribution lines should not be shared. This data would show the precise routes of the feeder lines that serve our customers, including critical customers, allowing a threat actor to plan an attack for maximum impact. The risk of sharing this data far outweighs the potential benefit. This information is also unnecessary for DER siting, as requestors would only need to know which feeder serves a particular location, not the physical route of the entire feeder.

We strongly recommend the Commission modify the proposed Framework so that it will clearly identify the type of data that requestors may seek, and link each type of data to a specific, well-defined need related to siting DER projects. We also recommend that a specific risk level is identified for each category of data. We propose the Commission task the GSWG to develop an exhaustive list of specific data points that can be requested, identify a risk level for each type of data, and specify a need related to siting DER for each type of data. Development of this exhaustive list will reduce utility judgment and provide consistency in treating data requests. Importantly, before any information is released, even if on any type of "approved" list, the release of data would need to comply with privacy expectations of our customers.

Additionally, the Report does not directly address the "Minimum Data needed" or "least data access" principle. Previous filings from stakeholders, including from the Commission and Minnesota Department of Commerce, support the principle that only the most essential and minimum necessary data should be shared with requestors. For example, in the February 7, 2025 Commission Order, Order Point No. 4 states "Within six months of this order, the workgroup must provide recommendations for a process for securely sharing *the minimum necessary data* [emphasis added] for DER interconnection."[19] The required discussion should

[19] *In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to*

therefore address in what way publicly available information (such as the monthly queue report or the hosting capacity map and related data) is not sufficient.

Including clear language that utilities should share only the minimum data necessary to support a requestor's stated purpose aligns with best practices for data sharing. Balancing the benefit of sharing grid data with the need for information security needs to be grounded in an understanding that utilities should only share relevant, purpose-driven data, avoiding providing broader or more detailed datasets than are reasonably required. Not addressing this in the final recommendations may be interpreted as lack of support for this principle, which we believe is not the case.

We recommend the Commission task the GSWG to develop a specific list of data that can be requested and to assign a risk level for each type of data. Importantly, before any information is released, even if on any type of "approved" list, the release of data would need to comply with energy security and privacy expectations of our customers.

II. XCEL ENERGY SUPPORTS MANY ASPECTS OF THE PROPOSED CONVERGE STRATEGIES GRID DATA SHARING FRAMEWORK

Notwithstanding our concerns noted above, the Report is a useful guide for securely sharing sensitive grid data. We support a number of the findings of the Report.

A. The Threat Landscape is Evolving and Increasing

We agree with how the Report characterizes the threat landscape. Ensuring the reliable delivery of power requires the recognition that adversaries and malicious actors are actively targeting grid infrastructure and seeking to degrade or destroy the grid in the most impactful ways possible. If sensitive data falls into the wrong hands, it could enable the planning and execution of coordinated attacks capable of causing widespread, long-term, and potentially catastrophic outages. There have always been risks to grid operations, including traditional hazards such as storms. But the advent of advanced cyberattacks on the grid present far more dangerous outcomes. Cyberattacks can render equipment, especially hard to replace equipment, inoperable by manipulating data so the mis-operation of the system short circuits the equipment at scale. Operational data for a distribution system in the wrong hands makes this type of outcome easier. Gathering and analyzing data can often go unnoticed until attacks

Electric Distribution Grid Data, p7, Docket No. E999/CI-20-800, ORDER ACCEPTING REPORT, ESTABLISHING STANDING WORKGROUP, AND ASSIGNING PROCEDURES AND TASKS FOR THE WORKGROUP (February 7, 2025).

occur. Proactively safeguarding sensitive data needs to be part of how utilities prevent such attacks. Federal and State law enforcement agencies and national security professionals, including the Department of Homeland Security and Intelligence Community agencies, have consistently emphasized that the electric grid is being targeted for cyber and physical attacks.

If a nation state adversary, domestic violent extremist, or criminal were to obtain sensitive grid data, that information could be used to identify vulnerabilities and execute targeted attacks with severe consequences. Losing power is not merely an inconvenience; electricity is the foundation that all other critical infrastructure, government, and private sector depend upon; without electricity, critical customer and services would not be able to function, with cascading and wide-ranging impacts. As the Report notes, such risks are particularly heightened for customers that are critical to national security, economic security, or public health or safety. Federal, State and local government facilities; telecommunications systems; water and wastewater infrastructure; hospitals; mass gathering venues (such as arenas); and the operations of law enforcement, first responders, and other critical public services all depend on the reliable supply of electricity powering their facilities. The consequences of a successful attack on the grid, and the resulting impact on critical public services, cannot be overstated.

Additionally, since our last filing in January 2025, there have been a number of concerning cyber-attacks that demonstrate the extent and severity of threat actors' ability to disrupt, degrade, or destroy critical infrastructure and services. Below we highlight some pertinent examples, underscoring a threat landscape where adversaries and criminals are seeking to disrupt critical infrastructure, including energy infrastructure. The threat to Minnesota's grid is not hypothetical; it is a real and present danger.

- As the Intelligence Community has reported, China remains the most active and persistent cyber threat to critical infrastructure networks, including the energy sector. China's campaign to preposition access on critical infrastructure for attacks during crisis or conflict demonstrates the growing breadth and depth of its capabilities to compromise U.S. infrastructure.[20] Having sophisticated knowledge of energy grids would enable a potentially catastrophic attack that could have maximum impact on the critical customers and services our grid powers.
- Threat actors affiliated with Iran have conducted reconnaissance and exploitation activity against U.S. critical infrastructure Operational Technology

[20] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf at p11-12.

(OT) and Industrial Control Systems (ICS), resulting in disruptions across several U.S. critical infrastructure sectors. Specific assets targeted were those used commonly in the electric and gas sectors.[21] Detailed maps of electric grid infrastructure and knowledge of load flows could enable an attack with maximum damage.

- In December 2025, likely Russian state sponsored actors conducted destructive cyberattacks on the Polish electric grid, targeting both renewable and thermal generation power plants. This attack demonstrates a strong ability to execute coordinated destructive campaigns, which could be used against the U.S. grid with growing DER.[22]
- In July 2025, likely a criminal group executed a sophisticated and impactful cyber-attack against the City of St. Paul, disrupting essential government services.[23] And in April 2026, a criminal group also executed an attack against the City of Winona, requiring the Minnesota National Guard to provide cyber defense assistance.[24] Although these attacks focused on government services, they demonstrate the intent and capability of threat actors to successfully attack and disrupt critical infrastructure in Minnesota.

B. The Four-Step Approach Emphasizes a Deliberate Risk-Informed Process

The Report seeks to operationalize the NARUC Grid Data Sharing Playbook by proposing a four step process: (1) pre-application verification, during which the requestor provides a statement of intent and undergoes a background check; (2) application, during which the requestor provides detailed information about the type of data being requested; (3) risk analysis, during which the utility conducts a preliminary review, hosts a scoping meeting, and determines the risk level associated with the requested data; and (4) data sharing method, where the utility chooses an appropriately secure sharing method.[25] We support this four step process and commend the Report for appropriately emphasizing the need to protect sensitive grid data through a deliberate and risk-informed process.

C. Requests Must be Specific and Include the Purpose

The Report appropriately incorporates an essential safeguard into the application

---

[21] https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a.
[22] https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/.
[23] https://www.cbsnews.com/minnesota/news/melvin-carter-st-paul-cyberattack-update-august-11/.
[24] https://www.kttc.com/2026/04/11/winona-county-announces-national-guard-bca-aid-following-cybersecurity-attack/.
[25] Converge Strategies Report at p10-17.

process by requiring individuals or organization requesting grid data to provide detailed information about the specific data being sought.[26] This level of specificity is necessary to enable utilities to conduct informed risk analysis and prevent wasted staff time and resources. Furthermore, the Report proposes applicants describe the end product they intend to develop using the requested data. Clear articulation of how the data will be used is a critical step in ensuring that only appropriate data is requested and shared, and that data disclosures are aligned with legitimate and well-defined purposes.

If requestors are not able to specify why they need certain data, or if they identify data that is not relevant (such as requests for data on circuits connecting to a substation that already has a significant queue of pending DER applications as reported in the DER public queue available on Xcel Energy's website),[27] the utility should retain the discretion to reject the data request and, if available, refer the requestor to the currently publicly available information. We discuss this gap in the Framework in Section I above.

D. Utilities are Appropriately Empowered to Determine Protective Measures to Share Information Securely

The Report appropriately proposes that utilities be afforded the discretion to choose how to share data securely, and identifies a range of potential options.[28] We strongly support this discretion. As a general principle, we anticipate using a secure, utility-managed portal for low- and medium-risk data, while limiting access to high-risk data to in-person viewing. The portal and credentialing process (e.g. establishment of a username, password, and multi-factor authentication) will at least provide traceability in the event of a security breach.

The Report empowers utilities to determine which protective measures are warranted based on the specific use case, including NDAs, business agreements, data sharing agreements, data access time limits, and cybersecurity guidelines/trainings, among others.[29] We note that NDAs depend on good faith implementation and will not resolve all risks associated with sharing sensitive data. Nonetheless, we support the recommended use of NDAs, and note our intent to require NDAs, at minimum, in advance of sharing non-public data.

---

[26] Converge Strategies Report at p13.
[27] The public DER Queue Report is available at https://mn.my.xcelenergy.com/s/renewable/developers/interconnection.
[28] Converge Strategies Report at p16-17.
[29] Converge Strategies Report at p16.

III. THE APPEALS PROCESS REQUIRES FURTHER DEFINITION

The Notice asks whether the Commission should accept, modify, or reject the Framework's appeals process; specifically, whether the Commission accept, modify, or reject the use of the Grid Security Working Group to address informal complaints to minimize submittal to Consumer Affairs Office (CAO).

The Report proposes an appeals process intended to standardize how disputes over grid data sharing are handled, with disputes first addressed through the GSWG and unresolved matters subsequently elevated to the CAO. We support the Commission adopting a dispute resolution process, since it is likely there will be disputes between utilities and requestors in some situations, especially regarding highly sensitive data. The Report suggests that disputes be handled by the GSWG, and unresolved disputes would then be elevated to the CAO. However, the Report does not sufficiently define how the proposed GSWG-based process would function in practice. In its current form, the Working Group lacks clarity regarding who would participate in dispute resolution, how conflicts would be evaluated, what criteria would be applied, and how recommendations or determinations would be documented and communicated. Absent this clarity, it is difficult for stakeholders to assess whether the proposed process would be fair, efficient, and effective.

We recommend the Commission direct the GSWG to develop a clearly defined dispute resolution process before this Report is accepted. The process must address, at a minimum, which parties will be involved in reviewing disputes, the criteria they will use to evaluate competing positions, and the procedural steps for elevating unresolved matters. One option could be for the Department to continue its work in this area and oversee the GSWG's efforts to identify consensus recommendations or, in the event there is not consensus, summarize parties' positions to the Commission for consideration.

IV. ACCEPT THE FRAMEWORK'S EVALUATION RECOMMENDATIONS

The Notice asks whether the Commission should accept, modify, or reject the framework's evaluation recommendations. The Report proposes that the Commission order a robust evaluation of the grid data sharing process three years after implementation, with utilities reporting annually on specific metrics.[30]

Evaluating the process and key metrics (how many data requests were lodged, how

[30] Converge Strategies Report at p22.

many data requests were fulfilled, how many disputes were brought, how many were resolved) will be valuable to monitor and assess. Given the evolving nature of threats to the grid, we support this recommendation, recognizing that this grid data sharing framework will be inherently iterative. Regular reporting and formal evaluation will allow the Commission and stakeholders to assess whether the framework is functioning as intended, identify unanticipated risks or burdens, and determine whether adjustments are warranted. In particular, tracking metrics such as the number of data requests submitted, the number of requests fulfilled or denied, the frequency and nature of disputes, and dispute-resolution outcomes will provide valuable insight into both the operational impacts and security implications of the framework over time.

For these reasons, the Company supports acceptance of the Report's evaluation recommendations.

CONCLUSION

We appreciate the Commission's efforts to develop a robust record on this issue of national concern – the proper balance between sharing information to enable DER without compromising grid or customer energy security, especially in the complex and active threat landscape that exists. We respectfully request the Commission to accept the Company's recommendations for further record development and to address gaps that exist in the Converge Strategies' Report.

Dated: April 30, 2026

Northern States Power Company

CERTIFICATE OF SERVICE

I, Joshua DePauw, 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 30th day of April 2026

/s/

_____

Joshua DePauw
Regulatory Administrator

#	First Name	Last Name	Email	Organization	Agency	Address	Delivery Method	Alternate Delivery Method	View Trade Secret	Service List Name
1	Roxanne	Achman	rachman@co.benton.mn.us			531 Dewey Street Foley MN, 56329 United States	Electronic Service		No	20-800 Official
2	Chad	Adams	chada@swmhp.org	Southwest Minnesota Housing Partnership		2401 Broadway Ave Slayton MN, 56172 United States	Electronic Service		No	20-800 Official
3	Michael	Ahern	ahern.michael@dorsey.com	Dorsey & Whitney, LLP		50 S 6th St Ste 1500 Minneapolis MN, 55402-1498 United States	Electronic Service		No	20-800 Official
4	Michael	Allen	michael.allen@allenergysolar.com	All Energy Solar		721 W 26th st Suite 211 Minneapolis MN, 55405 United States	Electronic Service		No	20-800 Official
5	Arnie	Anderson	arnieanderson@minncap.org	Minnesota Community Action Partnership		MCIT Building 100 Empire Drive, Suite 202 St. Paul MN, 55103 United States	Electronic Service		No	20-800 Official
6	Kristine	Anderson	kanderson@greatermngas.com	Greater Minnesota Gas, Inc.		1900 Cardinal Lane PO Box 798 Faribault MN, 55021 United States	Electronic Service		No	20-800 Official
7	Sarah	Anderson	sa@bomampls.org	Greater Minneapolis BOMA		Suite 610 121 South 8th Street Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official
8	Nichol	Beckstrand	nichol.beckstrand@mmha.com	Minnesota Multi Housing Association		1600 W 82nd St Ste 110 Minneapolis MN, 55431 United States	Electronic Service		No	20-800 Official
9	Sasha	Bergman	sasha.bergman@state.mn.us		Public Utilities Commission	121 7th Pl E Ste 350 St. Paul MN, 55101 United States	Electronic Service		Yes	20-800 Official
10	Martin S.	BeVier	bevi0022@umn.edu			4001 Grand Ave South # 3 Minneapolis MN, 55409 United States	Electronic Service		No	20-800 Official
11	Jon	Braman	jbraman@brightpower.com	Bright Power, Inc.		11 Hanover Square, 21st floor New York NY, 10005 United States	Electronic Service		No	20-800 Official
12	Sheri	Brezinka	sbrezinka@usgbcmn.org			701 Washington Ave. N Suite 200 Minneapolis MN, 55401 United States	Electronic Service		No	20-800 Official
13	Annika	Brindel	abrindel@nhtinc.org	National Housing Trust		1101 30th Street NW	Electronic Service		No	20-800 Official

#	First Name	Last Name	Email	Organization	Agency	Address	Delivery Method	Alternate Delivery Method	View Trade Secret	Service List Name
						Ste 100A Washington DC, 20007 United States				
14	Matthew	Brodin	mbrodin@allete.com	Minnesota Power		30 West Superior Street Duluth MN, 55802 United States	Electronic Service		No	20-800 Official
15	Mike	Bull	mike.bull@state.mn.us		Public Utilities Commission	121 7th Place East, Suite 350 St. Paul MN, 55101 United States	Electronic Service		Yes	20-800 Official
16	James	Canaday	james.canaday@ag.state.mn.us		Office of the Attorney General - Residential Utilities Division	Suite 1400 445 Minnesota St. St. Paul MN, 55101 United States	Electronic Service		No	20-800 Official
17	Richard	Carter	rick.carter@lhbcorp.com			2780 Shadywood Rd Excelsior MN, 55331-9599 United States	Electronic Service		No	20-800 Official
18	Brent	Christensen	brentc@mnta.org	Minnesota Telecom Alliance		1000 Westgate Drive, Ste 252 St. Paul MN, 55114 United States	Electronic Service		No	20-800 Official
19	Andrew	Clearwater		Future of Privacy Forum		1400 I St NW Ste 450 Washington DC, 20005-6503 United States	Paper Service		No	20-800 Official
20	John	Coffman	john@johncoffman.net	AARP		871 Tuxedo Blvd. St, Louis MO, 63119-2044 United States	Electronic Service		No	20-800 Official
21	Roger	Colton	roger@fsconline.com			34 Warwick Road Belmont MA, 02478 United States	Electronic Service		No	20-800 Official
22	Sheri	Comer	sheri.comer@ftr.com	Frontier Communications Corporation		1500 MacCorkle Ave SE Charleston WV, 25396 United States	Electronic Service		No	20-800 Official
23	Generic	Commerce Attorneys	commerce.attorneys@ag.state.mn.us		Office of the Attorney General - Department of Commerce	445 Minnesota Street Suite 1400 St. Paul MN, 55101 United States	Electronic Service		Yes	20-800 Official
24	George	Crocker	gwillc@nawo.org	North American Water Office		5093 Keats Avenue Lake Elmo MN, 55042 United States	Electronic Service		No	20-800 Official

#	First Name	Last Name	Email	Organization	Agency	Address	Delivery Method	Alternate Delivery Method	View Trade Secret	Service List Name
25	Stacy	Dahl	sdahl@minnkota.com	Minnkota Power Cooperative, Inc.		5301 32nd Ave S Grand Forks ND, 58201 United States	Electronic Service		No	20-800 Official
26	John	Farrell	jfarrell@ilsr.org	Institute for Local Self-Reliance		2720 E. 22nd St Institute for Local Self-Reliance Minneapolis MN, 55406 United States	Electronic Service		No	20-800 Official
27	Trent	Fellers	trent.fellers@windstream.com	Windstream		1440 M St Lincoln NE, 68508 United States	Electronic Service		No	20-800 Official
28	Sharon	Ferguson	sharon.ferguson@state.mn.us		Department of Commerce	85 7th Place E Ste 280 Saint Paul MN, 55101-2198 United States	Electronic Service		No	20-800 Official
29	Jenny	Glumack	jenny@mrea.org	Minnesota Rural Electric Association		11640 73rd Ave N Maple Grove MN, 55369 United States	Electronic Service		No	20-800 Official
30	Bill	Gullickson	wdgvc76@yahoo.com			1819 Colfax Avenue S Minneapolis MN, 55403 United States	Electronic Service		No	20-800 Official
31	Adam	Heinen	aheinen@dakotaelectric.com	Dakota Electric Association		4300 220th St W Farmington MN, 55024 United States	Electronic Service		No	20-800 Official
32	Michael	Hoppe	lu23@ibew23.org	Local Union 23, I.B.E.W.		445 Etna Street Ste. 61 St. Paul MN, 55106 United States	Electronic Service		No	20-800 Official
33	Frank	Hornstein	frank.hornstein@minneapolismn.gov	City of Minneapolis		350 South 5th Street Minneapolis MN, 55415 United States	Electronic Service		No	20-800 Official
34	Caroline	Horton	chorton@aeonmn.org	Aeon		901 N 3rd St Ste 150 Minneapolis MN, 55401 United States	Electronic Service		No	20-800 Official
35	Alan	Jenkins	aj@jenkinsatlaw.com	Jenkins at Law		2950 Yellowtail Ave. Marathon FL, 33050 United States	Electronic Service		No	20-800 Official
36	Craig	Johnson	cjohnson@lmc.org	League of Minnesota Cities		145 University Ave. W. Saint Paul MN, 55103-2044 United States	Electronic Service		No	20-800 Official
37	Richard	Johnson	rickjohnson@cozen.com	Cozen O'Connor		150 S. 5th Street Suite 1200 Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official

#	First Name	Last Name	Email	Organization	Agency	Address	Delivery Method	Alternate Delivery Method	View Trade Secret	Service List Name
38	Sarah	Johnson Phillips	sjphillips@stoel.com	Stoel Rives LLP		33 South Sixth Street Suite 4200 Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official
39	Nicolle	Kupser	nkupser@greatermngas.com	Greater Minnesota Gas, Inc.		1900 Cardinal Ln PO Box 798 Faribault MN, 55021 United States	Electronic Service		No	20-800 Official
40	Brenda	Kyle	bkyle@stpaulchamber.com	St. Paul Area Chamber of Commerce		401 N Robert Street Suite 150 St Paul MN, 55101 United States	Electronic Service		No	20-800 Official
41	Annie	Levenson Falk	annielf@cubminnesota.org	Citizens Utility Board of Minnesota		332 Minnesota Street, Suite W1360 St. Paul MN, 55101 United States	Electronic Service		No	20-800 Official
42	Todd	Liljenquist	todd.liljenquist@mmha.com	Minnesota Multi Housing Association (MHA)		1600 West 82nd Street, Suite 110 Minneapolis MN, 55431 United States	Electronic Service		No	20-800 Official
43	Kavita	Maini	kmaini@wi.rr.com	KM Energy Consulting, LLC		961 N Lost Woods Rd Oconomowoc WI, 53066 United States	Electronic Service		No	20-800 Official
44	Christine	Marquis	regulatory.records@xcelenergy.com	Xcel Energy		414 Nicollet Mall MN1180-07-MCA Minneapolis MN, 55401 United States	Electronic Service		No	20-800 Official
45	J.B.	Matthews		Cushman & Wakefield/NorthMarq		3500 American Blvd W - #200 Minneapolis MN, 55431 United States	Paper Service		No	20-800 Official
46	Craig	McDonnell	craig.mcdonnell@state.mn.us		Minnesota Pollution Control Agency	520 Lafayette Road St. Paul MN, 55101 United States	Electronic Service		No	20-800 Official
47	Matthew	Melewski	matthew@theboutiquefirm.com	Nokomis Energy LLC & Ole Solar LLC		2639 Nicollet Ave Ste 200 Minneapolis MN, 55408 United States	Electronic Service		No	20-800 Official
48	Joseph	Meyer	joseph.meyer@ag.state.mn.us		Office of the Attorney General - Residential Utilities Division	Bremer Tower, Suite 1400 445 Minnesota Street St Paul MN, 55101-2131 United States	Electronic Service		No	20-800 Official
49	Andrew	Moratzka	andrew.moratzka@stoel.com	Stoel Rives LLP		33 South Sixth St Ste 4200 Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official

#	First Name	Last Name	Email	Organization	Agency	Address	Delivery Method	Alternate Delivery Method	View Trade Secret	Service List Name
50	Pouya	Najmaie	najm0001@gmail.com	Cooperative Energy Futures		3416 16th Ave S Minneapolis MN, 55407 United States	Electronic Service		No	20-800 Official
51	David	Niles	david.niles@avantenergy.com	Minnesota Municipal Power Agency		220 South Sixth Street Suite 1300 Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official
52	Samantha	Norris	samanthanorris@alliantenergy.com	Interstate Power and Light Company		200 1st Street SE PO Box 351 Cedar Rapids IA, 52406-0351 United States	Electronic Service		No	20-800 Official
53	Logan	O'Grady	logrady@mnseia.org	Minnesota Solar Energy Industries Association		2288 University Ave W St. Paul MN, 55114 United States	Electronic Service		No	20-800 Official
54	Carol A.	Overland	overland@legalectric.org	Legalectric - Overland Law Office		1110 West Avenue Red Wing MN, 55066 United States	Electronic Service		No	20-800 Official
55	Greg	Palmer	gpalmer@greatermngas.com	Greater Minnesota Gas, Inc.		1900 Cardinal Ln PO Box 798 Faribault MN, 55021 United States	Electronic Service		No	20-800 Official
56	Jennifer	Peterson	jjpeterson@mnpower.com	Minnesota Power		30 West Superior Street Duluth MN, 55802 United States	Electronic Service		No	20-800 Official
57	Kristen	Peterson	kristenp@ips-solar.com	New Energy Equity		2670 Patton Road Roseville MN, 55113 United States	Electronic Service		No	20-800 Official
58	Gordon	Pietsch	gpietsch@grenergy.com	Great River Energy		12300 Elm Creek Blvd. Maple Grove MN, 55369-4718 United States	Electronic Service		No	20-800 Official
59	Phyllis	Reha	phyllisreha@gmail.com			3656 Woodland Trail Eagan MN, 55123 United States	Electronic Service		No	20-800 Official
60	Generic Notice	Residential Utilities Division	residential.utilities@ag.state.mn.us		Office of the Attorney General - Residential Utilities Division	1400 BRM Tower 445 Minnesota St St. Paul MN, 55101-2131 United States	Electronic Service		Yes	20-800 Official
61	Kevin	Reuther	kreuther@mncenter.org	MN Center for Environmental Advocacy		26 E Exchange St, Ste 206 St. Paul MN, 55101-1667 United States	Electronic Service		No	20-800 Official
62	Janet	Shaddix Elling	jshaddix@janetshaddix.com	Shaddix And Associates		7400 Lyndale Ave S Ste 190	Electronic Service		No	20-800 Official

#	First Name	Last Name	Email	Organization	Agency	Address	Delivery Method	Alternate Delivery Method	View Trade Secret	Service List Name
						Richfield MN, 55423 United States				
63	Bria	Shea	bria.e.shea@xcelenergy.com	Xcel Energy		414 Nicollet Mall Minneapolis MN, 55401 United States	Electronic Service		No	20-800 Official
64	Ken	Smith	ken.smith@districtenergy.com	District Energy St. Paul Inc.		76 W Kellogg Blvd St. Paul MN, 55102 United States	Electronic Service		No	20-800 Official
65	Peggy	Sorum	peggy.sorum@centerpointenergy.com	CenterPoint Energy		505 Nicollet Mall Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official
66	Sky	Stanfield	stanfield@smwlaw.com	Shute, Mihaly & Weinberger		396 Hayes Street San Francisco CA, 94102 United States	Electronic Service		No	20-800 Official
67	Byron E.	Starns	byron.starns@stinson.com	STINSON LLP		50 S 6th St Ste 2600 Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official
68	Richard	Stasik	richard.stasik@wecenergygroup.com	Minnesota Energy Resources Corporation (HOLDING)		231 West Michigan St - P321 Milwaukee WI, 53203 United States	Electronic Service		No	20-800 Official
69	Kristin	Stastny	kstastny@taftlaw.com	Taft Stettinius & Hollister LLP		2200 IDS Center 80 South 8th Street Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official
70	Cary	Stephenson	cstephenson@otpco.com	Otter Tail Power Company		215 South Cascade Street Fergus Falls MN, 56537 United States	Electronic Service		No	20-800 Official
71	Jason	Topp	jason.topp@lumen.com	Qwest Communications Company, LLC.		200 S 5th St Ste 2200 Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official
72	Jenna	Warmuth	jwarmuth@mnpower.com	Minnesota Power		30 W Superior St Duluth MN, 55802-2093 United States	Electronic Service		No	20-800 Official
73	Sarah	Whebbe	swhebbe@mnseia.org	MnSEIA		445 Minnesota Street Suite 730 St. Paul MN, 55101 United States	Electronic Service		No	20-800 Official
74	Patricia	Whitney	patricia@pwhitneylaw.com	St. Paul Assn of Responsible Landlords		627 Snelling Avenue South St. Paul MN, 55116 United States	Electronic Service		No	20-800 Official
75	Joseph	Windler	jwindler@winthrop.com	Winthrop & Weinstine		225 South Sixth Street, Suite 3500	Electronic Service		No	20-800 Official

#	First Name	Last Name	Email	Organization	Agency	Address	Delivery Method	Alternate Delivery Method	View Trade Secret	Service List Name
						Minneapolis MN, 55402 United States				
76	Robyn	Woeste	robynwoeste@alliantenergy.com	Interstate Power and Light Company		200 First St SE Cedar Rapids IA, 52401 United States	Electronic Service		No	20-800 Official
77	Yochi	Zakai	yzakai@smwlaw.com	SHUTE, MIHALY & WEINBERGER LLP		396 Hayes Street San Francisco CA, 94102 United States	Electronic Service		No	20-800 Official
78	Curtis	Zaun	czaun@mnseia.org	MnSEIA		PO Box 8141 Saint Paul MN, 55108 United States	Electronic Service		No	20-800 Official
79	Kurt	Zimmerman	kwz@ibew160.org	Local Union #160, IBEW		2909 Anthony Ln St Anthony Village MN, 55418-3238 United States	Electronic Service		No	20-800 Official
80	Patrick	Zomer	pzomer@cozen.com	Cozen O'Connor		150 S. 5th Street, #1200 Minneapolis MN, 55402 United States	Electronic Service		No	20-800 Official