COMMERCE DEPARTMENT

November 12, 2024

Will Seuffert
Minnesota Public Utilities Commission
121 7th Place East, Suite 350
St. Paul, Minnesota 55101-2147

RE: Comments of the Minnesota Department of Commerce
Docket No. E999/CI-20-800

Dear Mr. Seuffert:

Attached are the comments of the Minnesota Department of Commerce (Department) in the following matter:

In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data.

The Department provides its recommendations in the attached comments and is available to answer any questions the Minnesota Public Utilities Commission may have.

Sincerely,

/s/ Peter Wyckoff, Ph.D.
Deputy Commissioner, Division of Energy Resources

DT/DD/ad
Attachment

COMMERCE DEPARTMENT

Before the Minnesota Public Utilities Commission

Comments of the Minnesota Department of Commerce

Docket No. E999/CI-20-800

I. INTRODUCTION

The Minnesota Department of Commerce (Department) provides its comments in response to the Commission's Notice of Supplemental Comment Period in Docket No. E999/CI-20-800.[1] The Commission's investigation into grid security issues related to data access began in 2020, with an evolving discussion among docket participants across multiple rounds of comments. Prior iterations of stakeholder discussion in this proceeding presented conflicting perspectives on the risks associated with providing access to distribution grid data while maintaining grid security, including the decision-making framework to approach the inherent tradeoffs. Rather than revisit the entirety of this proceeding's history, the Department's comments will focus on the significant developments since the issuance of the Commission's 2023 Order, which provide a pathway to resolving disagreements among parties.

The disagreements in this proceeding regarding data access stem from the real challenge of weighing the potential benefits of greater access to distribution grid data with the potential risks associated with its provision. The status quo, in which this evaluation of the cost-benefit and access to additional data is determined solely by utilities, will remain in place absent further action from the Commission. Given the policy objectives of the state for renewable technology deployment and clean energy mandates, progress in the arena of data access, even if incremental, stands to benefit the state. The Commission will also continue to balance considerations of affordability, reliability, safety, and decarbonization with potential grid security risks. This consideration requires a nuanced understanding of risk, one which has not always been present in this proceeding. The establishment of a risk assessment framework will assist stakeholders and the Commission with properly assessing the risk associated with access to distribution grid data. Importantly, the presence of risk does not preclude access, merely that it will shape the form of access. In addition, a successful framework will ensure that there are not situations in which utilities can use the mere specter of risk to thwart any and all access.

The publication of the National Association of Regulatory Utility Commission (NARUC) Grid Data Sharing Playbook (NARUC Playbook) in 2023 provides a potential framework to approach these issues.[2] Importantly, during the 2024 workgroup process, parties have coalesced around the use of the NARUC Framework as the means to develop a Minnesota-specific framework to address distribution grid data

---

[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,* Minnesota Public Utilities Commission, Notice of Supplemental Comment Period, October 9, 2024, Docket No. E999/CI-20-800, (eDockets) 202410-210840-01 (hereinafter "Notice").

[2] The Department notes that the NARUC Grid Data Sharing Playbook is the publication that provided the context for the collaborative that developed the Framework, as well as discussion of its application for each state and the example use cases discussed by the group. Accordingly, the Department refers to the publication as the Playbook and the framework for grid data sharing decision-making as the Framework.

sharing. The workgroup process has also brought parties into alignment regarding the need for an ongoing dialogue to consider further developments regarding distribution grid security matters.

In addition, the Department has engaged Converge Strategies, LLC (Converge or CSL) to provide specialty services regarding grid security in response to the Commission's 2023 Order, in which the Commission requested additional record development regarding security risks. Converge has conducted stakeholder engagement concurrent with the 2024 workgroup process and assessed grid data and infrastructure security concerns as it relates to Minnesota distribution utilities. Converge has developed a written report (Converge Report) summarizing its findings and providing recommendations based on its analysis. The Department has filed the Converge Report along with these comments for Commission consideration.

The Department provides its comments below to provide context to the Converge Report and in response to the Commission's Notice. The Department appreciates the work of parties throughout the 2024 workgroup process, including the commitment to continue to engage in dialogue through a standing workgroup. The Department supports the use of the NARUC Framework by a standing workgroup, in tandem with the specific recommendations put forth in the Converge Report regarding key topics for the workgroup to address, to develop a data sharing process.

The Department's support for this approach is grounded in the belief that the status quo that has presided over the lengthy history of this proceeding does not serve the public interest. The collaborative process of the recent workgroup sessions has created real momentum that a standing workgroup can leverage to develop a data sharing process for Minnesota. Continuing this progress stands to benefit the stakeholders involved in this proceeding as well as the state in meeting its policy objectives.

II. PROCEDURAL BACKGROUND

June 7, 2023	The Minnesota Public Utilities Commission (Commission) issued an Order in Docket No. E999/CI-20-800 which, among other items, convened a work group to develop the record more fully for Commission consideration within 18 months and requested the Department retain specialty services to provide a recommendation on privacy and security and to participate in related analysis and stakeholder engagement.[3] The Department subsequently selected Converge Strategies, LLC (CSL or Converge) to provide the required specialty services.

[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,* Minnesota Public Utilities Commission, Order Establishing Work Group, June 7, 2023, Docket No. E999/CI-20-800, (eDockets) 20236-196417-02 (hereinafter "2023 Order").

July 2, 2024	The Commission issued a notice of work group to commence the process required by the 2023 Order for meetings later in the summer.[4]
August 28, 2024 and October 4, 2024	The Commission issued draft notes of the three Commission-led workgroup meetings.[5]
October 9, 2024	The Commission issued its mid-workgroup report with a summary of the discussions, conclusions, recommendations, next steps, and remaining points of disagreement.[6] The Workgroup Report also formally submitted into the record the NARUC Framework.[7] The Commission also issued its Notice of Supplemental Comment Period in the present docket.

The October 9, 2024 Notice included the following topics open for comment:

- Do parties have additional comments on the workgroup recommendations filed with this notice?
- What information from the DOE/NARUC collaborative framework (submitted into record on October 9th, 2024 as an attachment to the workgroup report) is applicable to decisions being made in this record? Should the Commission approve the framework for use by a standing workgroup to consider data sharing and security issues between parties as recommended by the workgroup?
- Was there any specific information provided by security experts and other new parties during the workgroup meetings that would help inform Commissioners in their decision making?

III. DEPARTMENT ANALYSIS

In this proceeding, the Commission and parties have grappled with the provision of distribution grid data to enable the effective deployment of distribution energy resources (DER) while maintaining grid

[4] *In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data,* Minnesota Public Utilities Commission, Notice of Workgroup, July 2, 2024, Docket No. E999/CI-20-800, (eDockets) 20247-208237-01 (hereinafter "Notice of Workgroup").
[5] *In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data,* Minnesota Public Utilities Commission, Notes from Workshops 1 and 2, August 19, 2024, Docket No. E999/CI-20-800, (eDockets) 20248-209599-01 (hereinafter "Meeting 1 and 2 Notes"); *In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data,* Minnesota Public Utilities Commission, Workgroup Session 3 Notes, October 4, 2024, Docket No. E999/CI-20-800, (eDockets) 202410-210725-01 (hereinafter "Meeting 3 Notes").
[6] *In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data,* Minnesota Public Utilities Commission, Workgroup Report, October 9, 2024, Docket No. E999/CI-20-800, (eDockets) 202410-210841-01 (hereinafter "Workgroup Report").
[7] Workgroup Report Attachment 1.

security. A forthright discussion of how to balance the risks of grid data disclosure with the benefits that can arise from increased data access has remained elusive.

The Department's comments, along with the work of its consultant, Converge, will inform the Commission's decision regarding how to solve for risk while balancing the various policy objectives of affordable and reliable electric service amidst the rapid deployment of clean energy technologies. A risk assessment framework that differentiates types and magnitudes of risk can ensure that data access and control policies can be properly matched to the risk associated with the data. The risk associated with access to data cannot be viewed consistently across different data items and at different times, and the presence of risk should not prohibit its availability. Instead, risk must be assessed based on the specific characteristics of the data requested and the means by which access is provided.[8]

The state's ability to meet its policy objectives regarding clean energy deployment, such as the 2040 carbon-free standard,[9] the Distributed Solar Energy Standard (DSES),[10] or the community solar garden (CSG) program,[11] among others, is heavily impacted by decisions regarding data access. Greater access to data can help the state meet its goals, which should motivate all parties in this proceeding to make progress beyond the current state of affairs. Therefore, the recommendations put forth by the workgroup, discussed in more detail below, are consistent with developing a data sharing process that that increases data access while retaining the security of the grid. It is important to not lose sight of the fact that the incremental provision of data, represented by the development of a data sharing process, reflects progress beyond the current status quo for data sharing.

Data access is at contention precisely because the data involved has value to all parties. Exclusive utility control of data may minimize risks, but it also serves to maximize the retention of benefits with utilities. However, the data generated from ratepayer-funded investments should also derive value for ratepayers, which a complete restriction of distribution grid data precludes. The public interest is served by enabling greater access to data in a manner which allows the state to meet its policy objectives and generates benefits to ratepayers. The Department also recognizes that greater data access can serve private interests of distributed energy resource (DER) developers, but circumstances of aligned interests do not negate the value to the public. In fact, an improved DER interconnection process stands to potentially benefit all parties, including utilities, if additional data sufficiently informs DER developers to avoid interconnection requests for assets whose interconnection will prove too costly to proceed and identifies those areas on the distribution system where DER deployment or other non-wires alternatives can defer costly infrastructure upgrades. Thus, utilities will save resources by avoiding processing futile applications, saving ratepayers as well. Ultimately, a balanced approach to

[8] *See* Converge Report Section 4.
[9] Minn. Stat. § 216B.1691, subd. 2g (2023).
[10] Minn. Stat. § 216B.1691, subd. 2h (2023).
[11] Minn. Stat. § 216B.1641 (2023).

data access, one in which the access provided is commensurate with the risks of sharing the data, ensures that the public interest is served.

A. FURTHER RECORD DEVELOPMENT FROM THE COMMISSION'S 2023 ORDER

A.1. The Department and Converge

The Commission's 2023 Order requested additional record development on security risks, particularly the perspective of security experts to inform the Commission's decision:

> Comments in this docket have developed a voluminous record, but the Commission concludes that additional record development is necessary. Largely absent are the perspectives of grid-and cyber-security experts who would be able to assess the degree of risk created when specific types of distribution grid data are publicly available. It is important for the Commission to have this information to adequately balance disclosure risks with the benefits of increased data access.[12]

To further this record development, the Commission requested the Department to incur costs for specialty services to participate in related analysis and stakeholder engagement to provide a recommendation on privacy and security to the Commission.[13] The Department selected Converge to provide the specialty services in this proceeding.

The Department provides a brief overview of the Converge contract efforts. Converge has conducted a landscape analysis of grid data sharing best practices, interviewed eight stakeholder participants engaged in this proceeding, and is planning to interview two additional trade association organizations who recently re-engaged with the docket. At the request of workgroup participants and supported by Commission Staff, the Department also convened a workgroup session in parallel with the supplemental comment period to maintain the ongoing dialogue, as well as the development of Converge's proposal, until further Commission action. The session provided participants an introduction to Converge's initial findings and framework proposal for further development by the standing workgroup. Converge has completed a written report (Converge Report) summarizing its work and findings, as well as presenting a framework proposal for the ongoing security workgroup discussions. The Department has filed the Converge Report as Attachment A with these comments. The Department notes that the Converge Report is meant to inform the Commission's consideration of security risks, rather than reflect a comprehensive assessment of the entirety of policy objectives the Commission will weigh in making its decision.

[12] 2023 Order at 9.
[13] 2023 Order Point 6.

The Converge Report provides recommendations for implementation of the NARUC Framework via a standing workgroup, consistent with the workgroup recommendations and discussed further below. Converge provides guidance on key topics that require further discussion among parties during the workgroup meetings, in order to develop a data sharing process to recommend to the Commission.

A.2. Security Risks

As it relates to electric system security, institutional inertia—in itself not unique to Minnesota— has frustrated open dialogue among parties. The potential disclosure of sensitive grid data through Freedom of Information Act (FOIA) requests may create risks to grid security when data is misused or mishandled by a requestor, and administrative transparency objectives are at times in conflict with the utilities' responsibility to properly protect this information in accordance with their internal information security policies. Minnesota currently lacks an exemption to the public disclosure of Critical Energy Infrastructure Information (CEII), unlike the majority of states.[14] Understandably, this shapes the perspective of utilities towards the provision of infrastructure data. Meanwhile, regulators may be barred from participating in forums where critical infrastructure owners and operators disclose emergent threats. As an example, the primary forum for electric industry sharing of security-related threats, vulnerabilities, and incidents occurs in the Electricity Information Sharing and Analysis Center (E-ISAC), operated by the North American Electric Reliability Corporation (NERC).[15] E-ISAC personnel, however, are prohibited from sharing information with other NERC personnel.[16] This separation of security threat discussions hampers regulatory body decision-making, forcing regulators to rely on incomplete information in exchange for fostering an environment where security practitioners are free to exchange critical real-time information needed to combat emerging threats free from the chilling effect of worrying about potentially sharing information that could materially harm the company during a post hoc prudency review.

Security considerations have largely extended beyond the traditional areas of state government expertise. For the Department and the Commission, economic regulation has served as the means to ensure the safe, affordable, and reliable provision of electric service in a manner that is equitable and meets the state's environmental and clean energy requirements. The provision of reliable service, however, is at least in part a function of security, and the electricity sector is incorporating security implications into the broader discussion of reliability. For example, NARUC partnered with the U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER) on an initiative to develop cybersecurity baselines for electric distribution systems and interconnected DER

---

[14] Rackley, Jessica. *State Protection of Critical Energy Infrastructure Information (CEII).* National Governors Association, (2019). At 1. Available at: https://www.nga.org/wp-content/uploads/2019/05/CEII-Paper-June-2019-Revised.pdf.
[15] Electricity Information Sharing and Analysis Center. *About the E-ISAC.* (Last visited November 4, 2024). Available at: https://www.eisac.com/s/about-the-eisac.
[16] North American Electric Reliability Corporation. *Separation Protocol Applicable to E-ISAC and NERC.* (2016). Available at: https://nerc123.my.salesforce.com/sfc/p/#2E0000012tgy/a/2E000000B1Ra/G_.twdIBsfvNx05Jn3_ujJczfHIvCcGMlyEWSbmvJvw.

and intends to issue implementation guidance for states.[17] The initiative is intended to aid states in addressing cybersecurity risks at the distribution level as part of an overall effort of enhancing the nation's grid reliability and resilience.

Meanwhile risk quantification, whether associated with cybersecurity, physical infrastructure, or otherwise, remains an area without a prescribed approach. Industry best practices exist, but absent requirements regarding the approach to risk assessment, each utility is left to establish its own process and develop its own expertise.[18] Customization is appropriate to meet the needs of each organization, particularly due to the variety of software and network configurations that may exist. However, customized approaches to risk also complicate the ability of external parties, such as the DER developers most engaged throughout this proceeding, to understand how each utility arrives at its conclusions regarding potential disclosure of information based on its assessment of risk. Thus, developing expertise across the sector, among utilities and government bodies, is imperative for consistent risk assessment.

Threat intelligence analysis regarding foreign nation-state and domestic terrorist adversaries is largely conducted and controlled at the federal level and, therefore, states are reliant on the advisories distributed by federal partners. However, this process has inherent limitations for application to state-level threats. First, the Federal Energy Regulatory Commission (FERC) dedicates its resources to the areas over which it has authority, i.e. generation and transmission, meaning its risks risk assessments and mitigations are lacking granularity to speak to geographically-specific distribution systems. Second, security clearance requirements further limit access to relevant information for state actors, requiring federal partners to disseminate information regarding specific threats. The White House's recently released National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) acknowledged the deficiency of this approach and established the following objective: "Improve the real-time sharing of timely, actionable intelligence and information at the lowest possible classification level among Federal, State, local, Tribal, territorial, private sector, and international partners to facilitate risk mitigation to critical infrastructure."[19]

In the absence of clearances to receive timely information regarding threat, states must rely on what information is available publicly. Public information, however, must be intentionally vague and is left open to the interpretation of state actors regarding the application to local circumstances. In

---

[17] National Association of Regulatory Utility Commissioners. *Cybersecurity Baselines for Electric Distribution Systems and DER.* (Last visited November 4, 2024). Available at: https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/

[18] O'Brien, Patrick. *Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2.* International Society of Automation Global Security Alliance. (Last visited November 4, 2024). Available at: https://gca.isa.org/blog/cybersecurity-risk-assessment-according-to-isa-iec-62443-3-2

[19] The White House. *National Security Memorandum on Critical Infrastructure Security and Resilience.* (April 30, 2024). Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/

particular, threats associated with nation-state and state-sponsored actors provides limited insight into the particular and localized threats to the electricity system.[20]

The application of federal threat discussions to the distribution system reveals limitations. As an example, NERC has developed Critical Infrastructure Protection (CIP) Reliability Standards to protect the bulk power system.[21] The standards are targeted to protect the system from the potential of cascading failures resulting from impacts to system assets. The standards apply to the large assets relevant to the bulk power system and the potential significant downstream consequences of failures. For example, high impact ratings applied for the categorization of bulk power system cyber assets apply to generation exceeding 3,000 MW in a single interconnection.[22] The risk mitigation required to protect the electric system from damage associated with such large assets is of an entirely different scale than the mitigation required for distribution system sized assets. Therefore, NERC CIP standards may largely not be relevant to the considerations at hand, nor need such standards automatically apply to the owners and operators of distribution-sized assets.

In the current paradigm, states are left in a challenging position. States need to solve for risk, but they must do so in an environment in which threat and vulnerability information is not typically shared with them. The history of this proceeding reveals the challenge of this dialogue around risk, as threats from nation-states related to the bulk power system have obscured the discussion. A nuanced discussion of risk is necessary to enable sound decision-making. Collectively, the workgroup recommendations for a standing workgroup applying the NARUC Framework, along with the framework proposal from the Converge Report, can develop a data sharing process that incorporates a nuanced risk assessment framework. Ultimately, a risk assessment framework can facilitate the Commission's decision-making as it balances its policy objectives including affordability, reliability, and clean energy.

Next, the Department responds to each of the Notice topics.

B. WORKGROUP RECOMMENDATIONS

The Commission included the following topic open for comment in its Notice:

> *Do parties have additional comments on the workgroup recommendations filed with this notice?*

---

[20] Cybersecurity and Infrastructure Security Agency. *Joint Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* (February 7, 2024). Available at: https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf

[21] North American Electric Reliability Corporation. *Reliability Standards.* (Last visited November 4, 2024). Available at: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

[22] North American Electric Reliability Corporation. *CIP-002-5.1a – Cyber Security – BES Cyber System Categorization.* (December 14, 2016). Available at: (https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

The Department addresses each of the workgroup recommendations identified in the Workgroup Report. First, the workgroup recommended the establishment of a standing workgroup. This recommendation came about to build upon the work completed to date, which has brought parties closer into alignment, and to allow for the parties to have an established structure in which to consider developing grid data security issues. As was evident in the docket through the prior comment periods in 2022 and 2023, the security landscape can shift rapidly due to arising threats. In addition, technological, policy, and regulatory changes can impact considerations regarding grid data security. A standing workgroup provides the venue to incorporate these changes. Parties arrived upon the comparison to the work conducted by the Distributed Generation Work Group (DGWG) for matters related to the Minnesota Distributed Energy Resource Interconnection Process (MN DIP).[23][24] In such a model, the parties work through disagreements collectively and provide recommendations or request further guidance from the Commission. The Department notes the shift in tone of the discussions in the docket in the most recent round of workgroup meetings and appreciates the willingness of parties to continue to productively work together.

The workgroup momentum was also evident in the participants coalescing around an agreed upon framework for its discussions. The workgroup recommended the Commission approve the use of the NARUC Framework in working through data sharing disagreements. The Department will discuss the contents of the NARUC Framework further in response to notice topic two but notes the progress it represents in the docket for parties to utilize an agreed upon framework for considering grid data security.

In addition, the adoption of the NARUC Framework reinforces the usefulness of a standing workgroup. The NARUC Framework is contemplated as a collaborative tool and iterative process. This iterative approach was informed by the input of security experts in the docket, as discussed further below in response to notice topic three. A standing workgroup utilizing the NARUC Framework provides the forum to develop final recommendations for the currently contemplated use case, that of DER interconnection, as well as consider new developments and use cases. **Accordingly, the Department recommends the Commission approve a standing workgroup to consider data sharing and security issues.**

The Department recognizes the risk of establishing a standing workgroup without more detailed guidance. Accordingly, the Department believes it is warranted to establish a set time frame for the

[23] Meeting 3 Notes at 5.
[24] *In the Matter of Establishing Generic Standards for Utility Tariffs for Interconnection and Operation of Distributed Generation Facilities Under Minnesota Laws 2001, Chapter 212; In the Matter of Updating the Generic Standards for the Interconnection and Operation of Distributed Generation Facilities Established under Minn. Stat § 216B.1611,* Minnesota Public Utilities Commission, Order Establishing Workgroup and Process to Update and Improve State Interconnection Standards, January 24, 2017, Docket Nos. E999/CI-01-1023, E999/CI-16-521, (eDockets) 20171-128408-01.; Minnesota Public Utilities Commission. *Stakeholders & Resources.* (Last visited November 4, 2024). Available at: https://mn.gov/puc/activities/economic-analysis/distributed-energy/resources/

workgroup to deliver a status report or final recommendation to the Commission for a data sharing process for DER interconnection. This time frame would not negate the need for a standing workgroup to take up additional matters as circumstances evolve and as assigned to it from other open dockets, a process similar to that of the DGWG. However, a time frame for a deliverable would provide participating parties and the Commission assurance of a conclusion to the data sharing process at question in this proceeding. The Converge Report contemplates three workgroup meetings.[25] The Department suggests a possible time frame of six months for the standing workgroup to conduct the meetings, as well as allow time for any additional meetings that may be required, and make its recommendation to the Commission. The Department requests parties submit comments on establishing goals and the timing of deliverables to guide the standing workgroup's efforts.

The Department recommends the Commission require the workgroup to provide its final recommendations regarding a data sharing process for DER interconnection within six months of the issue date of the Order.

Next, the workgroup made recommendations regarding the application of the NARUC Framework, which the Department considers related and therefore discusses collectively. First, the workgroup recommended the Commission affirm that the minimum necessary data should be shared and that it should be shared securely. Second, the workgroup recommended the Commission authorize the workgroup to determine the security methods to be applied to shared data. The Department notes that these items did not represent a consensus view and Commission Staff identified opportunities for further Commission guidance.[26]

The Department observes that these recommendations may be premature in the sense that part of the intent of the standing workgroup is to further refine the data elements to be shared and the corresponding security methods. These areas requiring further discussion align with the NARUC Framework categories of Data Details and Data Sharing Tactics, discussed further below. As parties are not yet aligned on the data details to enable the use case, parties will continue to interpret "minimum necessary data" based on their own understanding. Once the workgroup has recommendations on the specific data to be shared, defining "minimum necessary" data through the process and in the context of the specific use case, and the tactics to do so, it can bring those before the Commission for approval.

The workgroup also sought Commission guidance on whether federal requirements should be included in discussions, rather than just state requirements and priorities. The Department believes it is appropriate to include federal requirements in further discussions of the standing workgroup if those requirements can be proven to place limitations on the sharing of requested distribution data, as current and future requirements have the potential to impact both what data may be shared and the

[25] Converge Report Section 5.
[26] Meeting 3 Notes at 5.

manner in which it can be shared. Changes to federal requirements in response to new security developments can be incorporated into the discussions of a standing workgroup, as required.

C. NARUC FRAMEWORK

The Commission included the following topic open for comments in its Notice:

> *What information from the DOE/NARUC collaborative framework (submitted into record on October 9th, 2024 as an attachment to the workgroup report) is applicable to decisions being made in this record? Should the Commission approve the framework for use by a standing workgroup to consider data sharing and security issues between parties as recommended by the workgroup?*

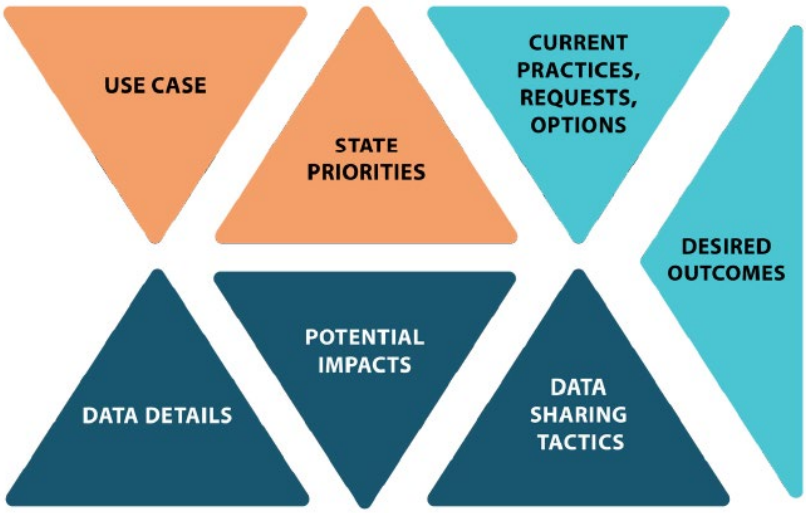
C.1. Framework Overview

It is an important step in this proceeding for parties to have agreed upon the use of the NARUC Framework for consideration of grid data sharing issues moving forward. The Framework provides a means to consider the development of a data sharing process appropriate for Minnesota utilities. However, while it is a useful guide, the Framework's limitations also reveal that it does not provide direct requirements or resolution to the disagreements at hand, as it "does not serve as a step-by-step planning document or a prescriptive set of recommendations. Rather, the playbook offers considerations for effective stakeholder engagement and provides practical insights that illustrate the application of the Framework."[27] Thus, the Framework is built upon and requires collaboration to be effective, reinforcing the value of a standing workgroup, as discussed previously. Further, as evidenced by the use case cases discussed by the collaborative and provided in the Playbook, these are not technical use cases that can offer detailed answers to the mechanism for data sharing. Rather, the Framework provides parties the means to develop a data sharing process that can be brought forth to the Commission for approval.

The Department provides a brief overview of the NARUC Framework, which is illustrated in the NARUC Playbook as follows:

[27] NARUC Playbook at 3.

Figure 1: NARUC Framework Categories



NARUC Playbook at 3

The NARUC Framework categories are briefly described as follows:

- Use Case – Short description of the scenario for which grid data sharing is relevant.
- State Priorities – State goals, policies, and authorities that may apply to the use case and grid data sharing.
- Current Practices, Requests, Options – Grid data already available or shared, additional data being requested, and existing options for enabling the use case.
- Desired Outcomes – Intended benefits enabled through the availability of electric utility grid data.
- Data Details – Data elements necessary to unlock the benefits of the use case.
- Potential Impacts – Incremental risks and consequences of sharing additional grid data details beyond current practices.
- Data Sharing Tactics – Approaches that can be implemented to mitigate potential negative impacts of grid data sharing.[28]

C.2. Framework Categories

Next, the Department briefly discusses each of the NARUC Framework categories as it relates to this proceeding.

[28] NARUC Playbook at 4.

C.2.1. Use Case

The NARUC Playbook includes example use cases discussed by the collaborative to develop the Framework. The use case "Improving DER Interconnection" is particularly relevant to the discussion in this proceeding and provides a helpful lens to understand the application of the Framework.[29] As discussed above, the current DER interconnection paradigm can result in customers and developers submitting interconnection requests to utilities in locations which will require costly system upgrades to allow interconnection. Thus, utility and developer resources are used inefficiently on requests with limited likelihood of proceeding. Greater access to data to improve the DER interconnection process can save developer, utility, and ratepayer resources by more effectively siting DER and promoting efficient interconnection. While DER interconnection is the primary use case contemplated in this proceeding, the NARUC Framework can be applied to other use cases, as well, allowing the Framework to serve as the basis for considering future data sharing needs.[30]

C.2.2. State Priorities

The Department notes a number of state goals, policies, and authorities that apply to the use case of DER interconnection, although not intended as an exhaustive list. DSES sets distributed solar generation requirements for Minnesota public utilities.[31] The Commission initiated Docket No. E002, E015, E017/CI-24-288 in response to a legislative requirement for a proceeding to develop standards for distribution system cost sharing for interconnection in constrained areas.[32] The NARUC Framework also incorporates into this category considerations of which party has the "burden of proof" for data sharing, regulatory mechanisms, and CEII protections.[33] Minnesota utilities are required to provide safe, adequate, efficient, and reasonable service,[34] and the Commission has authority to adopt standards for the provision of service,[35] including for safety, reliability, and service quality of distribution utilities.[36] While parties in this proceeding may not be in full agreement regarding the relative balance of the state's priorities, the Department observes that all parties, including utilities, have a shared understanding of the importance of meeting the policy objectives related to renewable and clean energy deployment.

C.2.3. Current Practices, Requests, Options

Distribution grid data is already available or shared in number of different ways. Xcel Energy provides a publicly available hosting capacity map.[37] The Minnesota DER interconnection process (MN DIP) allows

---

[29] NARUC Playbook Appendix A at 29.
[30] Workgroup Report at 2.
[31] Minn. Stat. § 216B.1691, subd. 2h (2023).
[32] *In the Matter of Establishing Tariffs for Distribution System Cost Sharing for Interconnection in Constrained Areas*, Minnesota Public Utilities Commission, Notice of Docket Opening, August 30, 2024, Docket No. E002, E015, E017/CI-24-288, (eDockets) 20248-209885-01.
[33] NARUC Playbook at 8-9.
[34] Minn. Stat. § 216B.04 (1974).
[35] Minn. Stat. § 216B.09 (1993).
[36] Minn. Stat. § 216B.029 (2007).
[37] Xcel Energy. *Hosting Capacity Program.* (Last visited November 4, 2024). Available at: https://mn.my.xcelenergy.com/s/renewable/developers/interconnection/hosting-capacity-map

for a pre-application report for parties considering interconnecting DER.[38] MN DIP also provides system impact studies and facilities studies for certain interconnection requests.[39] Dakota Electric Association, Otter Tail Power, and Minnesota Power provide discrete sets of information on-demand to interconnecting parties.[40] Non-disclosure agreements (NDA) are standard practice for DER requests.[41] The NARUC Playbook suggests consideration of data availability, data quality, data accuracy, data location, and data accessibility.[42]

The NARUC collaborative process also published a summary of current state practices towards data sharing, which discusses the differing regulatory approaches across the country.[43] While hosting capacity maps are the most common form of data sharing, states have different requirements regarding granularity and accessibility. The spectrum of approaches can assist the working group and the Commission by providing concrete examples of data access implemented in other jurisdictions.

C.2.4. Desired Outcomes

The NARUC Playbook's discussion of the Desired Outcomes category is informative:

> Articulating the expected benefits of sharing grid data, either generally or within the context of a given use case or state policy driver, provides valuable insights to regulatory decision-makers. Such benefits—the "desired outcomes" in Framework parlance—may be understood broadly as the public interest motivations for sharing data. They can be qualitative expressions of anticipated value creation from grid data sharing in broad terms or rooted in relevant quantitative analyses.[44]

As discussed above, the Department believes that the public interest motivation for making data sharing more efficient to promote DER interconnection while maintaining grid security is clear. The Department also observes general agreement among parties across the first four NARUC Framework categories, including Desired Outcomes. The disagreements that have been the primary areas of discussion in this proceeding, including those that still remain, reside in the three remaining categories: Data Details, Potential Impacts, and Data Sharing Tactics.

---

[38] Minnesota Public Utilities Commission. *State of Minnesota Distributed Energy Resources Interconnection Process (MN DIP) v2.3.* (April 15, 2024). At Section 1.4. Hereinafter "MN DIP". Available at: https://mn.gov/puc/assets/MN%20DIP%20updated%20by%204.15.24%20Order%20Clean_tcm14-623149.pdf
[39] MN DIP Section 4.
[40] 2023 Order, Order Point 1.
[41] Converge Report Section 3.2.
[42] NARUC Playbook at 11.
[43] National Association of Regulatory Utility Commissioners. *Grid Data Sharing: Brief Summary of Current State Practices*. (2023). Available at: https://pubs.naruc.org/pub/145ECC5C-1866-DAAC-99FB-A33438978E95?_gl=1*1c7ab9s*_ga*MTA4MDI3ODU1Mi4xNzEyOTM1MDY2*_ga_QLH1N3Q1NF*MTczMDQ3MjI0Ni4zMy4wLjE3MzA0NzIyNDYuMC4wLjA.
[44] NARUC Playbook at 12.

C.2.5. Data Details

Data Details refers to the data elements necessary to unlock the benefits of the use case under consideration. Data details have been a focal point of this proceeding since its inception.[45] Parties have spent significant time during the 2024 workgroup process to further develop this category, but consensus has not yet been reached regarding what data is truly necessary to improve DER interconnection and deployment.[46] Here, the NARUC Playbook's delineation of "need to have" data from the "nice to have"[47] can be instructive, but further dialogue among parties is necessary to arrive at an agreed upon set of data for access. Parties have made progress on data details, however, and the primary remaining data requiring discussion are hourly load shapes and forecasted annual load.[48]

C.2.6. Potential Impacts

The Potential Impacts category of the NARUC Framework is the foundation of this proceeding, as the Commission has been focused on understanding how to assess the risk associated with data sharing. The Commission's requests in its 2023 Order for further record development regarding security risks most directly pertain to potential impacts, and the Converge Report is also largely focused on this category. Despite being an area of significant discourse, further engagement is needed from utilities and developers to identify the risk values each industry sector associates with specific data details. Here, the development of a data-centric risk assessment framework, in which risk is appropriately matched to the specific data requested, will be vital.

C.2.7. Data Sharing Tactics

Data sharing tactics refers to the approaches that can be implemented to mitigate potential negative impacts of grid data sharing. Tactics include vetting processes for data recipients, legal protections, NDAs, secure portals, and others. The Converge Report offers implementation recommendations pertinent to data sharing tactics, specifically the discussion of data identification and classification and tiered access and disclosure.[49] Data sharing tactics are critical to ensure that risks can be sufficiently mitigated while facilitating greater access, i.e. the presence of risk does not require complete restriction. While the presence of data sharing tactics may still present a hurdle to data access, the continuum of tactics that are available should allow for risk mitigation that is appropriately matched to the data requested. Providing greater access to data, even if partially reliant on specific tactics, still represents progress and should be supported by all parties.

---

[45] *In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data,* Minnesota Public Utilities Commission, Notice of Comment Period, October 30, 2020, Docket Nos. E999/CI-20-800, E002/M-19-685, (eDockets) 202010-167790-01. Attachment 1.
[46] *In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data*, Xcel Energy, Materials for Grid Security Workgroup, October 8, 2024, Docket No. E999/CI-20-800, (eDockets) 202410-210812-01, (hereinafter "Xcel October 8, 2024 Letter"). Attachment A.
[47] NARUC Playbook at 14.
[48] Xcel October 8, 2024 Letter, Attachment A.
[49] Converge Report Section 4.

C.2.8. Framework Categories Conclusion

Based on the foregoing, the Department observes the applicability of the NARUC Framework to the decisions being made in the current proceeding, with a particular emphasis on the Framework categories of Data Details, Potential Impacts, and Data Sharing Tactics. **The Department recommends the Commission approve the use of the NARUC Framework by a standing workgroup. The Department also recommends the use of the proposal put forth by Converge supporting specific lines of inquiry for the additional work group sessions, as discussed in the Converge Report.**

D. SECURITY EXPERTS

The Commission included the following topic open for comments in its Notice:

> *Was there any specific information provided by security experts and other new parties during the workgroup meetings that would help inform Commissioners in their decision making?*

The Commission's 2023 Order discussed the absence of relevant security stakeholders from the docket record to that point, concluding that additional record development with the requested participation of additional stakeholders was needed.[50] The recent workgroup meetings reflect the desired expanded scope of participants, with representatives of the following agencies participating:

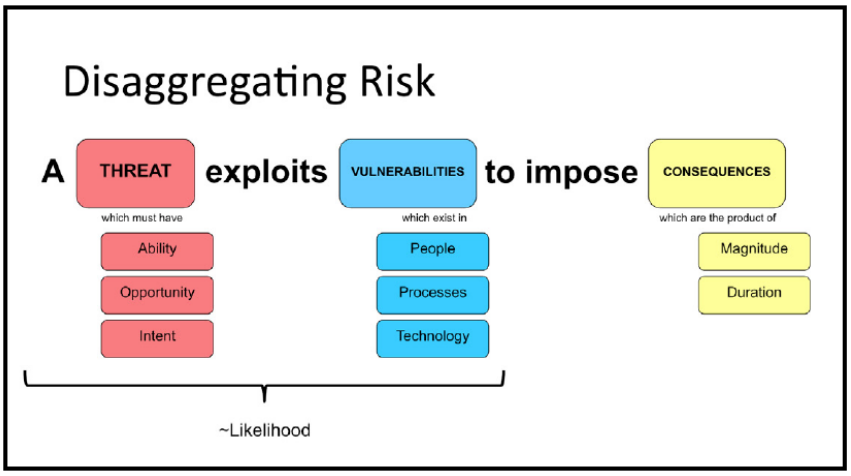
- MN Department of Public Safety's Homeland Security and Emergency Management division (DPS HSEM),
- MN IT Services (MNIT),
- US Department of Energy Cybersecurity, Energy Security, and Emergency Response (CESER),
- MN Bureau of Criminal Apprehension Fusion Center (FC), and
- Federal Bureau of Investigation, Minneapolis (FBI).[51]

The discussion of security threats during the latest round of workgroups evolved to provide a more nuanced understanding of the nature of threats. During the last round of comments in 2022 and 2023, parties raised security concerns in response to cyber-attacks by nation-state actors.[52] A shared understanding of the applicability of such threats to the issues of concern in this proceeding, namely that of distribution grid data sharing in Minnesota, remained elusive. Security experts have informed the discussion by delineating capability and intent in regards to threats, which together inform risk assessments. While the capability of nation-state actors to induce significant harms upon the Minnesota distribution system are apparent, the intent to do so remains unknown. In contrast, domestic violent extremists may pose greater threats when considering the intent of the actors, but the capability to do induce harm, both of in terms of magnitude and geographic scope, is distinct from a coordinated cyber action deployed as one tactic among many employed to obtain strategic

[50] 2023 Order at 9 and Order Point 4.
[51] Meeting 1 and 2 Notes, Meeting 3 Notes.
[52] 2023 Order at 3-4.

geopolitical advantage in a great power competition. The following figure from the NARUC Framework incorporates these elements and provides a helpful risk conceptualization tool:

Figure 2: NARUC Framework Risk Management Conceptual Mapping



NARUC Playbook at 16

The Department believes that the expanded scope of participation through the latest round of workgroups has successfully informed parties and informed the recommendations provided. Chief among the contributions was the necessity of a flexible framework to evaluate security issues through an iterative process.[53] The recommendations for the establishment of a standing workgroup to evaluate grid data security using the NARUC Framework are informed by these contributions. Retaining an open investigative docket provides a venue for a more rapid response to emergent issues, whether those relate to the threat landscape, policies, technology, or regulations. The workgroup can then submit its recommendations or issues requiring further Commission guidance into the record, memorializing the group's efforts. A standing workgroup also enables coordination across the state government for interrelated planning efforts around the distribution system, state energy security, and emergency response.

The discussion among parties around the risks and consequences associated with the sharing of additional grid data requires further development, which the standing workgroup affords. The specific incremental risk value for each of the data details, for example, requires further engagement under the Potential Impacts category of the NARUC Framework, as discussed above in response to notice topic two. The attached Converge Report provides a more comprehensive discussion of risks and the potential impacts of data sharing, as well.

IV. DEPARTMENT RECOMMENDATIONS

Based on the workgroup process, the attached Converge report, and the information in the record, the Department has prepared initial recommendations, which are provided below. The recommendations

[53] Workgroup Report at 1.

correspond to the subheadings of Section III above. The Department may provide additional recommendations in reply comments.

A. FURTHER RECORD DEVELOPMENT FROM THE COMMISSION'S 2023 ORDER

B. WORKGROUP RECOMMENDATIONS

- B.1. The Department recommends the Commission approve a standing workgroup to consider data sharing and security issues.
- B.2. The Department recommends the Commission require the workgroup to provide its final recommendations regarding a data sharing process for DER interconnection within six months of the issue date of the Order.

C. NARUC FRAMEWORK

- C.1. The Department recommends the Commission approve the use of the NARUC Framework by a standing workgroup.
- C.2. The Department also recommends the use of the framework put forth by Converge supporting specific lines of inquiry for the additional work group sessions, as discussed in the Converge Report

D. SECURITY EXPERTS

Attachments

Minnesota Department of Commerce

Grid Data Sharing Report

November 2024

Prepared for the MN Department of Commerce
by Converge Strategies, LLC

Image Source: Minnesota Star Tribune

TABLE OF CONTENTS

1. INTRODUCTION

1.1 ABOUT CONVERGE STRATEGIES, LLC

Converge Strategies, LLC (CSL) provides consulting services focused on the intersection of clean energy, resilience, and national security. CSL's mission is to integrate resilience and security as first principles in the clean energy transformation. CSL provides project facilitation services, policy design and research, and market strategy development. CSL works frequently with the U.S. Department of Defense (DoD), the U.S. Department of Energy (DOE), the national laboratories, city and state governments, and a variety of private sector organizations.

1.2 ABOUT THIS EFFORT

In response to the Commission's 6/7/2023 Order Paragraph 6, CSL was hired to provide specialty services, conduct analyses and stakeholder engagement, and provide recommendations on privacy and security in the Commission's investigation. CSL's work began in August 2024 with a Grid Security Study that involved a thorough analysis of infrastructure security programs, policies, and reports at relevant Minnesota electric utilities and in other states to identify where grid information and data should be protected. These findings were then benchmarked against risk assessment frameworks and security plans, such as the Threat and Hazard Identification and Risk Assessment (THIRA) process, utility Integrated Resource Plans (IRP), and Emergency Operations Plans (EOP). CSL also reviewed national and state security reports to better understand the probability and severity of threats to the Minnesota electric grid.

CSL then conducted interviews with various stakeholders involved in the 20-800 Docket, including utility companies, developers, and Minnesota security offices, to gather their insight on the current status of grid data sharing. These stakeholders identified numerous security-related challenges in the data sharing process. Developers, for example, stressed the importance of accessing utility grid data to properly conduct distributed energy resource (DER) siting, and to facilitate the interconnection process. However, utility companies were concerned that developers lacked adequate cybersecurity measures to protect grid data from a potential breach. Utilities highlighted the possibility of malicious third-party actors gaining access to grid data and using it to attack infrastructure systems. CSL drew on these comments to inform a landscape analysis of grid data sharing practices, needs, and concerns.

The challenges identified during the interviews underline the need for a collaborative approach to developing a standardized data sharing process in Minnesota. The NARUC Grid Data Sharing Playbook was identified during work groups and interviews as an important resource to guide future discussions and provide possible solutions to grid data sharing. CSL analyzed this playbook and other grid data sharing frameworks to pinpoint potential areas of alignment for stakeholders.

This report addresses grid data and infrastructure security concerns related to DER implementation; explores the ongoing cyber and physical security risks to grid infrastructure and supply chain vulnerabilities; details the anonymized findings of the stakeholder interviews; and provides recommendations for the structure and content of future work groups. The report is structured as follows:

- **Section 2.** Cyber, physical security, and supply chain risks to grid infrastructure.
- **Section 3.** Anonymized findings of the stakeholder interviews.
- **Section 4.** Preliminary recommendations for improving the grid data sharing process.
- **Section 5.** Recommended discussion topics for ongoing stakeholder work groups.
- **Section 6.** Conclusion.

2. SECURITY RISKS TO THE ELECTRICITY GRID

The U.S. energy system faces coinciding climate, technical, and geopolitical challenges. The country is rapidly transitioning towards clean energy generation, transportation electrification, and the proliferation of internet-connected devices supporting grid automation, all at a time when the U.S. anticipates a period of unprecedented load growth[1]. Simultaneously, the increased frequency of severe weather events places energy systems at risk, while increasingly sophisticated threat actors seek to exploit the cyber and physical vulnerabilities of interdependent critical infrastructure. This foreboding threat landscape serves as a call to address infrastructure vulnerabilities as a national security imperative instead of treating them as a technical challenge. This report will focus on cybersecurity, physical security, and supply chain risk to help government and private sector stakeholders understand what drives risk, and how to address risk through targeted investment in physical and cyber infrastructure. Each section below includes a definition of the risk, an overview of the threat landscape, and examples of recent attacks.

2.1 CYBERSECURITY OVERVIEW

Cybersecurity focuses on deliberate attacks on Information Technology (IT) and Operations Technology (OT) that aim to disrupt the effective operation of the grid. These threat actors have varying degrees of capabilities, tactics, and potential for disrupting energy systems:

[1] Robert Walton, " U.S. electricity load growth forecast jumps by 81% led by data centers, industry," Utility Dive, last modified December 13, 2023, https://www.utilitydive.com/news/electricity-load-growing-twice-as-fast-as-expected-Grid-Strategies-report/702366/.

Description	Capabilities	Tactics	Grid Risk
HACKTIVISTS			
Individuals or groups who use disruptive tactics, such as denial of service attacks, for political, social, or ideological reasons.	Sophisticated techniques in highly specialized areas of malware. Limited knowledge of OT systems.	Emphasis on reputational impacts to organizations, which has limited implications for grid data.	Not known for actively targeting critical infrastructure owners + operators.
CYBERCRIMINALS			
Attackers who use cyber crime for financial gain, such as through ransomware attacks, fraud, or theft.	Mostly utilize readily available malware on "soft targets" with limited security. Limited knowledge of OT systems.	Opportunistic exploitation of vulnerabilities. Primarily interested in data as a means to secure ransom, not execute attacks.	Not known for actively targeting critical infrastructure owners + operators, however events like the Colonial Pipeline attack demonstrate potential consequences of malware attacks on IT or business systems.
NATION-STATE ACTORS			
Government-affiliated groups that use cyber espionage, disruption, or sabotage to target other nations.	Sophisticated techniques in highly specialized areas of malware, including a deep knowledge of OT and infrastructure systems.	Gain and maintain a presence in the IT or OT system of a critical infrastructure owner/operator with the intent of pursuing espionage.	Known for actively targeting critical infrastructure owners + operators.
INSIDERS			
Employees or associates who misuse their access to internal systems for personal gain, espionage, or sabotage.	Sophisticated techniques in highly specialized areas of malware, including a deep knowledge of OT and infrastructure systems.	Utilize their authorized access to data and OT systems to achieve success against current or former employers for personal or financial gain.	Potential for a successful attack is high, but severity is also limited based on the individual's access to systems and data.

Table 1. Overview of Cybersecurity Threat Actors' Capabilities, Tactics, and Risks

2.1.1 CYBERSECURITY THREAT LANDSCAPE

The 2022 National Defense Strategy (NDS) states that foreign adversaries such as the People's Republic of China (PRC) and Russia could "attempt to hinder U.S. military preparation and response in a conflict" by attacking our domestic critical infrastructure.[2] The 2023 Intelligence Community Threat Assessment echoes this point, stating that China would consider cyber operations against critical infrastructure "designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces."[3] Active targeting of U.S. critical infrastructure systems has already begun. CISA issued a warning in 2022 identifying multiple instances where Russian state-sponsored actors have targeted the operations and control systems required for real-time grid operations.[4] While there are no confirmed instances of cyber attacks successfully disrupting the delivery of electricity to customers of any U.S.-based utility, the risks continue to grow. In September of 2024, reports indicated that cyberattacks on U.S. utilities have increased 70% (1162 attacks) compared to 2023 and are expected to rise this year due to the presidential election.[5] Not only does the geopolitical environment increase the risk of cyber attacks, but increased automation and the presence of more hardware and software points of presence on the grid create a growing number of potential cyber attack points.[6] The following incidents highlight threat actors' ability and desire to access and disrupt networks:

Volt Typhoon. In 2023, DHS CISA issued a Cybersecurity Advisory identifying Volt Typhoon as a state-sponsored cyber actor of the PRC. Volt Typhoon employs "living off the land" techniques to hide their activity on networks by embedding or masking their communications in standard Windows system and network activities.[7] This tactic helps them evade endpoint detection and response products that would otherwise alert security personnel to their presence. This is a documented example of a foreign adversary conducting successful

---

[2] Department of Defense, *2022 National Defense Strategy of the United States of America* (Washington, DC: Department of Defense, 2022), https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

[3] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington DC: Office of the Director of National Intelligence, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

[4] "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," Cybersecurity and Infrastructure Security Agency (CISA), March 1, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-011a

[5] Seher Dareen and Srivastava Vallari, "Cyberattacks on US utilities surged 70% this year, says Check Point," Reuters, September 11, 2024, https://www.reuters.com/technology/cybersecurity/cyberattacks-us-utilities-surged-70-this-year-says-check-point-2024-09-11/#:~:text=To%20date%2C%20the%20attacks%20have,2023%2C%20Check%20Point%20data%20showed.

[6] Laila Kearney,"US electric grid growing more vulnerable to cyberattacks, regulator says," Reuters, April 4, 2024, https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/

[7] "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection," CISA, May 24, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

offensive cyber operations by pre-positioning themselves on IT neworks to enable lateral movement into OT assets to disrupt functions.

SolarWinds. The Russian Foreign Intelligence Service led a campaign of cyberattacks in September 2019, breaking into the computing networks of SolarWinds—a Texas-based network management software company. The software was widely used by the federal government to monitor activities and manage devices on federal networks. Hackers injected trojanized (hidden) code into verified SolarWinds software updates. When SolarWinds released the software updates to its customers, the threat actor gained a "backdoor," or remote access, to customers' networks and systems. The attack was discovered more than a year later in November 2020.[8]

Despite the evolving threats, continued efforts are underway to mitigate risks and improve cybersecurity protection standards at the federal and state levels of government, as well as improve best practices within critical infrastructure sectors. The CISA Cybersecurity Advisory Committee published a draft report to the CISA Director, determining that, "improving cyber defense can help shrink attack surfaces and reduce risk, but a focus on the resilience of critical entities and functions is ultimately necessary."[9] This finding would indicate that cyber protection is not enough by itself; it must be supported by risk-informed investment in infrastructure to ensure continued operation, even in a cyber-contested environment.

2.2 PHYSICAL SECURITY OVERVIEW

Physical security focuses on targeted attacks on physical grid assets, including generation, transmission, and distribution sites, with the intent of destroying equipment to delay or disrupt electric service. Similar to cybersecurity, the threat actors in this space have a broad range of motives, capabilities, and potential impacts:

[8] U.S. Government Accountability Office (GAO), "CrowdStrike Choas Highlights Key Cyber Vulnerabilities with Software Updates," GAO, July 30, 2024, https://www.gao.gov/blog/crowdstrike-chaos-highlights-key-cyber-vulnerabilities-software-updates

[9] CISA, *Building Resilience for Critical Infrastructure* (Washington DC: Department of Homeland Security, 2024), https://cyberscoop.com/wp-content/uploads/sites/3/2024/10/CISA-Cybersecurity-Advisory-Committee_DRAFT-Recommendations_20241011.pdf

Description	Capabilities	Tactics	Risk
VANDALISM			
Individuals or groups with the primary intent of obtaining valuable equipment or materials (i.e. copper).	Minimal resources, using readily available tools such as bolt cutters, crowbars, etc. Limited knowledge (if any) of infrastructure systems.	Target poorly protected assets, including remote, unmanned sites with ineffective physical barriers and no real-time monitoring.	Not motivated to create grid disruptions, any impacts to the grid are likely incidental.
DOMESTIC VIOLENT EXTREMISTS (DVES)			
Individuals who use unlawful violence to further political or social goals in the United States and act without foreign direction.	Primarily self-funded, with access to commercially available tools and weaponry.	Focused on "soft" assets, including remote, unmanned sites with ineffective physical barriers and no real-time monitoring; however, they are more willing to risk targeting a more protected site.	Act with intent to destroy or disrupt electricity service to bring attention to a social or political ideology or to discredit the government.
COORDINATED TERRORIST ATTACKS			
Individuals or groups equipped, trained, or funded by international terrorist organizations or hostile nation-states.	Well-funded and resourced with advanced technology capable of breaching even well-protected sites.	Utilize various sophisticated technologies (ballistics, explosives, drones) to execute coordinated attacks.	Highly motivated to degrade, disrupt, or destroy critical infrastructure to achieve a geopolitical objective or disrupt national defense functions.

Table 2. Overview of Physical Security Threat Actors' Capabilities, Tactics, and Risks

2.2.1 PHYSICAL SECURITY THREAT LANDSCAPE

The grid's vulnerability to direct physical attacks reflects an increasing trendline of DVEs targeting power systems in the past several years.[10] The U.S. power grid is suffering a decade-high surge in attacks as extremists, vandals, and cyber criminals increasingly aim for the nation's critical infrastructure.[11] Several attacks in late 2022 impacted more than 10,000 customers:

[10] Michelle J. Howard, "America's Aging Grid Threatens National Security. Here are Some Steps to Fix It," Utility Dive, January 24, 2024, https://www.utilitydive.com/news/aging-grid-threatens-national-security-reliability-cyber-threat-transmission/705362/
[11] Catherine Morehouse, "Physical Attacks on Power Grid Surge to New Peak," Politico, December 26, 2022, https://www.politico.com/news/2022/12/26/physical-attacks-electrical-grid-peak-00075216

- **North Carolina.** More than 36,000 people in the defense community around Fort Liberty in Moore County, N.C. lost power for multiple days after unknown attackers shot two Duke Energy substations in December 2022.[12]
- **State of Washington.** Four substations, owned by Tacoma Power and Puget Sound Energy, were attacked on Christmas Day 2022, causing a power outage for more than 14,000 customers and causing at least $3 million in damage.[13]

The rate of attacks is increasing, with a total of 1,665 security incidents involving the U.S. and Canadian power grids during 2023, including 60 incidents that led to outages. The number of attacks increased by 71% between 2021 and 2023.[14] This concerning trend highlights the fact that energy infrastructure is inherently difficult to physically secure, given the volume of assets that must be protected.

2.3 SUPPLY CHAIN VULNERABILITIES OVERVIEW

Supply chain attacks compromise both hardware and software assets that are essential to grid reliability. Of particular concern is the reliance on grid components produced and imported from foreign nations. Vulnerabilities in this category are almost always created by reliance on third-party companies who are contracted for service by electric utilities for use on their systems. Production of these assets resides outside of the security footprint of utilities and may require special technology or attention to detect vulnerabilities, presenting hidden risks that may not be exposed until a major security or operational disruption event. Additionally, the supply chain is impacted by the difficulty of obtaining specialty parts, making it costly and challenging to replace damaged equipment. These supply chain vulnerabilities further undermine grid resilience and security.

[12] Timothy Cama, "Who shot the North Carolina power grid?," Politico, December 5, 2022, https://www.politico.com/newsletters/power-switch/2022/12/05/who-shot-the-north-carolina-power-grid-00072235
[13]"Two charged with attacks on four Pierce County substations," U.S. Department of Justice, January 3, 2023, https://www.justice.gov/usao-wdwa/pr/two-charged-attacks-four-pierce-county-power-substations
[14] Catherine Morehouse, "Extremists keep trying to trigger mass blackouts — and that's not even the scariest part," Politico, September 10, 2023, https://www.politico.com/news/2023/09/08/power-grid-attacks-00114563

Description	Impacts
HARDWARE	
Physical assets, including routers, switches, servers, digital relays, and other devices are essential to maintaining the effective operation of IT and OT systems.	Compromise of these assets can come in the form of zero-day vulnerabilities (a security flaw in software or hardware unknown to the vendor or developer and for which there is no patch or fix available) or other vulnerabilities exploited by threat actors.
SOFTWARE	
Tools and applications developed by utilities or provided by third-party developers that are essential to maintaining the effective operation of IT and OT systems, including the Energy Management System (EMS), Supervisory Control and Data Acquisition (SCADA), operating system platforms such as Microsoft Windows, or security software programs.	The compromise, damage, or destruction of these components by cyber or physical means would likely cause grid outages and customer disruptions.
GRID COMPONENTS	
Physical assets on grid systems that are essential to reliable operation, including transformers, relays, insulators, busbars, conductors, and other components.	Can provide "backdoor" into grid systems, allowing for threat actors to monitor the grid to plan a cyberattack or modify grid operations (e.g. changing frequency). Replacement of these components following energy outage events can be slowed or stopped due to supply chain disruptions.

Table 3: Overview of Supply Chain Vulnerabilities and their Impacts

2.3.1 SUPPLY CHAIN THREAT LANDSCAPE

While the electric grid and the companies who own and operate grid assets are the targets of attacks, the same is true for the supply chain that supports hardware and software systems essential to grid operation, especially for materials that are not domestically produced. The result is vulnerabilities to reliable grid operations that are not under the direct control or purview of the operating utility. Recent examples highlight this vulnerability:

Crowdstrike. The 2024 incident began as a simple software update, but resulted in global impacts to Windows computers running their program, including those of critical

infrastructure owners/operators.[15] While the event did not result in any grid disruptions or outages, it highlighted the consequences of compromises to IT systems that are used by a substantial number of utilities and the potential for adversaries to target these providers as a means to attack critical infrastructure. While this event was not the result of an attack, CISA Director Jen Easterly stated that it was, "a useful exercise, like a dress rehearsal for what China may want to do to us."[16]

Nari Technologies. In December 2023, the United Kingdom's (UK) National Grid ended its contract with Nari Technologies, a Chinese state-owned electric components supplier. This was done at the request of the UK government's National Cyber Security Center who believe the smart grid components provided by the company are a cybersecurity risk to the UK grid.[17]

High-Voltage Transformers. The proliferation of foreign-made transformers in the U.S. heightened security concerns in 2019 when a transformer purchased by the Washington Area Power Administration was seized by the federal government and taken to Sandia National Laboratory. It is believed the government wanted to investigate the transformer for evidence of manipulated electronics or sensors that provide a "backdoor" for hackers to make changes to or monitor its operations to coordinate a cyber attack.[18]

These recent incidents underscore the connection between grid resilience, supply chain vulnerabilities, and the challenge of maintaining a secure, reliable grid. The risk mitigation strategies necessary to handle this challenge will require ongoing, proactive coordination between developers, suppliers, utilities, and government agencies to ensure the timely identification and remediation of potential vulnerabilities.

2.4 ELECTRICITY GRID RISK MITIGATION STRATEGIES

Each security vulnerability comes with a myriad of mitigation strategies. However, these mitigations all rely on timely, persistent access to data and information to conduct risk assessments, infrastructure and operational planning, and response to disruption events. Addressing these vulnerabilities will require state and federal energy, regulatory, emergency management, and homeland security agencies to collaborate with energy companies, technology providers, and security experts. Effective risk mitigation depends on

[15] David Jones, "CloudStrike software update at the root of a massive global IT outage," Cybersecurity Dive, July 19, 2024, https://www.cybersecuritydive.com/news/crowdstrike-microsoft-global-IT-outage/721874/

[16] Matt Kapko, "CrowdStrike snafu was a 'dress rehearsal' for critical infrastructure disruptions, CISA directors says," Utility Dive, August 12, 2024, https://www.utilitydive.com/news/crowdstrike-critical-infrastructure-resiliency-cisa/723832/

[17] Benedict Collins, "National Grid drops Chinese tech supplier over cybersecurity fears," Energy Central, December 18, 2023, https://energycentral.com/news/national-grid-drops-chinese-tech-supplier-over-cybersecurity-fears

[18] Llewellyn King, "How America's Power Grid Is Vulnerable to Undetected Cyberattack," Forbes, January 28, 2021, https://www.forbes.com/sites/llewellynking/2021/01/28/how-the-supply-chain-in-heavy-bulk-power-equipment-is-vulnerable-to-undetected-cyberattack/

public-private partnerships enabling information sharing, identifying security best practices, and coordinating responses to cyber, physical, and naturally occurring threats. These efforts should emphasize standardization and regulation to establish security baselines for the electric sector. Additionally, a process of continuous improvement must match the evolving threat landscape where security practices are regularly evaluated and updated to address new risks and vulnerabilities.

3. LANDSCAPE ANALYSIS

CSL conducted a series of interviews with stakeholders involved in the 20-800 Docket to understand their perspectives on data use and grid data sharing as well as their existing internal policies and processes. In total, eight stakeholder groups were interviewed, including all regulated utilities under the PUC's jurisdiction, several solar developers, and multiple Minnesota security groups. The increased focus on grid data sharing, pursuant to the Commission's order, enabled CSL to have productive discussions with interviewees. CSL and the Commerce Department welcome additional engagement from interested parties that have not participated in this effort thus far.

Stakeholders agreed that risks to the grid are real and expressed a mutual interest in developing a data access process that supports decision-making while maintaining grid protections. They also agreed that a statewide standard for data classification, requests, and disclosure would help limit confusion, ensure data protection, and streamline the data request process. There was consensus that a tiered approach to data protection and access is desirable for all parties despite the challenges of implementation. Additionally, utilities and developers both pointed to the NARUC Grid Data Sharing Playbook as a good starting point for discussions around existing internal policies and how they can be more broadly applied or developed into a statewide standard. Specific concerns of each stakeholder group included:

- **Utilities.** Utilities are responsible for the collection, use, and storage of grid data utilized by generation, transmission and distribution asset owners and operators. As the stewards of grid data, utilities are seeking a better understanding of what data grid developers need to site, design, and construct their projects. They expressed concerns about attributing responsibility in the event of a data breach, which they believe should fall on the data requester. Most utilities have internal risk processes to guide policies on data categorization and sharing.
- **Developers.** Developers described robust internal processes for using detailed grid data to guide DER development. The quality and accuracy of the outputs of these modeling and planning systems depend on the inputs, which is why access to data is so important. Without the proper data, developers cannot effectively assess the costs of interconnecting generation assets. In their view, they have yet to receive a satisfying explanation of the security risks cited by utilities, and would like to be included in conversations about the specific risks posed by "adversaries".
- **Minnesota Security Groups.** Security groups typically work with government and private sector stakeholders to classify data according to information sharing processes developed by the DHS or law enforcement agencies such as the Federal Bureau of

Investigation (FBI). Stakeholders from these groups indicated that handling requests for utility data at the state level would be challenging due to the variety of technical capabilities and policy/legal constructs needed to support sharing and protecting data. They support risk mitigation, access controls, checks, and auditable processes.

The interview findings highlight the importance of improved collaboration between utilities, third-parties, and security experts to adequately address grid risk. The Solar Energy Industries Association (SEIA) has emphasized a similar finding, noting that, "there are many different cybersecurity frameworks that organizations use, but without an industry-wide approach, some organizations will remain vulnerable to attacks that could jeopardize others operating on the grid."[19] The same is true for the lack of a grid data sharing framework and the importance of developing an industry-wide approach that protects the grid while also providing the data required for DER deployment.

Additional themes from the stakeholder interviews are summarized in the sections below.

3.1 DATA SHARING CONCERNS

Bottom Line Up Front (BLUF). More specificity around grid data sharing concerns and existing internal tools is required to adequately address stakeholder concerns and develop a framework that can be applied across the state.

Challenge. Some utilities shared concerns about misinterpretation of provided data, and highlighted that improving their understanding of the data that developers need to execute projects can help utilities provide the correct data and limit the risk of misinterpretation. Developers had the opposite concern, noting that they prefer to do their own analyses rather than relying on utility summaries. Developers have a high level of trust in the robust internal GIS systems they have built for DER development, which draw on both publicly available data like Google Maps and on utility data provided through required Federal Energy Regulatory Commission (FERC) pre-application reports. Some utilities have developed internal DER screening tools that could potentially be adapted to provide the requested information without exposing underlying data. Utility representatives also cited the cost of providing grid data, which is borne by ratepayers, as a reason for limiting data requests to only essential information.

Potential Path Forward. Additional discussions about use case development, risk and vulnerability identification, and data classification are necessary to develop a data request

[19] Solar Energy Industries Association, " Securing Our Solar Future: How Clean Energy Can Be the Most Cybersecure, Reliable Technology on the Grid,"*Solar Energy Industries Association* (blog), December 10, 2021, https://seia.org/blog/securing-our-solar-future-how-clean-energy-can-be-most-cybersecure-reliable-technology-grid/

process that provides adequate data while considering incremental data risks and costs. Additionally, improved understanding of the internal tools used within organizations can help (a) provide the right data inputs and (b) alter internal tools to be external facing and share findings without sharing underlying data.

3.2 DATA REQUEST PROCESSES

BLUF: Currently, the data request process varies from utility to utility, requiring developers to follow a different process based on the service territory.

Challenge: Interviewees highlighted that different utilities receive vastly different numbers of data requests and implement different data collection protocols, meaning that smaller utilities might not collect all of the information sought by developers. Utilities that receive fewer data requests handle them on a case-by-case basis and provide "white glove" service to data requesters, whereas utilities that handle a larger volume of requests have more established internal processes. Utilities expressed a preference for sharing access to data via data hosting on their internal systems without transferring the data itself to a third party. This method of sharing data could help reduce risk and expedite data request timelines.

In order to site renewables and conduct cost-benefit analyses, developers rely heavily on the FERC-required pre-application reports, through which utilities provide site-specific data under non-disclosure agreement (NDA). Stakeholders agreed that the use of NDAs for DER requests is standard practice and developers did not take issue with NDA requirements. However, developers indicated that pre-application reports are less useful for exploratory studies or siting storage facilities, both of which require supplemental information. Additionally, pre-application reports do not provide information about required system upgrades triggered when exceeding the "upgrade threshold" for a grid component. Without this information, it is difficult for developers to complete a cost-benefit analysis for upgrading the component to accommodate a new project.

Potential Path Forward: Both utilities and developers could benefit from a more standardized data request process. Any grid data sharing framework should seek to balance developers' data requirements with utilities' concerns about data protection. For example, a data request template agreed upon by stakeholders could streamline the process for developers and help utilities better understand what information is critical for developers to complete their projects.

3.3 RISK ASSESSMENT PROCESSES

BLUF: Utilities each use unique internal risk assessment and data classification processes to develop internal policies around data protection and sharing. The lack of third-party visibility into these utility-specific processes leads to confusion around risk classification.

Challenge: There is no standard risk assessment process employed by all government and private sector stakeholders, and utilities are reluctant to speak at length about their internal risk assessment processes due to the sensitivity of proprietary processes. This results in a lack of clarity around how risk is evaluated and how data is classified. Developers indicated that specific risks associated with certain grid data could be better articulated and that it is unclear why discussing risks is itself a risk. Stakeholders want to participate in discussions about the types of attacks being imagined by adversaries.

Utilities use their internal data categories such as public, protected, confidential, and confidential-restricted to protect data from unauthorized disclosure. This is allowable under the Minnesota Distributed Energy Resources Interconnection Process (MN DIP), which states that, "Confidential Information shall mean any confidential and/or proprietary information provided by one Party to the other Party that is clearly marked or otherwise designated 'Confidential'."[20] The MN DIP also states that, "if requested by either Party, the other Party shall provide in writing the basis for asserting that the information warrants confidential treatment." However, unlike the numerous established data designations described in section 4.2, the threshold for designating utility data at a certain level is unclear. While utility categories may give direction on who may access data within each tier, the classification methodology is typically not shared. There is an overall lack of transparency around the specific criteria a data set must meet to be designated at each level. For tiered data classifications to be applied more broadly or included in a statewide framework, there must be additional clarity on the types of vulnerabilities that warrant classification at the higher levels as well as clear communication to developers as to what data is shareable and what data they cannot access.

Potential Path Forward: Identifying a forum where utilities and developers can comfortably engage in discussions about risk types is critical to establishing a mutual understanding of the incremental risks posed by specific grid data types.

[20]Minnesota Public Utilities Commission, *State of Minnesota Distributed Energy Resources Interconnection Process (MN DIP)* (St Paul, MN: Minnesota Public Utilities Commission, 2024), https://mn.gov/puc/assets/MN%20DIP%20updated%20by%204.15.24%20Order%20Clean_tcm14-623149.pdf

4. RECOMMENDATIONS FOR IMPLEMENTATION

A successful data sharing process depends on the implementation of several policies and processes to streamline data requests, screen and verify personnel, protect data from unauthorized or accidental disclosure, and maintain trust between stakeholders. Previous grid data sharing efforts, such as the NARUC Grid Data Sharing initiative, highlight the importance of security and provide an effective baseline for state-specific adaptation and implementation of the NARUC Playbook. Current practices have not delved deeply into specific threats, risks, and potential impacts as a means to understand the importance of grid data for informing policy and regulation.[21] This section provides preliminary recommendations for implementation of a secure and effective grid data sharing program for Minnesota.

4.1 RISK ASSESSMENT

The type and severity of risk is driven by a variety of factors, and a clear articulation of risk categorization is needed to support the grid data sharing process. The disparity in risk assessment methods utilized by government and private sector stakeholders presents a challenge for determining the best means to share data. The relative risk associated with a data set is a reflection of the degree to which it provides insight or capability to disrupt or degrade electric service. However, access to data alone does not provide threat actors with the ability to conduct successful attacks on cyber or physical systems. The sophistication of security tools and protocols, as well as the levels of physical and operational redundancy built into the electric grid, serve as effective mitigants. Additional clarity is needed to better understand the relative sensitivity of data risk as a function of several variables:

- **Granularity.** Grid data is not a one-size-fits-all, and risk varies based on the volume of data as well as the level of detail requested. Detailed data on a small segment of the grid (feeder level or below) is not automatically a high risk if there are no critical assets on that feeder or it is the only feeder from which data is requested. Similarly, detailed data on a larger section of the grid could still have moderate risk if it is aggregated or anonymized.
- **Means of Access.** The manner by which requested grid data is provided, stored, and utilized has a bearing on the level of risk. Potentially sensitive data that is shared under controlled circumstances (i.e. on a utility-hosted portal with controlled access) poses lower risk than data that is provided electronically and stored by the requester (see section 4.3).

[21] "Grid Data Sharing," National Association of Regulatory Utility Commissioners (NARUC), accessed March 26, 2024, https://www.naruc.org/core-sectors/energy-resources-and-the-environment/electric-vehicles/grid-data-sharing/.

- **Associated Infrastructure.** The electric grid is designed to maximize reliability through redundancy and flexibility. Operational risk is largely a reflection of the potential for important assets, or "nodes" on the Bulk Electric System (BES) to experience failures. A high-voltage transmission substation poses a greater risk to the overall system than a smaller distribution substation. Even detailed data can be lower risk if it is associated with a small distribution feeder, while small amounts of data that apply to critical BES assets can present a high risk. Categorizing data relative to grid scale can provide valuable context to risk assessments.
- **Classification.** Clear and accurate classification of grid data is an essential component of the risk assessment process, as it helps guide risk identification, requirements for handling/sharing, and access protocols commensurate with the sensitivity of the requested data. See section 4.2 for an overview of the multiple data classification criteria that exist among stakeholders, and section 4.3 for recommendations on how a "crosswalk" approach can help determine equivalencies between the categories.

4.2 DATA IDENTIFICATION AND CLASSIFICATION

There are numerous existing models for indicating the sensitivity and shareability of certain data across various government and private sector entities:

- **Federal Government.** The most well-known federal data classification scheme is the Classified, Secret, and Top Secret designations, which are assigned based on the potential damage to national security (see Figure 3).
- **Critical Energy Infrastructure Information (CEII).** CEII is another federal designation specifically for critical infrastructure information that is not classified national security information. CEII includes details about the production, generation, transmission, transportation, or distribution of energy and is exempt from disclosure under the Freedom of Information Act (see Figure 1).
- **Additional Federal Designations.** There are other federal designations, like the DHS Traffic Light Protocol (TLP), that are not official classification schemes and are not exempt from disclosure. TLP has four designations (clear, green, amber, amber+strict, and red) to ensure that sensitive information is shared with the appropriate audience, but is primarily intended to promote frequent and effective collaboration (see Figure 2).
- **North American Electric Reliability Corporation (NERC) Designations.** NERC has designations like Critical Infrastructure Protection (CIP) and the Bulk Electric System Cyber System Information (BCSI). CIP is a cybersecurity framework for securing critical infrastructure in the bulk power system. BCSI includes information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat.

- **State Designations.** The State of Minnesota has its own data classification tiers (i.e., Public, Private, and Confidential) (see Figure 4).

Each classification process has criteria for categorizing data at specific levels. Additional details for each classification model can be found in Appendix A.

4.3 TIERED ACCESS AND DISCLOSURE

A tiered access process for vetting individuals and organizations requesting grid data can minimize the risk of sharing it. Similar to data and information classification, multiple sets of criteria are currently used by government and private sector organizations to facilitate this process. A more uniform approach is needed to streamline requester validations, reduce risk, provide adequate data protections, and reduce the burden on utilities to fulfill requests. A framework should address the following aspects of tiered access:

Vetting Process. Validating the people and organizations requesting data is currently completed at the discretion of the data owner. The data sharing process can be improved by identifying additional means for confirming the eligibility of individuals to receive and handle sensitive information. Reviewing current state processes for security clearances through agencies such as DHS, DoD, and DOE can help identify equivalent credentials to streamline the process (e.g. a DoD security clearance holder is authorized to access specific data).

Legal Protections. Organizations utilize NDAs to address the terms of compliance for information disclosure and the consequences associated with intentional or accidental release of protected, sensitive, or proprietary information. Developing an NDA template for grid data sharing in Minnesota would clarify and align the requirements for accessing and sharing data across the utilities, developers, and state agencies.

Access and Storage. The transmittal and storage of data is an important risk driver because security controls are difficult to maintain as information moves between organizations and IT systems. The data classifications identified in section 4.2 should correspond to how requesters access, transmit, and store data. For example, several controls can be utilized to reduce or eliminate unauthorized sharing, including:

- Granting temporary access to a utility-hosted portal
- File sharing with embedded, password-protected encryption
- On-site data sharing (requester can visit the utility in person to review data)
- Cloud-based data hosting with credentialed access

The method(s) used by utilities should be considered when determining the overall risk of data sharing.

4.4 DATA REQUEST PROCESS

Across the utilities, there are multiple different web- or paper-based request processes that third parties must follow. A standard Grid Data Request Template would provide clarity and consistency to third-party requesters while improving the predictability and uniformity of the requests received by utilities. A consistent template will help limit unnecessarily broad data calls by ensuring the specificity of requests, increase efficiency and reduce the time required to respond to or fulfill requests, and reduce the labor burden on all parties. A Minnesota Grid Data Sharing Framework should include the development of a Grid Data Sharing Template that addresses the following topics:

- Risk category/tier of the data being requested for expedited sorting by the receiver based on pre-assigned criteria
- Credentials of individual(s) seeking access which reflects the identified risk tier
- Acknowledgment of data protection and handling requirements, including the penalty for non-compliance commensurate with the classification equivalent for the data requested
- A clear articulation of the proposed use of the data
- Timeline for the data sharing process, including the duration of the review period and the length of time the requester will have access to the data

The template should be compatible/compliant with all legal and regulatory requirements for all parties.

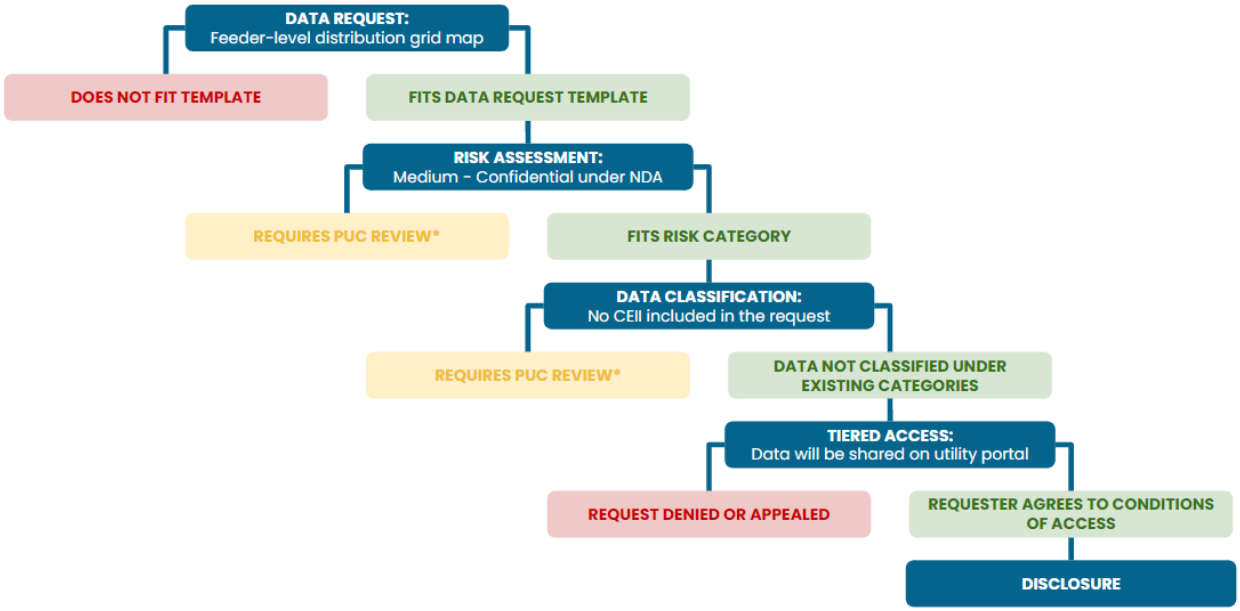
4.5 USE CASE DEVELOPMENT

Developing use cases to test the efficacy of the Grid Risk Data Sharing Framework will help stakeholders understand how individual requests are reviewed, how risk is evaluated, and how a sharing/disclosure decision is made. Future working groups should develop a series of use cases to demonstrate and evaluate the proposed process and recommend refinements. The text and figure below provide an example of how requests can be reviewed using the recommendations described in the previous sections:

- **Data Request.** The case is reviewed based on the granularity of the data requested and the associated infrastructure. For example, a request for a feeder-level distribution grid map (granular) could be considered high risk; however, if no critical infrastructure is

included on the requested map and the map is limited to a small geographic area, the risk would be reduced.

- **Classification.** If the request includes information protected under an established program (e.g., CEII or TLP), then the associated risk of disclosing this data is higher. In the example, no CEII information is requested, indicating low risk.
- **Tiered Access.** If the requester lacks established security clearances from sponsoring agencies or the industry equivalent, they could be considered a higher risk. Risk, however, can be reduced to a low level if information is protected from intentional or accidental disclosure using measures such as NDAs or accessing data through utility-hosted portals.
- **Risk Assessment.** In the example below, a request was made for a feeder-level distribution map for specific feeders that do not contain critical infrastructure or CEII information. Risk is further mitigated by only allowing access to the data through the utility's hosted portal. These combined factors reduce the risk of this data request to a moderate level, indicating that an NDA is sufficient to protect and access this data.



*The PUC could be asked to weigh in if the data does not fit within a predetermined risk type or data classification OR where there are disagreements between utilities and data requesters as to the proper classification of data.

Figure 1: Example of Feeder Level Data Request and Sharing Process

5. RECOMMENDATIONS FOR THE STAKEHOLDER WORKING GROUP

In the interviews, stakeholders expressed a shared interest in developing a data sharing process that provides the right amount of data while maintaining appropriate protections, as well as a desire to build a mutually beneficial relationship between developers and utilities. A Commission-hosted working group (referred to here as the "Stakeholder Working Group") could help achieve these goals. The Stakeholder Working Group should focus on adapting the NARUC Grid Data Sharing Playbook to suit Minnesota's specific data sharing needs.

On September 17, 2024, Xcel Energy submitted an Ex Parte Communication Report, outlining a proposed roadmap for the Stakeholder Working Group.[22] The roadmap consists of thematic discussions addressing the NARUC Playbook process over three meetings. The proposed topics for discussion are:

- **Use Case Establishment.** Determine the importance of a grid data point in accomplishing a requester's goals by creating narrative descriptions of specific scenarios.
- **Data Protection Capabilities**. Mitigate risk by understanding the cybersecurity capabilities of data requesters' systems to reduce the likelihood of data breaches.
- **Data Sharing Mechanisms.** Identify methods that can streamline the data request process.

Specific recommendations on the goals and topics that could be covered during the Commission-hosted Stakeholder Working Group meetings are described in detail below. The recommendations are informed by insights from the research and policy analysis process, as well as from stakeholder interviews.

5.1 USE CASE ANALYSIS WORKSHOP

Observation. In the Ex Parte Communication Report on September 17, 2024, Xcel Energy proposed discussing use case establishment with developers during the September workgroup. The request was framed as a firm prerequisite for further discussions on the NARUC Playbook process, specifically data protection and sharing. The goal of this conversation was to identify common data needs across Minnesota developers.[23] In the interviews, some stakeholders emphasized the importance of use case development and developers provided their reasoning for requesting each data point.

[22] Christian Noyce, *RE: Permissible Ex Parte Communications Pursuant to Minn. Rules, Part 7845.7400* (St Paul, MN: Department of Commerce, 2024), https://efiling.web.commerce.state.mn.us/edockets/searchDocuments.do?method=showPoup&documentId={60270192-0000-CB12-A693-29EA0CFBCE4D}&documentTitle=20249-210261-01

[23] Christian Noyce, *RE: Permissible Ex Parte Communications Pursuant to Minn. Rules, Part 7845.7400*

Recommendation. The use case analysis meeting should identify commonalities and differences in how developers use specific data points. Specifically, stakeholders should discuss how they use the data (e.g. to understand sizing or placement of assets). These findings can later be used to inform a standardized data request process, where predetermined data sets are automatically authorized to be distributed to developers upon meeting other conditions.

5.2 DATA PROTECTION CAPABILITIES ANALYSIS WORKSHOP

Observation: Utility companies shared concerns about third-parties' ability to secure and protect data shared with them. Some utilities use internally managed data hosting platforms to share data with developers, allowing them to provide or revoke access at any time. This risk mitigation measure can reduce the potential for data leaks or breaches by allowing the utility to maintain positive control over their data. However, developers expressed confidence in their data storage policies and cyber security measures, noting that they do have the ability to protect sensitive data received from utilities. Overall, stakeholders lack understanding of each other's data practices.

Recommendation: The data protection capabilities workshop should cultivate a mutual understanding of the risks associated with sharing certain data types. The first step is for stakeholders to discuss their current data protection measures and identify gaps and best practices. Stakeholders should then determine criteria for categorizing data based on the level and type of risk. These criteria should include considerations for potential uses or the data as well as the general availability of the data (e.g. whether the information is easily found on Google Maps). For example, the location of distribution lines feeding a hospital would not be considered high risk because although the facility is critical, the information is easily found online or seen while driving. Stakeholders should also consider how access requirements tied to the data category/risk level can further strengthen data security. For example, determining that the risk associated with residential energy use data can be reasonably mitigated by requiring the requester to sign an NDA.

5.3 DATA SHARING MECHANISMS WORKSHOP

Observation: In the stakeholder interviews, utilities noted both the cost of providing grid data, which is borne by ratepayers, and the risk of data requesters misinterpreting utility information. They also expressed a preference for sharing access to data via a utility-hosted portal. On the other hand, developers pointed to the varied data request processes across

the different utilities and the lack of access to certain data that is required to adequately plan and analyze DER development.

Recommendation: This workshop should focus on identifying shared priorities, concerns, and capabilities around data needs and access. In particular, stakeholders should analyze commonalities in the utility data request processes to develop a standardized request process. Stakeholders should also discuss criteria that determine who may access which data tiers based on the data set's associated level or type of risk. The workshop should result in framework concepts that address stakeholder concerns and enhance grid data accessibility through a standardized data sharing process.

6. CONCLUSION

Three key themes appeared consistently throughout stakeholder interviews and the policy analysis:

Threats to the grid are real, but they are surmountable. The grid faces growing risks from cybersecurity threats; physical security vulnerabilities; and complex supply chains of hardware, software, and grid components, exacerbated by the increasing frequency and severity of extreme weather events. Organizations cannot adequately address these risks alone, and there is a lack of public and private sector collaboration. This causes underinvestment in infrastructure, which is a more significant driver of risk to the grid than the sharing of grid data or potential access by malicious actors.

Understanding how risk is assessed impacts grid operation and infrastructure investment. Public and private sector stakeholders identified ways in which risk informs investment in technical solutions that reduce the likelihood and impact of potential grid disruptions. However, the lack of transparency in the risk assessment process and the articulation of risk should be addressed through collaboratively-developed policies and processes.

Grid data sharing is essential to improving grid reliability and resilience. Grid data sharing can provide insight into how infrastructure hardening, redundancy, and additional electric generating capacity can address vulnerabilities.

An ongoing Stakeholder Working Group will help stakeholders adapt the NARUC Grid Data Sharing Playbook into a Grid Data Sharing Framework for Minnesota. The Commission should ensure this working group addresses the open comments associated with this docket, particularly those concerning grid data use, protection, and sharing. The recommended meeting structure in this report allows conversations to build on one another, generating support among stakeholders through collaboration. The use case development discussion will inform discussions on risk assessment, data protection, and tired access. To maximize the effectiveness of the working groups, meetings should have clear goals, adequate time for detailed discussions, and metrics for success. In conclusion, creating a Stakeholder Working Group that utilizes the NARUC Playbook to address data sharing concerns is crucial to solving the challenges raised in this docket.

7. APPENDIX

7.1 FIGURE 1

Critical Energy Infrastructure Information (CEII)		
	Definition	**Access**
PUBLIC	-	Public has unrestricted access in public reference room and on eLibrary
CEII (NONPUBLIC)	Information about proposed or existing critical infrastructure that: (1) is exempt from disclosure under FOIA, (2) relates to the production, generation, transportation, transmission or distribution of energy, (3) could be useful to a person planning an attack on the infrastructure, and (4) does not simply give the location of the critical infrastructure.	Public may file a CEII request under 18 C.F.R. §388.113 or a FOIA request under 18 C.F.R. §388.108
PRIVILEGED (OTHER NONPUBLIC)	This is usually confidential business information or cultural resource reports submitted under 18 C.F.R. §388.112.	Not maintained through Public Reference Services or on eLibrary except as an indexed item (i.e., no public eLibrary image) Public may file FOIA request under 18 C.F.R. §388.108

7.2 FIGURE 2

	Department of Homeland Security Traffic Light Protocol (TLP)
Clear	Disclosure not limited
Green	Limited disclosure, restricted to the community
Amber	Limited disclosure, restricted to participants' organization and its clients
Amber + Strict	Limited disclosure, restricted to participants' organization
Red	Not for disclosure, restricted to participants only

7.3 FIGURE 3

U.S Government Classification			
Uncontrolled Unclassified Information	Information that is neither classified nor CUI, but is still subject to agency public release policies	Public Information	Information that is not controlled or classified, but that agencies must still handle in accordance with Federal Information Security Modernization Act (FISMA) requirements
		Federal Contract Information (FCI)	FCI is not intended for public release. It is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government
Controlled Unclassified Information ("CUI")	Sensitive information that does not meet the criteria for classification but must still be protected	CUI Basic	A subset of CUI for which there are no specific handling or dissemination controls
		CUI Specified	A subset of CUI whose underlying authority has specified something different or extra is required for that type of information (e.g., limited distribution, additional protections, etc.)
Classified Information	Information that the United States government has determined needs protection from unauthorized disclosure for national security reasons	Confidential	Data that could cause damage to national security if released
		Secret	Data that could cause "serious" damage to national security if released
		Top Secret	Data that could cause "exceptionally grave" damage to national security if released

7.4 FIGURE 4

Data Classifications under the Minnesota Government Data Practices Act (MGDPA)		
Data on Individuals	Public	Public data is accessible by anyone. The MGDPA provides that, unless specifically authorized by statute, a government entity may not require persons to identify themselves, state a reason for, or justify a request to gain access to public government data.
	Private	Private data on individuals is data classified by statute or federal law as not public but accessible to the individual subject of that data.
	Confidential	Confidential data on individuals is data made not public by statute or federal law and is inaccessible to the subject of that data.
Data not on Individuals	Nonpublic	Nonpublic data is data not on individuals that a statute or federal law makes not accessible to the public but accessible to any subject of that data.
	Protected Nonpublic	Protected nonpublic data is data not on individuals that is neither public nor accessible to the subject of that data.

CERTIFICATE OF SERVICE

I, Sharon Ferguson, hereby certify that I have this day, served copies of the following document on the attached list of persons by electronic filing, certified mail, e-mail, or by depositing a true and correct copy thereof properly enveloped with postage paid in the United States Mail at St. Paul, Minnesota.

Minnesota Department of Commerce
Comments

Docket No. E999/CI-20-800

Dated this **12th** day of **November 2024**

/s/Sharon Ferguson

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
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
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
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
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
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
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