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

March 4, 2026

RE: IN THE MATTER OF A COMMISSION INVESTIGATION ON GRID AND CUSTOMER SECURITY ISSUES RELATED TO PUBLIC DISPLAY OR ACCESS TO ELECTRIC DISTRIBUTION GRID DATA

DOCKET NO. E999/CI-20-800

Dear Mr. Seuffert,

Converge Strategies, LLC (CSL) is pleased to submit these recommendations in response to the Minnesota Public Utility Commission's (the Commission's) February 7, 2025 Order in Docket No. E999/CI-20-800.

CSL provides consulting services at the intersection of resilience and national security, with a mission to integrate these as first principles in grid evolution. Engaged by the Department of Commerce, CSL facilitated the three workshops outlined in Order Point 6 and developed recommendations for a process to securely share distribution grid data with interested parties.

These recommendations are informed by stakeholder input gathered across the three workshops—documented in the included After Action Reports (Appendices A, B, and C)—and by CSL's professional expertise in energy security, stakeholder convening, and process design. Stakeholders were given opportunities to review and provide feedback on each session's AAR and on a draft of these recommendations; that feedback has been incorporated where appropriate, factual, and within scope. This report therefore reflects areas of general alignment identified through the workgroup sessions, but does not represent unanimous agreement or incorporate topics not discussed during the workshops.

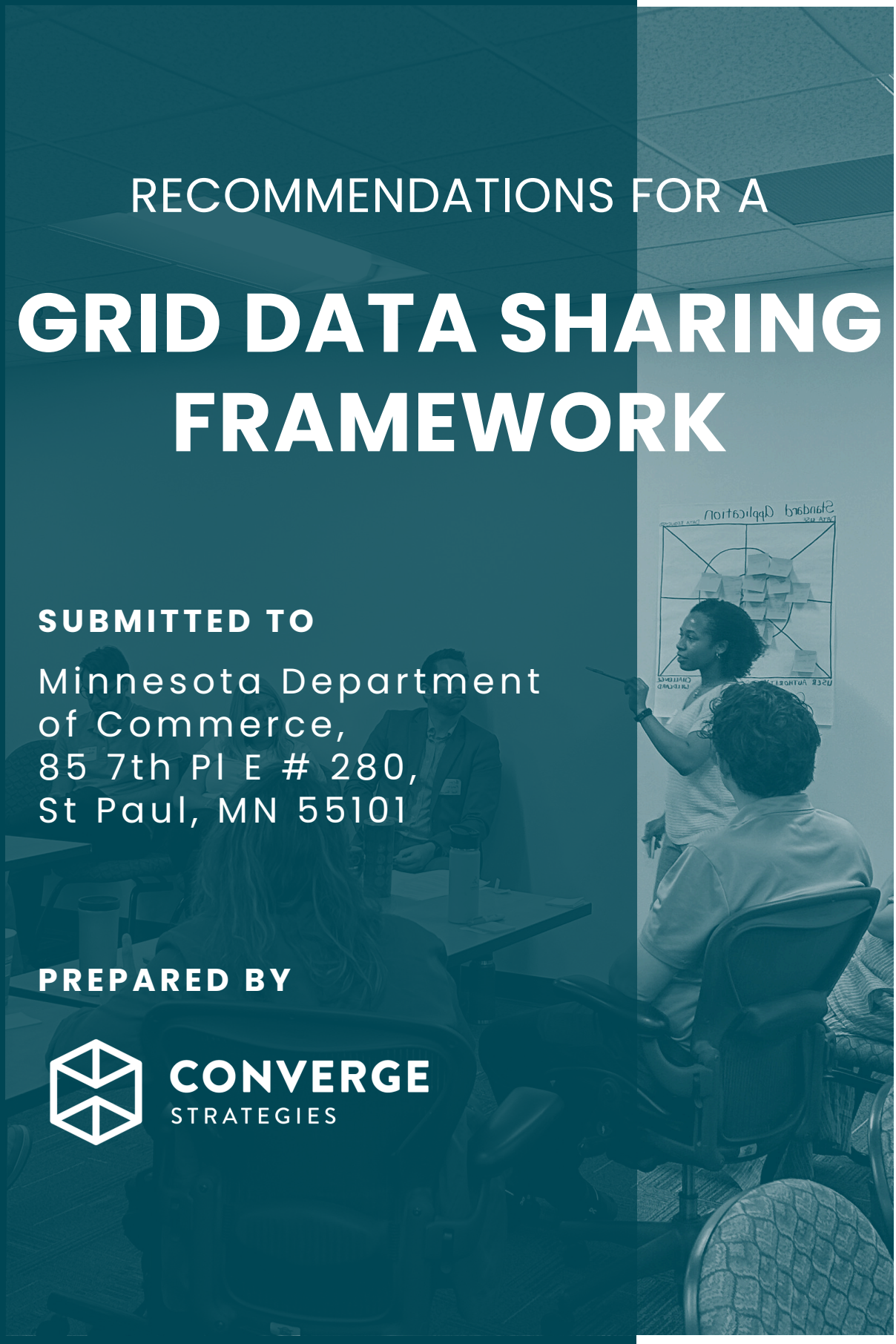
CSL appreciates the partnership with the Minnesota Department of Commerce and the time and thought that all involved parties contributed to this effort. We look forward to answering any questions the Commission may have.

Sincerely,

Wilson Rickerson
President and Co-Founder
Converge Strategies, LLC
50 Holbrook Street
Boston, MA 02130
(202) 875-2201

RECOMMENDATIONS FOR A

GRID DATA SHARING FRAMEWORK



SUBMITTED TO

Minnesota Department
of Commerce,
85 7th Pl E # 280,
St Paul, MN 55101

PREPARED BY

CONVERGE
STRATEGIES

MARCH 2026

Page intentionally left blank

ABOUT CONVERGE STRATEGIES, LLC

Converge Strategies, LLC (CSL) provides consulting services focused on the intersection of 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 DoD, the U.S. Department of Energy (DOE), the national laboratories, city and state governments, and a variety of private sector organizations.

ACKNOWLEDGEMENTS

This report was commissioned by The Minnesota Department of Commerce.

Converge Strategies would like to thank the following organizations for their participation in the three workgroup sessions that preceded this report. This document benefited from their input and feedback:

- Citizen's Utility Board
- Clean Energy Economy Minnesota (CEEM)
- Dakota Electric Association
- Fresh Energy
- Minnesota Attorney General's Office
- Minnesota Bureau of Criminal Apprehension/MN Fusion Center
- Minnesota Department of Commerce
- Minnesota Information Technology Services (MNIT)
- Minnesota Power
- Minnesota Public Utilities Commission
- Minnesota Solar Energy Industries Association (MnSEIA)
- Nokomis Energy
- Otter Tail Power
- R Street Institute
- U.S. Solar
- Xcel Energy

TABLE OF CONTENTS

ACRONYMS

APT	Advanced Persistent Threat
BCA	Bureau of Criminal Apprehension
CAO	Consumer Affairs Office
CEII	Critical Energy Infrastructure Information
CEUD	Customer Energy Use Data
CHS	Criminal History Search
FERC	Federal Energy Regulatory Commission
GSWG	Grid Security Working Group
HCA	Hosting Capacity Analysis
IT	Information Technology
MCRO	Minnesota Court Records Online
MGPDA	Minnesota Government Data Practices Act
NARUC	National Association of Regulatory Utility Commissioners
NDA	Non-Disclosure Agreement
NERC	North American Electric Reliability Corporation
NRC	Nuclear Regulatory Commission
ODAS	Open Data Access Standards
PACER	Public Access to Court Electronic Records
PDF	Portable Document Format
PTO	Paid Time Off
PUC	Public Utilities Commission

1.0 INTRODUCTION

1.1 ABOUT THIS EFFORT

Following Xcel Energy's 2019 Hosting Capacity Analysis (HCA) Report (Docket No. E002/M-19-685), the Minnesota Public Utilities Commission's ("Commission") July 2020 order directed the creation of a docket to address concerns around the electrical distribution grid and customer data security. Between July 2020 and June 2023, there were several rounds of comments, culminating in the Commission's June 2023 order establishing a working group. This working group met during a series of workshops from July to September 2024, to develop the record more fully and look at data sharing models from other states and utilities.

During these meetings, the working group made progress on individual data details, but were unable to come to full agreement within the timeframe provided by the Commission. However, parties agreed to continue working on these details and recommended that the Commission establish a formal working group and that the NARUC Grid Data Sharing Framework Playbook (released in November 2023) ("Playbook") should guide further discussions.

The Playbook is a comprehensive, flexible framework designed to help state regulators and stakeholders navigate and articulate the complexities, benefits, challenges, and tradeoffs of sharing electric grid data. It aims to balance the pursuit of diversified energy portfolios with the risks to grid security, by helping utility commissioners and interested parties in determining what grid data to make public and how to share it appropriately without prescribing a rigid, "one process fits all states" plan. It does not serve as a step-by-step planning document, and each utility commission is encouraged to follow a regulatory process that fits its needs.

In summer 2024, Converge Strategies was hired to facilitate a collaborative stakeholder approach to implementing the NARUC playbook in Minnesota, pursuant to Commission Order Point 3 in the Commission's February 2, 2025, order in Docket No. E-999/CI-20-800. Commerce's intent was for Converge to focus on the three topical considerations from the NARUC Playbook: data details, potential impacts, and data sharing. To that end, in 2024, Converge reviewed infrastructure security policies and risk assessment frameworks, researched cyber and physical security risks to grid infrastructure and supply chain vulnerabilities, conducted interviews with stakeholders involved in the docket to gather insight on the current status of grid data sharing, and provided recommendations for the structure and content of future workgroup sessions.

Converge wrote a report ("Minnesota Commerce Grid Data Sharing Report") on those efforts and submitted it to the Commission for an open comment period in November 2024. The Commission accepted the report in February 2025, and directed the workgroup to complete three workshops on *Data Protection Capabilities*, *Data Sharing Mechanisms*, and *Use Case Analysis*. The Commission additionally ordered the workgroup to craft a standardized data request template and provide recommendations for a process for securely sharing the minimum necessary data for DER interconnection.

In summer 2025, Converge led stakeholders through a series of three workshops to inform a standard grid data sharing framework for Minnesota:

- **Data Protection Capabilities.** Focused on developing data protection categories and criteria for categorizing data based on level and type of risk.
- **Data Sharing Mechanisms.** Focused on developing a structure for a standardized data request process based on best practices.
- **Use Case Analysis.** Focused on validating the data sharing framework developed in previous workshops by developing use cases of sample grid data requests.

The drivers of these discussions and the overall effort were the fundamental changes in the security landscape for electrical systems over the last several years. As evidenced by advisories and alerts from U.S. intelligence agencies, Advanced Persistent Threat (APT) actors (sophisticated hackers, often backed by nation-states) are increasingly targeting the technologies and control systems that operate electrical grids, and these observed activities over the past several years are the primary driver of these discussions in Minnesota. Federal partners, including the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency, have issued numerous advisories for the domestic power grid, focusing on Industrial Control System vulnerabilities, threats from nation-states, and domestic extremism, and urging operators to adopt stronger cybersecurity benchmarks.

For state Commissions, data security for the distribution systems within their jurisdiction is not simply an IT concern as it directly impacts their core regulatory mandate to ensure safe, reliable, and efficient electric service for customers. If highly sensitive grid data falls into the wrong hands, malicious actors could identify vulnerabilities and leverage them to plan and execute targeted attacks that cause wide-spread outages, or exploit weak points to cause disruption during critical events.

A successful attack on grid infrastructure could leave millions of customers without power for extended periods, undermining the fundamental reliability obligation that the Commission is charged with enforcing. At the same time, parties outside of utilities (e.g. developers, academic organizations) have legitimate uses for grid data, such as research, adding new capacity resources, building infrastructure, and adding energy services to the grid. These contributions support Minnesota's energy policies and the needs of customers at a time when grid investment is essential to meeting the challenges of customer load growth, and frequent impacts of extreme weather. Therefore, careful consideration of what grid data to share publicly, and how to share it safely, has become essential to maintaining the secure and reliable electric service that customers depend on daily while upholding the principles of free and fair open markets predicated on both service providers and customers having full, immediate, and equal access to relevant data (e.g., prices, qualities, costs, and capacities) needed to participate in the market.

1.2 RECOMMENDATIONS OVERVIEW

The recommendations in this document are intended to inform decisions by the Minnesota PUC and are based on information gathered from stakeholders during the three workgroup sessions described in Section 2.0 *Workgroup Sessions Summary* and the corresponding After Action Reports (Appendices A, B, and C) as well as further evaluation of these using Converge's professional expertise in energy security issues, convening stakeholders groups,

and designing new and innovative processes. In addition to the open invitation to all utility and energy developer stakeholders in Minnesota to attend the three workgroup sessions, stakeholders were provided with opportunities to review and submit feedback and corrections on each session's respective After Action Report and on a draft version of these recommendations during the following times:

- July - August 2025
- August - September 2025
- October - November 2025
- January 2026

That feedback has been incorporated where appropriate, factual, and within scope of the docket. Therefore, this report reflects areas of general alignment identified through the workgroup sessions, but it does not always represent unanimous agreement among all participants or incorporate topics or options not discussed among all attending stakeholders during the workgroup sessions.

This report does not address or provide recommendations on the following topics, as they were outside the scope of this effort, as stipulated by the docket. Any authority, deliberation, or decision made regarding them lies with either the Minnesota PUC, the Department of Commerce, or the relevant state agency or legislative authority:

- Estimated costs for implementation.
- How or by whom costs should be covered.

Converge's recommendations focus on the development of a standardized data request template and a modular request and review process with built-in optionality that, if implemented, will support more secure, transparent, rapid, and consistent grid data sharing practices in the state. The report is structured as follows:

- **SECTION 2.0.** Workgroup Sessions Summary
- **SECTION 3.0.** Grid Data Sharing Framework
- **SECTION 4.0.** Application Appeals Process
- **SECTION 5.0.** Timeline
- **SECTION 6.0.** Addressing State and Federal Regulations
- **SECTION 7.0.** Conclusion
- **APPENDIX A.** July 2025 After Action Report
- **APPENDIX B.** August 2025 After Action Report
- **APPENDIX C.** October 2025 After Action Report

2.0 WORKGROUP SESSIONS SUMMARY

2.1 WORKGROUP SESSION 1: DATA PROTECTION CAPABILITIES

On July 7, 2025, the Minnesota Department of Commerce ("Commerce") convened stakeholders for an in-person workgroup session focused on developing grid data risk categories and establishing or defining the appropriate corresponding criteria and protections. A total of 23 participants—representing 12 Minnesota state offices, utilities, non-profit organizations, and private energy infrastructure developers—attended the session, which was facilitated by Converge.

During this session, participants discussed:

- How to define and evaluate the level of risk associated with sharing grid data.
- Appropriate protection mechanisms for data of varying risk levels.
- Criteria for assigning a risk level to a particular data set (e.g., what criteria must be met in order to label something as "high risk").

During small and large group discussions, stakeholders coalesced around three risk tiers—low-, medium-, and high-risk data—on which to build the framework. Stakeholders also raised questions about several topics, some of which are discussed below:

Public and Non-Shareable Data. Stakeholders were concerned about how publicly available data and non-shareable data (e.g. state or federally protected data) would be treated in the framework. It was eventually decided that both were outside the scope of the task. The Minnesota Grid Data Sharing Framework will not recategorize data that falls under existing classifications that prohibit sharing, and currently publicly available data that does not require protection measures and controls. As such, this framework will only focus on providing the methods to identify, assess, and categorize data into the low-/medium-/high-risk tiers described above.

Personally Identifiable Information (PII). Utilities have an obligation to protect PII, prompting concerns about how it would be addressed. However, this issue is also out of scope, as it is addressed in Docket No. E,G-999/CI-12-1344 (*In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities*).

Formal Process for Disputes. Participants acknowledged that even with clearly defined risk levels and criteria, there may be circumstances where data owners (i.e., utilities) and requesters are not aligned regarding the risk level assigned to a data request. The process and venue to resolve these disputes—which include the option of referring the issue to the PUC—should continue to be discussed both within and outside of the workshop series.

For a complete overview of Workgroup Session 1, please see *Appendix A*: *Data Protection Capabilities After Action Report*.

2.2 WORKGROUP SESSION 2: DATA SHARING MECHANISMS

On August 11, 2025, Commerce convened stakeholders for a second in-person workgroup session, focused on developing a proposed structure for a standardized data request process. A total of 24 participants—representing 12 Minnesota state offices, utilities, non-profit organizations, and private energy infrastructure developers—attended the session, which was facilitated by Converge.

During this session, participants discussed:

- Prerequisites to submitting a data request application.
- Information that should be included in a standard data request.
- Reasonable timelines for data request application review.
- How denied applications and appeals should be handled and the potential role of state agencies in that process, based on existing legislative rules.

Attendees were encouraged to consider what a state-wide, standardized data request process could look like. The following application hallmarks emerged:

Pre-Application Process. This discussion centered around what steps, if any, prospective requesters should take before submitting a data request application to simplify and expedite the process. There was general agreement that all parties requesting data should pass some form of a background check to confirm their identity in order to be eligible to request and receive data. A detailed example of what this can consist of is addressed below in Section 3.1 *Background Check.*

Building a Standard Application. Participants discussed having a statewide standard request template concept and identified the information that is essential to help utilities evaluate risk in a more uniform and transparent manner as they receive requests. Essential information for any data request broadly included:

- Who was requesting the data (including any other individuals, such as coworkers or contractors who would need to handle the data);
- A clearly articulated need;
- The defined data type (e.g. equipment, load, capacity);
- Validation of a passed background check; and
- The length of time the requester would need access to the data in order to fulfill their requirements.

Timeline. While the timeline for reviewing and fulfilling a request may be impacted by the risk level of the requested data and the complexity of the request, participants agreed that a general guideline of three months, or 90 days, is a maximally reasonable amount of time for a utility to complete their review of an application. Due to the emphasis on communicating clearly and consistently, secure data sharing, and appropriate data control, some participants suggested developing a portal or tracker through which requesters can monitor progress on their request and utilities can share data.

Appeals Process. Participants agreed that a denied request should be accompanied by clear, criteria-based reasoning and an invitation for further discussion. They also agreed that a formal appeals process should be a last resort, and that utilities and requesters should make every good-faith effort to resolve disputes without escalation. However, a need was seen for an official, state-mediated appeals process for extreme situations.

For a complete overview of Workgroup Session 2, please see *Appendix B: Data Sharing Mechanisms After Action Report.*

2.3 WORKGROUP SESSION 3: USE CASE ANALYSIS

On October 6, 2025, Commerce convened stakeholders for the last of three in-person workgroup sessions. It focused on validating and refining the data sharing framework developed in Workgroup Sessions 1 and 2, by developing use cases based on sample grid data requests to test the process. A total of 23 participants—representing 12 Minnesota state offices, utilities, non-profit organizations, and private energy infrastructure developers—attended the session, which was facilitated by Converge.

During this session, participants discussed:

- Use cases (scenarios) that tested the Grid Data Sharing Framework draft outcomes form Workgroup Sessions 1 and 2.
- Areas of convergence and divergence in the Grid Data Sharing Framework draft.

Attendees were encouraged to treat the use cases as an opportunity to test the draft Grid Data Sharing Framework and clarify what factors and mitigations would cause risk levels to the system to increase or decrease, while considering the suitability and feasibility of data protection measures.

Key takeaways from the discussions are summarized below:

Business Agreements are Essential. Stakeholders agreed that all data-sharing should be accompanied by a business agreement (e.g. NDAs, data sharing agreements), but that different kinds of agreements may be more appropriate than others, depending on the situation.

Appropriate Risk Drivers. Participants agreed that, for the purposes of the Grid Data Sharing Framework, the risk level of requests should be evaluated based on risks to security, the integrity and reliability of the distribution grid, and public safety. Risks related to corporate and business operations were deemed out-of-scope for this effort.

Mitigation Options are Dynamic. There is rarely a single mitigation that will effectively protect shareable data. Rather, the mitigation options are flexible, scalable, and can be layered depending on the risk level of the request.

Vetting is Essential. To ensure the safety and reliability of the grid, it is critical that requesters—both individuals and organizations involved—be vetted.

Secure Sharing Methods. Secure sharing and storing of data becomes challenging to assess and keep consistent when requesting entities have differing capabilities. Participants agreed that a secure portal could be the safest, most uniform method of sharing data.

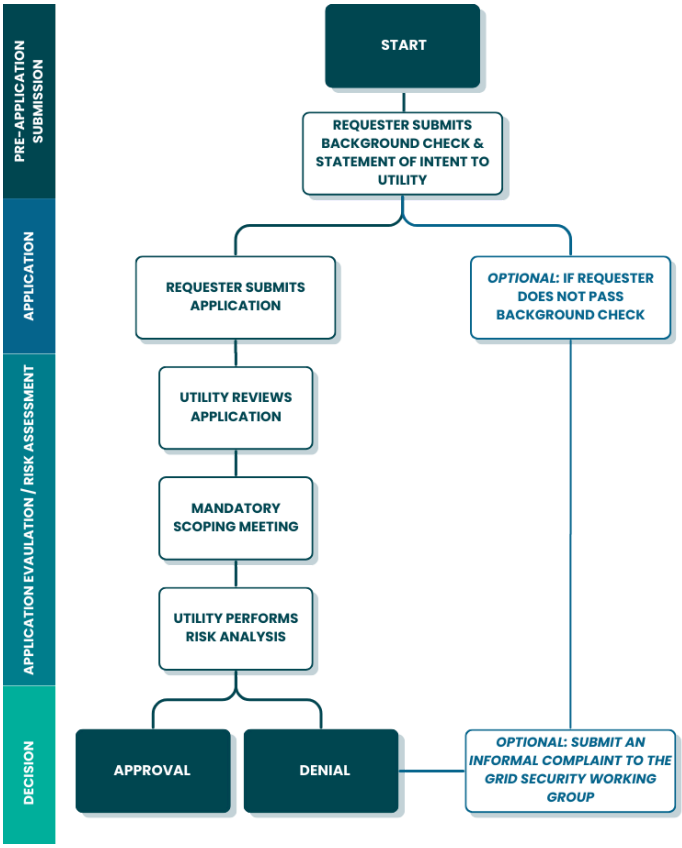
Details Matter. Amongst other things, the granularity of requested data, the number of years requested, and the intention of a requester to make the data or conclusions drawn from the data public in the form of a report or derivative product all have a significant impact on risk level.

For a complete overview of Workgroup Session 3, please see *Appendix C: Use Case Analysis After Action Report.*

3.0 RECOMMENDED GRID DATA SHARING FRAMEWORK

This section presents Converge's recommendations for a framework for protecting and securely sharing the distribution grid data consistent with elements of the NARUC Grid Data Sharing Playbook. The recommendations reflect collective insights from stakeholders that were gathered across the three workgroup sessions discussed above combined with our own expertise. To provide a modular, flexible approach that can be tailored to each unique data request and varying utility and requester capabilities, optionality is offered at various decision points throughout the Grid Data Sharing Framework to allow the Commission to make decisions regarding which options are most suitable for Minnesota. *Figure 1: Grid Data Sharing Framework* below shows the process at a high level.

Figure 1: Grid Data Sharing Framework



As depicted in *Figure 1*, there are four main steps of the framework, which are discussed in sub-sections 3.1 to 3.4 below:

- Section 3.1: Pre-Application Verification
- Section 3.2: Application
- Section 3.3: Risk Analysis
- Section 3.4: Securely Sharing Data

Figure 1 also shows places where requesters may logically choose to challenge a utility's decision. This is further discussed in Section 4.0, *Application Appeals Process*.

3.1 PRE-APPLICATION VERIFICATION

Because non-public distribution grid data is sensitive and could cause harm to the grid and society if used maliciously, it is important that all individuals and organizations requesting data be vetted to limit the risk posed by the requesting individual or organization. To reduce burden on all parties, we recommend that this be completed before the requester submits an application and contain only two components: a statement of intent and a background check. This step in the process, while important, is not meant to be overly burdensome in terms of time and should take no more than two weeks to complete (see *Section 5.0 Timeline* for our full recommendation on the timeline of the entire process).

Statement of Intent

The purpose of the statement of intent is to notify the utility in question that the requester intends to submit an application, pending passage of a background check. Additionally, it can serve as the initiation of the background check and related paperwork, depending on the method the utility uses (see below).

We recommend this be templatized and available as an electronic form (e-form) or a PDF the requester can complete and submit to a utility-specified email address. The use of a template promotes equality and efficiency in the data request process by ensuring requesters have similar or equal experiences and expectations when engaging with utilities, regardless of their own or the utility's size and capabilities.

Further, this form and its content should be determined by the PUC for use in this process. Converge recommends this form be kept simple, so as to not pose a barrier to entry, and cover information such as:

- Contact information (e.g., name, organization, etc.)
- Statement of why data is being requested (e.g., project type, research, etc.)

Background Check

A background check should be completed for the individual making the request, in addition to ancillary personnel who may handle the data (e.g. contractors, student workers, other third-party organizations or personnel), and the organization(s) the individual is making the request on behalf of (if applicable). The primary objective of this step is to confirm there are no impediments to continuing this process. For individuals (i.e., those unaffiliated with an organization), the background check should verify their identity and that they do not have

criminal records or personal concerns that could pose a security risk. A reasonable level of scrutiny to pass would be the same level required for employment by the utility the requester is applying to; however, further specifics of this check, or an increased level of scrutiny, should be determined by the PUC. For companies, the background check should confirm that: there are no ties to or ownership by foreign entities of concern; poor financial history, such as bankruptcy; or a history of significant cybersecurity incidents (e.g., causing excessive financial or operational damage to the company).

Below are two methods utilities could implement for obtaining a background check on requesters: verified third parties or publicly available resources. For equality of experience, procedural consistency within the state, and security, Converge recommends that the Commission choose one method.

Verified Third Parties. Many utilities have contractual relationships with verified third parties for purposes such as performing background checks on prospective employees. Providing a list of these vendors on the utility website for requester utilization would be simple, and the utility would know that the background check is coming from a legitimate source. If this option is chosen, the requester(s) must indicate that the results of the background check should be shared with the utility they are intending to request data from.

Publicly Available Resources. There are two ways utilities could use publicly available resources to conduct a state-level background check on prospective requesters: a no-fees, self-service limited search; and a more comprehensive, fee-based request through the Minnesota Bureau of Criminal Apprehension (BCA).

Utilities could perform the no-fees background check using internal resources, but there are limitations on the data and time period covered. Further, a comprehensive check must be constructed from multiple sources, such as the Minnesota Public Criminal History Search (CHS), Minnesota Court Records Online (MCRO), and for a more thorough search, local and federal sources (e.g. Public Access to Court Electronic Records [PACER]).

Utilities could also request a complete criminal history from the BCA. This would involve submitting a formal request, notarized consent from all individuals involved in the request, and paying a nominal fee. This process provides a more comprehensive report, including both public and private criminal history data. Federal records can be included in the BCA check but only if specifically authorized by law for certain purposes.[1]

Should utilities feel the background check information is insufficient and would like to conduct further investigation into applicants (e.g., for the purposes of analyzing risk), they should feel empowered to do so. Whichever option utilities employ, they should be sure to follow all state and federal rules and regulations concerning background checks and apply the methodology consistently. For transparency, the background check process and all relevant resources should be clearly stated and provided on the utility's website and preapplication instructions.

[1] Minnesota Department of Public Safety, Bureau of Criminal Apprehension, "Background Checks," accessed October 29, 2025, https://dps.mn.gov/divisions/bca/bca-divisions/criminal-justice-information-services/background-checks.

3.2 APPLICATION

The application itself should be simple, not overly burdensome for requesters to fill out, and provide information essential to the utility's initial review, scoping meeting (described in Section 3.3) preparation, and risk analysis (see Section 3.3 *Risk Analysis* below). To that end, we recommend that the following information be collected:

Who. The individual making the request, the organization they are making the request on behalf of (if applicable), other individuals who will handle the data (e.g. coworkers, contractors, student workers), and type of user (e.g. developer, academic researcher, non-profit, etc.).

Data Request. Detailed information about the type of data being requested, the time period of interest (e.g. 2020, 2021-2023), and the geographic footprint of interest (e.g. a single transformer, a list of diffuse transformers, a list of concentrated transformers, etc.).

Why. A written explanation of the project and end product the data will be used for. This should be sufficiently granular so the intent and scope are clear without requiring an overly burdensome amount of detail. It is important to note that the 'why' should serve to help utilities understand what data will ultimately be helpful or informative to requesters, not for use in an evaluation of a proposed project's merits.

For process uniformity and consistency, we recommend templatizing the form and making it available through an e-form or a PDF the requester can download, fill out, and submit to the appropriate utility using whatever application method is used by the utility at the time of adopting the data sharing framework process (i.e., using utility-specified email address or website).

3.3 RISK ANALYSIS

The risk analysis portion of the process should consist of three stages: preliminary review, scoping meeting, and risk analysis. Each stage is discussed below.

Preliminary Review

When a utility receives an application from a fully vetted requester, they should review it for completeness and prepare for the scoping meeting (described below in this section). If the application is not complete, the utility may return it to the requester with a clear explanation of why it is being returned and what steps should be taken before resubmission.

With a complete application, the utility should identify the following:

If the Request Includes Data That Is Out of the Grid Data Sharing Process Scope. This includes data that is either publicly available at the time of the request,[2] or data that can

[2] Data that is already provided publicly may include public information currently provided in Integrated Distribution Planning dockets; public information currently provided in Safety, Reliability, and Service Quality dockets; information currently provided on publicly available hosting capacity/outage maps; information currently provided under existing MN-DIP procedures (with and without NDA requirements that should be considered and retained).

never be shared due to state or federal policies (i.e., "unallowable data").[3] Whether the request consists entirely or partially of these data types, the utility should inform the requester prior to scheduling the scoping meeting. In the case of publicly available data being requested, the utility should immediately direct the requester to where that information can be found so they can access it. In these instances, a scoping meeting would not be needed unless the request also asks for non-public data. In the case where unallowable data is requested, the utility must inform the requester regarding what regulatory policies are affecting them and offer to work with the requester to find alternative data points or types.

If the Request Includes Data That Is Regulated by State or Federal Policies. In instances where the data type, format, or amount are within the scope of the Grid Data Sharing Process but are also regulated by state or federal policy, the utility should review the relevant policy for data sharing guidelines and apply it accordingly. If state or federal policy dictates that data needs to be protected or presented in a certain way, this must be clearly communicated to the requester during the scoping meeting and in writing. A non-exhaustive list of examples of such policies can be found in Section 6.0, *Addressing State and Federal Regulations*.

If the Data Being Requested Is Not Collected by the Utility at That Time. In the event that data requested is of a type not collected by the utility, is not maintained in the requested format, or would require additional system analysis in excess of existing efforts at the time of request, the utility cannot be compelled to create, collect, or reformat the data. However, the utility must notify the requester of the situation prior to scheduling the scoping meeting and offer to work with them to find an alternative solution.

If a Different Data Set May Be More Appropriate. If the utility believes this to be the case, it should be discussed during the scoping meeting.

Aspects of the Request That Require Clarification. These gaps should be discussed during the scoping meeting.

Scoping Meeting

The scoping meeting is an opportunity for the utility and the requester to have open dialogue about the request, including the points discussed above and any additional information that is needed for the utility to perform a risk analysis. The utility's objective should be to understand the request so they can ask clarifying questions and suggest appropriate alternatives if they believe a different data set or alternative solution would better meet the requester's needs. The requester's objective should be to help the utility understand their needs and be open to alternatives. Parties should communicate in good faith, so the most appropriate and least-risk data sharing option can be agreed upon.

[3] Due to state and federal policies and regulations, there are certain kinds of data that will never be shareable under any circumstances. These policies and regulations are out-of-scope of this workgroup and the data request process and include DCEI/CEII/PCII, National Security Information, information categorized at TLP:AMBER and above, Nuclear Restricted Data as per 10 C.F.R. §95.5. Nuclear Safeguards Information as per 10 C.F.R. §73.2., "Trade Secret" and "Security" information as defined and controlled as per Minn. Stat. 13.37.

Risk Analysis

Once the scoping meeting is complete, the utility should have enough information to perform a risk analysis, determine the data request's risk level (i.e., low, medium, or high), and determine what mitigations and release criteria will sufficiently protect the data. The results of the risk analysis should be clearly communicated to and shared with the requester, regardless of the request being approved or denied. This should include any policy- and/or regulatory-based justifications for the risk-level classification, as well as mitigations and release criteria that will be applied. The requester may ask clarifying questions, which the utility should make every good-faith effort to answer.

The three risk levels and appropriate mitigations and release criteria are outlined below. As previously stated, data that is publicly available at the time of the request and data that can never be shared due to certain state or federal policies exist outside this process and are not categorized or addressed below.

Low-Risk

Definition. Low-risk data is unlikely to cause disruptions or degradation of the grid that would cause significant harm to infrastructure and society, without significant data aggregation efforts or other prior non-public knowledge. Data in this category does not offer enough visibility into the system to reveal physical or cyber vulnerabilities of assets or information about individual customers.

Examples. Historical data. Peak load, and load shape at low granularity and/or at discrete sites.

Medium-Risk

Definition. Medium-risk data carries the risk of limited potential impacts to the system and people (e.g. short duration or localized disruptions). It may offer some visibility into system vulnerabilities but not to a level that could result in significant harm to the distribution grid and society. It can also be the result of specific points or types of aggregated data that would be normally categorized as low-risk, either in the single request or in a series of requests from an individual or organization over a period of at least three years.

Examples. Areas with enhanced resiliency measures or limited redundancy. Peak load, and load shape for a diffuse area. Aggregated distribution system capacity data. Substation ratings.

High-Risk

Definition. High-risk data is anything that could result in the grid being harmed, significantly degraded, or destroyed, resulting in operations being disrupted on a societal-level. Data in this category reveal specific physical or cyber vulnerabilities of assets or information about individual customers that is critical to security, economic security, public health or safety, or any combination thereof. In Minnesota, these are referred to as Priority End Users, which can

include law enforcement, firefighting units, and emergency medical services.[4] It can also be the result of specific points or types of aggregated data that would be normally categorized as medium-risk, either in the single request or in a series of requests from an individual or organization over a period of at least three years.

Examples. Any data that is considered operational data. Load-flow model data. Bulk electric system data. 8760 models.[5]

Mitigations and Release Criteria

Mitigations and release criteria are flexible, scalable, and can be layered, appropriate to the risk level of the specific request. The list below outlines the appropriate options for protecting shared distribution grid data. Utilities can decide which of these measures are appropriate, given the risk level of a specific use case.

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

If this list needs to be amended in the future to respond to shifts in the security landscape, or to account for changes in authority, policy, or technology, we recommend that the new or amended measures be developed and agreed upon by the Grid Security Working Group (GSWG), discussed in detail in Section 4, *Application Appeals Process*. This ensures the data sharing environment in the state remains procedurally equal for all stakeholders involved.

3.4 LEAST-RISK DATA SHARING

In addition to the mitigations and release criteria listed above, utilities should also choose a secure sharing method that best fits their capabilities and is appropriate for the data request. Below are three methods of securely sharing data.

Portal

Secure portals are commonly used by industries that regularly handle and share sensitive information—such as finance, healthcare, and law—because they offer significant advantages over other methods, such as email and file sharing. Security-focused advantages can include end-to-end encryption, centralized document management, audit

[4] *HF3315, 89th Leg., Reg. Sess.*, 2016, https://www.revisor.mn.gov/bills/89/2016/0/HF/3315/versions/0/pdf/#:~:text=6.12,6.29.

[5] 8760 models are hourly, year-long simulations used in energy analysis (365 days x 24 hours). Using actual weather data and operational schedules, they simulate an energy system's performance for every hour of the year, including energy use, operating costs, and renewable energy generation estimates.

trails, and technologies to prevent printing and screen-sharing. These features make complying with legal requirements for data protection easier and reduce liability associated with sending sensitive files. Other advantages include the ability to share large files that email cannot accommodate.

In the case of sharing grid data, a secure portal could mitigate concerns like data viewing versus data possession, ensuring data is properly destroyed, and enforcing data access time limits. It could also simplify sharing and signing documents such as NDAs, attestations, and data sharing agreements. Some utilities may prefer to use a portal for all grid data sharing—regardless of risk level—in order to maintain consistency and efficiency in their internal processes, handle large data files, and reduce overall risk and liability.

Email Encryption

Email encryption protects the confidentiality and integrity of information by converting it into a format unreadable to anyone who is not the original recipient(s). This ensures that data remains private and secure from unauthorized access. An example of an encryption method is a digital signature, which ensures that the email is authentic and has not been compromised. Email encryption also protects server backups of the email in question, ensuring long-term protection.

However, this method offers limited control—after the email is sent, the sender cannot revoke access. Additionally, the overall effectiveness of email encryption relies on the security of the recipient's email account, which the sender has no control over. There is also no audit trail created with email encryption, meaning there is no record of who has viewed, downloaded, or shared the data. There are also technical considerations to consider, such as the compatibility of different email platforms and the size of the files being shared, as well as equity concerns, as reading encrypted emails can require specific software, plug-ins, or key management for end-users.

Utilities may decide that email encryption may be appropriate, depending on the particular situation at hand.

In-Person Viewing

In-person viewing of data is conceptually straightforward—the requester goes to the utility's office, looks at the data, conducts analysis in the moment, and leaves, taking no physical utility-provided documents with them.

When deciding if this is the most appropriate method for securely sharing data with a requester, the utility should take into consideration whether or not it is appropriate for the requester's project needs. For example, the requester might not be able to conduct on-the-spot analysis, or may be unable to travel to the utility office to view the data. Additionally, the time commitment required for all parties should be considered. Requesters may need to view data for an extended period of time (e.g., six hours) and may need multiple visits to properly conduct analysis (e.g., returning to their office to adjust assumptions, calculations, or models and repeat the process). This means the utility would need to dedicate significant personnel hours and other resources to facilitate this.

4.0 APPLICATION APPEALS PROCESS

Currently, complaints related to grid data sharing requests may be filed with the Consumer Affairs Office (CAO). Due to the technical nature of distribution grid data and grid security, we recommend following the alternative appeals process outlined below.

If a requester believes their application has been unfairly categorized or denied, they should make a good faith effort to resolve the dispute with the utility. However, if a mutually satisfactory resolution cannot be reached and the requester still believes their request has been unfairly categorized or denied the Grid Security Working Group (GSWG)—here proposed as a subcommittee of the Distributed Generation Working Group (DGWG)—is the body with whom it is most appropriate to file informal complaints.

The ideological genesis of the GSWG was first established by the Commission's June 7, 2023, Order in Docket No. E-999/CI-20-800. The Order delegated authority to the Executive Secretary to convene the appropriate parties in a work group and develop the record around frameworks for securely sharing appropriate grid data more fully. The Commission's February 7, 2025, Order in the same docket established the body as an ongoing workgroup under the Commission's authority to address matters associated with the efforts discussed within these recommendations. This makes the GSWG the ideal forum for receiving informal complaints related to the grid data sharing process going forward.

If a requester chooses to file an informal complaint with the GSWG, the following information must be provided:

- The complete application originally filed with the utility, including what data is being requested and the project it will support;
- The reasoning the utility gave for their decision;
- Documentation of what steps of the Grid Data Sharing Process have been taken; and
- Explanation of what attempts at resolution have been made by the parties involved.

If asked by the GSWG, the utility should be prepared to provide or elaborate on their policy-based reasoning for their classification or denial of a request.

After reviewing the situation, the GSWG will gather the parties to resolve the issue. If no resolution is reached, the complainant may file with the CAO under current standards. Then, the Commission may either dismiss the matter if there is no reasonable basis on which to proceed, send the matter to the Court of Administrative Hearings for Mediation, or create a contested case.

All parties in this Grid Data Sharing process have the right to file an informal complaint with the GSWG, or a formal complaint with the CAO at any time. However, there are logical places in the process for complaints to occur (indicated in *Figure 1*: *Grid Data Sharing Framework*), and an informal complaint should be considered an action of last resort, in order to prevent administrative burden on the GSWG, the CAO, and the Commission.

5.0 TIMELINE

Establishing a clear, realistic timeline for the overall Grid Data Sharing Process and the individual steps within it is important for effective implementation. A reasonable overall timeline for completion of a request—from background check initiation to fulfillment of data request—is two months. Within those two months, the response to the Pre-Application should take no more than two weeks; the initial review of the application and scheduling of the scoping meeting should take less than two weeks; and the Risk Assessment and fulfillment of the request should take no more than 30 days. *Figure 2: Process Timeline* below depicts this.

While utilities should make every good-faith effort to resolve requests in an efficient and timely manner, we recognize that some requests may take longer due to their complexity or the need to facilitate engagements with the Commission. Additionally, normal activities (e.g., utility employees taking PTO, medical, or family leave, and natural staff turnover) and fluctuating volumes of requests, could impact the timeline. These circumstances should be clearly communicated to the requester, along with a reasonable estimated time of completion.

Regardless, this suggested timeline is meant to set time-based goals and expectations for utilities when navigating this process. However, if timelines become extended, for reasons that are not—or are not demonstrably not similar to—the ones discussed above (e.g., total unexplained lack of communication at any point during process, inflexibility in scheduling meetings that can be a means to block progress, etc.), then the appeals process discussed in Section 4 should be used by the aggrieved party.

Figure 2: Process Timeline

6.0 ADDRESSING STATE AND FEDERAL REGULATIONS

Electricity grid data is governed by state and federal regulations. In Minnesota, the Commission regulates policies pertaining to rates and services to ensure safe, reliable, and affordable service. The Minnesota Department of Commerce, Division of Energy Resources is responsible for regulating and planning the state's energy programs, promoting reliable and affordable energy, managing emergency energy planning and recovery efforts, and advocating for customers in utility proceedings. On the federal level, the Federal Energy Regulatory Commission (FERC) regulates the interstate transmission of electricity, wholesale sales, and hydropower projects, while the Department of Energy sets national policy and collects national energy statistics.

Each of these entities creates rules, regulations, and policies, some of which protect certain types of data and dictate how and if data can be shared. In instances where a data request

is impacted by a state or federal rule, regulation, or policy, the utility should reference the language in question for guidance on how to proceed and apply it accordingly and faithfully.

Such rules and regulations may include, but are not limited to:

Open Data Access Standards (ODAS).[6] Approved in a November 20, 2020, Order, ODAS applies to electric and natural gas utilities with more than 50,000 customers. It addresses collection and sharing of Customer Energy Use Data (CEUD) for use by third parties. Both aggregated CEUD and anonymized CEUD are addressed. Aggregated CEUD datasets must pass a 4/50 screen, meaning the data must come from at least four customers with no single customer's energy use exceeding 50 percent of the total energy consumption within the dataset. Anonymized CEUD must pass a 15/15 screen, meaning that the dataset must contain at least 15 customers and no single customer's energy use can exceed 15 percent of the total energy consumption for the dataset.

Minnesota Government Data Practices Act (MGDPA).[7] For municipal or cooperatively-owned utilities considered government entities under the MGDPA, sharing customer information with a third party is subject to specific legal controls. The MGDPA classifies government data, including utility customer data, as either public or not public (e.g., private or confidential). A utility can freely share public data, but to disclose any "not public" personal data, such as a customer's name, address, and usage patterns, it must meet specific criteria specified in the act's language. In cases where a utility contracts with a third party to perform a function, the third party becomes subject to the MGDPA and must be contractually obligated to protect any non-public data it receives.

North American Electric Reliability Corporation (NERC) CIP-014.[8] Adopted by FERC in 2014, this NERC standard regulates the physical security of critical electric facilities by requiring owners and operators to identify critical assets, perform threat and vulnerability assessments, and implement security plans to protect against physical attacks on certain substations and control centers that, if compromised, could cause instability, uncontrolled separation, or cascading failures on the bulk power system. The standard outlines the process utilities must undergo to identify and protect such assets. This includes identifying critical facilities, third-party verification of the facilities, conducting threat and vulnerability assessments, development of a physical security plan, and notification thresholds for critical failures. The standard also requires entities to have procedures to protect sensitive or confidential information, which may include control and retention of information on site for third parties, sharing information on a need-to-know basis, marking documents as confidential, securely storing or destroying information that is no longer needed, and NDAs made available to third parties.

10 C.F.R. §95.5.[9] This Nuclear Regulatory Commission (NRC) regulation establishes procedures for safeguarding Secret and Confidential National Security Information and Restricted Data received or developed in conjunction with activities licensed, certified, or regulated by the

[6] In the Matter of a Petition by Citizens Utility Board of Minnesota to Adopt Open Data Access Standards, Docket No. E,G-999/M-19-505, Order Adopting Open Data Access Standards and Establishing Further Proceedings (November 20, 2020).
[7] Minn. Stat. ch. 13
[8] Adopted by FERC in *Physical Security Reliability Standard*, Order No. 802, 149 FERC 61,140 (2014).
[9] 10 C.F.R pt. 95, §95.5 (2022)

Commission. The regulation institutes both physical and information security measures to safeguard certain NRC-regulated information. Restricted data is defined as: information related to the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy. Restricted Data cannot be accessed unless the requester has "L" or "Q" access authorization,[10] an established "need-to-know" for the matter as determined by the data holder, and NRC-approved storage facilities if documents will be transferred.

10 C.F.R. §73.2.[11] This NRC regulation establishes physical security measures for special nuclear material at fixed sites, in transit, and for plants in which special nuclear material is used. Nuclear Safeguards Information is defined as information that details physical protection and security measures for special nuclear material, its sources, byproducts, and relevant plant equipment. In order to gain access to Nuclear Safeguards Information, at a minimum, individuals must have a "need-to-know" determination made by the information owner, undergo fingerprinting, and complete an FBI criminal history records check. These checks assure the NRC that giving the requester access to Nuclear Safeguards Information does not constitute an unreasonable risk to public health, safety, or national defense and security. Additionally, requesters of Nuclear Safeguards Information must demonstrate that they also have the knowledge, skill, training, or education to effectively utilize it. The regulation establishes that Nuclear Safeguards Information can be transmitted through a physical copy or digitally using only an NRC-approved device. The physical copy must be kept in a locked, unmarked storage container; digital versions can be kept on a computer or phone that only the approved individual only has access to. However, additional security measures for digital devices, including removable storage and physical security, may be required.

18 C.F.R. §388.113.[12] This FERC regulation governs the procedures for submitting, designating, handling, sharing, and disseminating Critical Energy/Electric Infrastructure Information (CEII) submitted to or generated by FERC. It defines CEII as specific, non-public engineering or vulnerability information regarding generation, transmission, or distribution systems, which, if released, could assist in planning an attack, and is exempt from Freedom of Information Act (FOIA) disclosure. Criteria and procedures for applying the CEII label to information, who may access CEII and how, a process for appealing decisions to deny access to CEII, protection measures for shared CEII (i.e., NDAs), and penalties for misuse.

[10] "L" and "Q" access authorizations are security clearances granted by the U.S. Department of Energy. They are equivalent to Secret and Top Secret, respectively.
[11] "Definitions," 10 C.F.R. § 73.2 (2026), *Electronic Code of Federal Regulations*, https://www.ecfr.gov/current/title-10/chapter-I/part-73/subpart-A/section-73.2.
[12] "Critical Energy/Electric Infrastructure Information (CEII)," 18 C.F.R. § 388.113 (2025), *Electronic Code of Federal Regulations*, https://www.ecfr.gov/current/title-18/chapter-I/subchapter-X/part-388/section-388.113.

7.0 EVALUATION OF THE GRID DATA SHARING PROCESS

To ensure that the data sharing process is effective in its goal of safely and securely sharing grid data with developers, academics, and other interested parties with legitimate need, we recommend that the Commission perform an evaluation of the process. We recommend that this occur three years after the process has been fully implemented and be based on clear, measurable metrics. These metrics could include, but not limited to, data points such as:

- Total number of data requests per utility, per year.
- Total number of fulfilled requests per utility, per year.
- Total number of denied requests per utility, per year.
- Total number of fulfilled requests for each risk level (high-, medium-, and low-risk), per year.
- Reasons why requests (if any) were denied, per year.
- How many requests were brought to the GSWG for dispute resolution, with an explanation of why the dispute occurred (e.g., why request was denied, timeline of remediation efforts between the utility and requester, and statements of position and desired outcome by both the dispute initiator and responder), per year.
- Average fulfillment time for requests per utility, per year.
- List of requesters for the year from each utility, per year.
- Any data breaches from requesters who have been given data that each utility knows of, per year.

Leading up to and after the initial review, utilities should report on Commission-determined metrics annually so that effectiveness can be tracked.

8.0 CONCLUSION

The proposed framework has four parts: Pre-Application Verification, Application, Risk Analysis, and Securely Sharing Data. The Pre-Application ensures that requesters are appropriately vetted for anything that would pose a security risk to the grid. The ability to choose how the background check is performed allows utilities to select the method that best suits their needs and capabilities. The Application provides the utility with the specifics of the request, which will allow them to perform the activities in Risk Analysis. The Risk Analysis step involves a preliminary review to understand the request and prepare for the scoping meeting, where questions can be answered and alternatives can be considered before the utility does the full risk analysis. This ensures that the request is properly evaluated and placed in the appropriate risk level, so the menu of mitigations and release criteria can be applied and layered in the most effective way. Securely sharing data can take whichever form fits the risk level of the data and the utility's capabilities and needs, but ultimately protects the shared data from being accessed by unapproved individuals.

This approach provides utilities with a practical path for exchanging grid data with requesters in a timely manner without compromising security. By building in optionality at various stages of this process, the framework is flexible enough to support a wide range of use cases, yet predictable enough to provide requesters with a consistent experience with utilities in the state. Equally, it provides utilities with the flexibility to tailor the process to fit their unique capabilities.

Additionally, as regulations, rules, and guidelines change, new technologies emerge, and the security landscape shifts, this framework provides a strong foundation that can be easily updated to meet future demands. The next steps—implementation, education, and iterative improvement—will ensure the process functions well and delivers the consistency and security benefits Minnesota stakeholders desire. Ultimately, this method provides a clear, controlled, and consistent procedure for utilities to evaluate grid data requests and share that data with requesters, thereby maintaining the security and reliability of the grid while supporting energy policies.

APPENDIX A: July 2025 After Action Report

Minnesota Grid Security Study: Data Protection Capabilities Workshop

After Action Report

July 2025

Minnesota Department of Commerce
Jessica Burdette
jessica.burdette@state.mn.us

Converge Strategies
Jonathon Monken
jmonken@converstrategies.com

Table of Contents

Executive Summary

On July 7, 2025, the Minnesota Department of Commerce ("Commerce") convened stakeholders involved in Docket No. E-999/CI-20-800 (*In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data*) for an in-person workshop focused on developing grid data risk categories and establishing the appropriate criteria and protections for each tier. A total of 23 participants, representing 12 Minnesota state offices, utilities, non-profit organizations, and private energy infrastructure developers, attended the workshop, which was facilitated by Converge Strategies, LLC ("Converge").

During this workshop, participants discussed:

- How to define and evaluate the level of risk associated with sharing grid data
- Appropriate protection mechanisms for data of varying risk levels
- Criteria for assigning a risk level to a particular data set (e.g., what criteria must be met in order to label something as "high risk")

The Data Protection Capabilities workshop was the first in a series of three workshops designed to inform the creation of a standard grid data sharing framework. This After Action Report (AAR) summarizes key findings from the workshop, but does not provide final recommendations regarding Docket 20-800. Future workshops will build on these findings to continue developing the Minnesota Grid Data Sharing Framework.

Following this workshop, Converge hosted a virtual outbrief for parties who were unable to attend the workshop in person. Similar outbriefs will be held after the second and third workshops to share the discussions and outcomes with interested parties.

Key Findings

The workshop encouraged attendees to think critically and collaboratively about best practices for grid data protection within the state. The morning activity included small-group discussions focused on defining the criteria for different risk levels. The afternoon activity featured a consensus-building conversation with all participants, where groups reported on their morning discussions and highlighted points of agreement or disagreement. Stakeholders began to coalesce around three risk tiers, summarized below, which will continue to be refined in future workshops.

High Risk Data. Non-public data that could jeopardize the integrity of the entire electric grid, creates risk to state or national security, and carries a significant risk of operational disruptions with widespread impacts (e.g., risk to critical infrastructure). Due to the sensitivity of high risk data, stakeholders identified protection measures such as strict access control (e.g., sharing within a portal or via secured video conference), training requirements for requesters, and requester vetting. Participants identified challenges such as varied protection capabilities across entities and recourse for misappropriated use of high-risk data.

Medium Risk Data. Non-public data that is less sensitive than high risk data, but could still cause harm if mishandled. Potential impacts are lower (e.g., short duration disruptions impacting fewer customers), but they are still significant and can typically be prevented or

mitigated with proper safeguards. This category could also encompass scrubbed high risk data and certain aggregated low risk data, such as system maps. Some high risk protection measures, like access controls and requester vetting and training, may be appropriate for medium risk data. However, the threshold between the three risk categories needs to be defined further. Participants highlighted challenges with the financial and administrative burden of sharing data and the need to define different types of risk associated with data sharing (e.g., economic, reputational, operational).

Low Risk Data. Non-public data unlikely to cause harm without significant aggregation effort or other prior non-public knowledge. Low risk data has minimal potential to cause system impact or disrupt daily operations. Stakeholders assigned fewer protections to low risk data, accepting general NDAs, attestations, or documentation of the request as sufficient measures. Challenges include the financial and administrative burden of sharing (as the data typically exists in large, non-sharable formats) and the need to distinguish between business and technical risk when categorizing data.

During the large group discussion, stakeholders raised several other data protection topics:

1. **Risk levels outside of the proposed process.** Stakeholders agreed that the statewide data sharing process should use three risk tiers (high, medium, and low). However, some expressed the need for a category above the high risk level for non-shareable data like proprietary information or data protected by other authorities that prevent sharing (i.e., NERC-CIP-014). Others highlighted the need for a category below the low risk level to encompass data that can be shared publicly or published online. These additional categories are outside of the scope of the working group because the Minnesota Grid Data Sharing Framework will not recategorize data that falls under existing classifications that prohibit sharing and publicly available data does not require stakeholders to develop protection measures and controls.
2. **Formal process for risk categorization disputes.** Participants acknowledged that even with clearly defined risk levels and criteria, there may be disagreements between utilities and requesters regarding the risk assigned to a data point. The process and venue to resolve these disputes, which could include referring the issue to the PUC, should continue to be discussed both within and outside of the workshop series.
3. **Cybersecurity-physical security risk nexus.** Numerous participants expressed concern that if a requester lacks the proper cybersecurity protections, threat actors could target their system to access grid data and determine the locations of critical nodes or assets. While this was acknowledged as possible, participants were reminded that this concern also exists outside of grid data itself. For example, even a less sophisticated threat actor can see and infer the criticality of an asset through platforms like Google Earth (i.e., a large natural gas plant or military installation) without using specific or granular data about loads or assets.
4. **Data containing Personally Identifiable Information (PII).** Several participants shared concerns about PII, which utilities have an obligation to protect. This issue is not relevant to this workshop series, as it is addressed in Docket No. E,G-999/CI-12-1344 (*In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities*).

Working Group Background

Following Xcel Energy's 2019 Hosting Capacity Analysis (HCA) Report (Docket No. E002/M-19-685), the PUC initiated orders to address concerns around the electrical distribution grid and customer data security between July 2020 and June 2023, culminating in the establishment of a working group. These working groups met during a series of workshops from July to September 2024.

In summer 2024, and in response to the June 2023 order, Converge was hired to provide services and recommendations to the Commission regarding open topics in the docket. Converge reviewed infrastructure security policies and risk assessment frameworks, researched cyber and physical security risks to grid infrastructure and supply chain vulnerabilities, conducted interviews with stakeholders involved in the docket to gather insight on the current status of grid data sharing, and provided recommendations for the structure and content of future workgroups.

Converge wrote a report ("Minnesota Commerce Grid Data Sharing Report") on those efforts and submitted it to the PUC for an open comment period in November 2024. The PUC accepted the report in February 2025 and directed the working group to continue and provide recommendations for a secure data sharing process for DER interconnection.

Timeline

Converge will lead stakeholders through a series of three workshops to inform a standard grid data sharing framework for Minnesota:

- **Data Protection Capabilities.** Focuses on developing data protection categories and criteria for categorizing data based on level and type of risk.
- **Data Sharing Mechanisms.** Focuses on developing a structure for a standardized data request process based on best practices.
- **Use Case Analysis.** Focuses on validating the data sharing framework developed in previous workshops by developing 6-8 use cases of sample grid data requests.

Following each workshop, participants will have the opportunity to provide comments on the workshop AAR to ensure that the conversations are accurately reflected. Additionally, each workshop will have a virtual outbrief for those who cannot attend in person and are interested in updates. While clarifying questions and comments are welcome in the AAR review period and virtual outbrief, they are not an opportunity for parties to reinterpret previous comments or add new considerations. Workshop activities will follow the timeline below:

Topic	Event	Date
Data Protection Capabilities	*Workshop (Complete)*	*July 7, 2025*
	Virtual Outbrief (Complete)	July 18, 2025; 10-11AM CT
	Report Comment Period	July 24 - August 4, 2025

Data Sharing Mechanisms	Workshop	August 11, 2025
	Virtual Outbrief	August 22, 2025; 11AM-12PM CT
	Report Comment Period	August 27 - September 8, 2025
Use Case Analysis	Workshop	October 6, 2025
	Virtual Outbrief	October 17, 2025; 11AM-12PM CT
	Report Comment Period	October 22 - November 5, 2025
Final Report	Final Report Comment Period	January 9 - 22, 2026

Summary of Working Group 1: Data Protection Capabilities

Objectives

The goal of the Data Protection Capabilities workshop was to develop shared practices related to access criteria and vetting of individuals and organizations. To achieve this goal, this workshop had three objectives:

1. Discuss existing data identification and classification methods used by workgroup stakeholders.
2. Develop shared practices related to access criteria and vetting of individuals and organizations.
3. Develop proposed data protection categories and criteria for categorizing data based on level and type of risk.

Participants

The Data Protection Capabilities workshop convened a total of 23 participants from 12 state offices, utilities, non-profit organizations, and private energy infrastructure developers:

- Minnesota Bureau of Criminal Apprehension/MN Fusion Center
- Minnesota Department of Commerce
- Minnesota Information Technology Services (MNIT)
- Clean Energy Economy Minnesota (CEEM)
- Minnesota Solar Energy Industries Association (MnSEIA)
- Nokomis Energy
- U.S. Solar
- R Street Institute
- Dakota Electric Association
- Minnesota Power
- Otter Tail Power
- Xcel Energy

Risk Categorization Small Group Activity

For this activity, stakeholders were assigned to small groups with varied representation from utilities, developers, non-profit organizations, and representatives from Minnesota security and regulatory agencies. Each group worked to define the high-, medium-, and low-risk data categories using the following guiding questions:

- **Definition.** How would you define this risk level? What risks are we trying to mitigate by placing data in this category?
- **Criteria.** What factors (e.g., technical needs, security, business considerations, regulatory concerns) should we consider when deciding if data fits here?
- **Protection Measures.** What data protection and/or risk mitigation techniques are reasonable and appropriate at this risk level? How do we ensure protections are appropriate, feasible, and reasonable while not blocking statewide coordination?
- **Challenges.** What makes it difficult to share or protect data at this risk level? What concerns do you have about sharing or protecting this type of data (e.g., person-based, organization-based, cybersecurity, business-related, etc.)?

The small groups then shared their risk categories with the large group and Converge facilitated a discussion with the full group where participants asked questions, provided feedback, and worked to build consensus on the risk categories. The themes for each risk level are summarized below. See Attachment A and B for full notes.

High Risk Data

Definition. Stakeholders defined high risk data as non-public data that could jeopardize the integrity of the entire electric grid, creates risk to state or national security, and carries a significant risk of operational disruptions with widespread impacts (e.g., risk to critical infrastructure). This includes information that could be used by bad actors to harm, cripple, or destroy the electric grid, disrupt operations, or expose ratepayers to significant financial risk. There was a question about whether Personally Identifiable Information (PII) falls into the high risk category. However, this topic is covered under Docket No. E,G-999/CI-12-1344 (*In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities*), and is out-of-scope for this workshop series.

Criteria. High risk data includes operational data such as load flow design, black start capabilities, and grid architecture; data relevant to national security or designated by state or federal policy; and site- or location-specific data. Stakeholders agreed that existing standards with established requirements around data sharing, such as NERC/FERC critical infrastructure, will not be revisited as part of this process. Some stakeholders argued that the aggregation of low or medium risk data can result in a data set that is high risk. However, there was disagreement on how this could be fairly determined and defining what instances or specific data points this could apply to.

Protection Methods. Stakeholders generally agreed that Non-Disclosure Agreements (NDAs) alone are insufficient to protect high risk data. Additional options for protection measures include a state-backed vetting process for requesters, enforceable accountability mechanisms (e.g. penalties, legal protections for breaking agreements or terms of use), data access time limits or view-only capabilities (i.e., non-downloadable, secured portals), and

data encryption. Stakeholders also discussed data handling and cybersecurity guidelines and training requirements for requesters. While many were in favor of this, some stakeholders voiced concerns about how burdensome or expensive this could become for both utilities and requesters. However, there are examples from other sectors of free online training resources that can be referenced as best practice, such as the Department of Defense (DoD) Mandatory Controlled Unclassified Information (CUI) Training or Cyber Awareness Challenge.

Challenges. In addition to the limitations of NDAs and ambiguity around how data aggregation impacts risk categorization, stakeholders were concerned about the lack of uniformity in operational and technical protection capabilities across utilities and requesters. For example, organizations use different cybersecurity standards/software and have different internal policies about handling sensitive information. Once data is provided, the utility loses sight of how the data is being stored and protected, which can pose a risk. Other challenges include the cost to utilities of gathering, storing, and managing data and the cost to requesters of additional training and security measures to comply with proposed requirements.

Medium Risk Data

Definition. Stakeholders defined medium risk data as non-public data that advances the public interest and is less sensitive than high risk data, but contains some vulnerabilities and could still cause harm if mishandled. This data carries a risk of limited potential impacts (e.g., short duration or localized disruptions), but not societal-level disruption, and can typically be prevented or mitigated with proper safeguards. Examples of this kind of data include data for less vulnerable or more networked grid areas, proprietary operational data, or scrubbed high risk data.

Criteria. Medium risk data includes information on areas with enhanced resilience measures, such as redundancies or accessible alternate service options in case of an outage, as these measures reduce the likelihood and harm level of disruptions. There was some agreement that discrete data points, such as maps showing asset locations, customers, and system components would be included in this category. Stakeholders also discussed how aggregating certain types of lower risk data or scrubbing high risk data could reclassify it as medium risk. Further discussion is required to ensure this is done fairly, and the medium risk category should continue to be refined to avoid becoming a "catch all" category.

Protection Methods. Stakeholders applied some high risk protection measures, like access controls and requester vetting and training, to medium risk data. Training and vetting of requesters refers to potential background checks, government vetting, or a process similar to the NERC/FERC vendor vetting process. Scrubbing and encryption of sensitive data could also make it more easily shareable. To address the risks of aggregating data through multiple requests, some utility stakeholders suggested limits on the granularity and amount of data a single entity could request. This caused concern among other stakeholders, as these limits are highly subjective and run counter to the objectives of creating a clear, well-defined grid data sharing process. Some utility stakeholders also believe that access to medium and high risk data should require requesters to demonstrate a legitimate commercial or academic need for the data, though it was unclear who should determine the legitimacy of a request.

Challenges. Medium risk discussions highlighted the challenges of clearly defining the thresholds between high, medium, and low risk data. It is challenging to quantify potential impacts and differentiate between the scale and likelihood of actual harm versus perceived risk. Stakeholders agreed that distinguishing between operational, economic, and reputational risk could provide some clarity. Stakeholders also noted that establishing clear exemptions for activities that serve the public interest, distinguishing between facility-specific risks and broader public safety concerns, and evaluating the vulnerability of critical community lifelines could support decision-making. Cost-related challenges include, first, determining how to calculate the expenses associated with security assessments, the execution of NDAs and business agreements, and the development of new programs and procedures for data sharing; and second, identifying who should bear the financial responsibility for these efforts.

Low Risk Data

Definition. Stakeholders defined low risk data as non-public data that is unlikely to cause disruptions or material harm to individuals, organizations, or infrastructure without significant aggregation effort or other prior non-public knowledge. Stakeholders concluded that public data is a separate category from low risk, as additional protections beyond the sanitization that already occurs is not required (e.g., peak load data, outage maps, service territory, queue reports, interconnection processes, and reliability metrics).

Criteria. Low risk data is the lowest level of scrutiny that still requires some controls and is not available publicly. It is available upon request with minimal requester requirements. This category also encompasses historical data that may have previously been categorized as medium or high risk, but has been recategorized as low risk due to its age. This applies to cases where the age of the data limits its potential to cause harm, and requires further discussion at future workshops.

Protection Methods. Stakeholders agree that fewer protections are required for low risk data, and that measures such as general NDAs, attestations, or documentation of the request are adequate. Some participants still support data handling training requirements for requesters, but others disagreed that this is a reasonable requirement for low risk data. Future workshops should continue defining the lines between low, medium, and high risk and developing guidance for aggregation and scrubbing of data to reduce risk.

Challenges. The primary challenge for low risk data is the potentially high administrative cost of fulfilling large volumes of low risk data requests. Utility stakeholders explained that even if it is low risk, non-public data is often not stored in a shareable format. Therefore, more resources are required to appropriately sanitize and package data for sharing, and not all utilities have the capacity to do this. If low-risk data is being provided to many requesters with minimal requirements, there may be an argument for packaging the data and making it public to reduce administrative burden.

Open Questions

Stakeholders made progress defining the different tiers of risk and appropriate protection measures for each. Future workshops will continue building on these concepts and further defining the risk categories to ensure that the resulting Minnesota Grid Data Sharing Framework is transparent and fair. These open questions will be revisited in future workshops:

- Who will resolve disputes between utilities and requesters over the risk level assigned to data?
- Who bears the cost of gathering, storing, and managing data on the utility side? Who bears the cost of complying with training and additional security measures on the requester side?
- Further defining thresholds between the risk levels. How do we ensure that risk is accurately evaluated?
- Do utilities have any recourse if data is provided and misused, resulting in negative impacts?

Attachment A: Risk Categorization Small Group Activity

This section includes the full notes from each small group's discussion of high-, medium-, and low-risk data.

Group 1

High Risk	
Definition	• Data that poses a threat to grid reliability and system operation, including information that could be used by bad actors to harm, cripple, or destroy the electric grid or disrupt operations. • Sensitive infrastructure and security-related data, such as critical infrastructure information (CEII) (including water and defense infrastructure), grid design documentation, and classified or regulated content like CEII and NERC CIP data. • Customer-specific and PII data, including non-aggregated customer data, personalized data, and anything that compromises privacy or could be exploited for harm. • Data that could expose the utility or ratepayers to significant financial losses.
Criteria	• Requests that raise security or trust concerns, such as those from unknown or new requesters, requests with red flags (e.g., unusually high volume), or multiple seemingly low-risk requests that may signal probing behavior. • Sensitive infrastructure and operational details that expose vulnerabilities or could enable exploitation, such as feeder data (especially with few customers), site-specific or location-specific data, and infrastructure serving critical facilities (e.g., water, wastewater, military, medical). • Information that compromises confidentiality or privacy, including individual ratepayer data or trade secrets. • Data that could lead to loss of service and/or has broad or critical impact, such as outages affecting areas for extended periods or disruptions to community lifelines like water, gas, or medical facilities.
Protection Methods	• Clear terms for data use and sharing, including with whom it will be shared and how (e.g., over secure video, with encryption), and protection agreements or NDAs, including those requiring executive approval. • Evaluation of the requester, including conducting a risk assessment or background check, and requiring a clear justification or understanding of why the data is needed. • Enforcement and accountability mechanisms, such as penalties for breaking agreements and stipulations that data not be shared. • Governance and training requirements, including organizational policies around data sharing practices and required training.
Challenges	• Who pays for data? • Who is responsible for the data? • What is the recourse for misappropriated use of data?

	• Difficulties of balancing privacy needs with climate goals, business needs, and state policies. • Administrative burden of responding to requests.
Medium Risk	
Definition	• High risk data that is adequately protected lowers risk to medium, with some exceptions (ex. military installations, trade secrets). • Data that covers less vulnerable facilities. • Data that may impact public safety or community lifelines. • Exploitation may cause only a short duration disruption. • Data that, when aggregated, could become high risk.
Criteria	• High risk data that is properly protected. • The criteria is already defined by order 12-1344 (15/50). • Impacted areas have adequate redundancy and/or accessible alternate service options in case of an outage. • Release of data may provide additional information on an individual or group of ratepayers. • Creates significant financial or technical challenges.
Protection Methods	• NDAs. • requester vetting and training requirements. • Participants are interested in examples from other states.
Challenges	• Trouble deciphering the threshold between medium and low, and medium and high. • Managing interconnectedness of utilities across territories. • Vulnerability of community lifelines. • Risk to the end user of a DER asset.
Low Risk	
Definition	• Minimal-to-no disruption possibility. • Data that is available by request or application. • Nuisance-to-no operational impact, but potentially economic or reputational impacts.
Criteria	• Data sharing is memorialized. • Doesn't qualify for mandatory outage reporting. • Must receive consumer consent. • Minor disruption to the daily course of business.
Protection Methods	• A minimal or procedural step is needed to access it. • A time horizon for when data becomes out of date or data sharing consent expires. • Memorialize and document the sharing. • Requirements for the pre-application.

Challenges	• Can be requested at high volumes, so the financial and administrative costs or capacity to respond to them may be high. • Can become high risk data under certain conditions.

Group 2

High Risk	
Definition	• Data that could materially harm individuals, organizations, or society, including information that could compromise public safety, result in economic loss, or disrupt essential services. This data ranges from personal data (e.g., SSNs, licenses) to infrastructure data tied to critical infrastructure like nuclear, medical, or telecommunications. • Information that exposes grid or system vulnerabilities, such as system or solution mapping, critical infrastructure data, and data that, if exploited, could compromise grid stability or public safety. • Customer and other sensitive information, including PII, customer usage data, trade secrets, or any information that violates customer privacy. • National or state-level security risks, including data that impacts military, government, or medical infrastructure or undermines broader security or economic advantages. • Data that could cause societal harm, like nuclear power station data.
Criteria	• Information not generally visible to the public that, if breached, could have catastrophic societal impacts. • Individually identifiable or customer-specific data, like PII or infrastructure that serves a single customer (e.g., airport, industrial site), especially when tied to sensitive or high-value assets. • Data relevant to national security or designated by state or federal policy. • Context-sensitive risk factors, such as data from areas with known reliability issues or datasets where risk varies based on aggregation, and situations where risk can be reduced through redaction.
Protection Methods	• Delay release of data and require timed access. • Require data handling training. • Ensure data is not on the public internet and cannot be downloaded. • Limit access to those with specific login credentials.
Challenges	• NDAs may not cover everything and are more of a reactive tool than a proactive one (i.e., protections kick in after negative incidents, meaning the utility will need to 'fight' on multiple fronts). • Need to be cognizant of tracking sensitive data aggregation over time, and understand which data becomes riskier when aggregated. • Definitions of high risk may differ within an organization (e.g., cyber team views risk more severely than business operations personnel).

Medium Risk	
Definition	• Nonpublic or proprietary information with limited potential impact, including trade secrets, private operational data, or scrubbed high-risk data that, if released, would cause localized harm or modest economic or reputational damage, but not societal-level disruption. • Data that advances public interests but contains vulnerabilities, where disclosure carries some risk but potential impacts can be prevented or mitigated through safeguards (e.g., redaction). • Lower-risk data that, when aggregated, becomes more dangerous. • Data that would not result in material or immediate harm, or at most only affect several customers or non-critical facilities.
Criteria	• Lower risk data that, when aggregated, could become higher risk. • High risk data that has been adequately scrubbed of sensitive information. • Nonpublic data that could cause material economic harm or localized impacts to non-critical infrastructure.
Protection Methods	• NDAs. • Data protection methods like encryption, sharing limits, and limits on data granularity. • Requiring a background check or data handling training for requesters. • Only sharing data for investment-based requests.
Challenges	• Quantifying potential impacts may be difficult, as well as differentiating between actual harm and perceived risk. • Differentiating data based on facility and public safety (e.g. 1 substation in a residential area vs. an airport substation). • Coming up with uniform definitions of economic, reputational, and operational risk. • How to track and account for data across its sharing lifecycle once external parties have accessed it. • Coming up with appropriate exemptions for public benefit.
Low Risk	
Definition	• Low-risk or minimal-impact data, which is nonpublic but would not cause material harm to individuals, organizations, or infrastructure if disclosed. These datasets pose no economic, reputational, or physical risk, or only minimal risk under limited circumstances. • Data requiring the lowest level of control, such as information not available on the public internet but still subject to basic restrictions (e.g., the 15/15 rule), and where any potential consequences are minor, economic, or would require significant additional nonpublic knowledge or aggregation to be harmful. • Non-critical or non-sensitive data, where breach consequences are negligible and no critical systems or customers would be affected.
Criteria	• Data must still be applied for; it's not public. • Real time data that would be released after its origin point.

Protection Methods	• Higher risk data that has a delayed release (i.e., medium risk data becomes low risk data if released after 2 years). • Require data handling training. • Automated process for acquiring data or made otherwise easily accessible. • Simple NDAs or attestations.
Challenges	• How to balance technical vs. business risk. • Time restrictions can change risk and what data is requested or useful. • Compliance issues with data retention and deletion. • Aggregation can increase risk level.

Group 3

High Risk	
Definition	• Data tied to regulated sites, national security, or critical infrastructure, such as information associated with FERC/NERC. • Cybersecurity-relevant or compromise-enabling data, including anything that could be used to initiate a cyber event or disrupt system functionality if used by bad actors. • Sensitive customer data like PII.
Criteria	• Operational and grid security data, including load flow design, black-start capabilities, grid architecture, and passwords. • Data tied to critical infrastructure and established thresholds, such as assets transporting over 100kV or generating over 100MW, or information related to key resources that support or interconnect critical infrastructure. • Sensitive password and customer data, including employee information and PII.
Protection Methods	• NDA combined with other methods, such as a vetting process, encryption of data, and with legal protections in place (accomplished through legislation or an executive order). • Even with protections, it may be inappropriate to share the highest risk data under any circumstances.
Challenges	• Enforceability of NDAs and management of the data once it leaves the utility's possession. • The grid is constantly changing, so some data can quickly become outdated. • The capabilities to securely share and keep data might vary from utility-to-utility and requester-to-requester. • The cost of collecting, storing, and developing a new program and systems to share data.
Medium Risk	

Definition	• Data that is not public and does not contain information that is categorized as high or low risk, and is distributed only on a 'need to know' basis. • Some data in this category could be low risk itself, but could rise to high risk if combined with other data.
Criteria	• Data, such as maps, that show the location of assets, customers, and system components and types. • Data that could create cyber vulnerabilities, such as vendor lists. • Incident data, Suspicious Activity Reports, and other information that could provide insight to activities of potential bad actors.
Protection Methods	• Methods that go beyond the powers of an NDA and mitigate risk to industry, such as business agreements, executive orders, and legislation. • Sanitization process (ex. HCA). • Granting access to individuals who have been vetted/verified (e.g. government vetting or a process similar to the NERC/FERC vendor vetting process) and who have a role-based need to view the data and have demonstrated a legitimate commercial or academic objective. • Allow the requester to view the data in an interactive session with the utility, but not for the data to leave the premises.
Challenges	• There can be significant differences between utilities in terms of data availability, the form data is kept in, threat assessment capabilities, and sharing requirements (especially between private and public utilities). • Vendors are a vector for cyber incidents that utilities have little control over. • It is difficult to define the scale of potential impacts related to certain data sets. • Cost to perform security assessments; issue NDAs; record, retain and compile data; and create new programs and procedures for data sharing. • Determining who will pay and how cost is calculated. • Regulatory requirements exist that draw clear lines around certain kinds of data (e.g. customer data) and what can and cannot be shared.
Low Risk	
Definition	• Data that is publicly available either through reporting requirements or voluntarily or has been appropriately sanitized.
Criteria	• Data that is often already public includes aggregate and peak load data, outage maps, blurred hosting capacity maps, service territory, queue reports, interconnection processes, and things required by law or Commission Order, such as reliability metrics. • Historical data, especially for market or academic research purposes, if appropriately sanitized.
Protection Methods	• Broad, system-wide aggregation that effectively sanitizes the data to the appropriate level (i.e. "tear lines").

Challenges	• There are inconsistencies between utilities in what is publicly available (e.g. service territory maps). • Utilities only keep this type of data for a certain amount of time due to operational need, cost, and space. • Data retrieval can be costly because it may not exist in a sharable format and need to be sanitized or reformattied before it can be released.

Attachment B: Data Protection and Risk Categorization Criteria Concept Alignment

Following the Exercise, workshop attendees were asked to provide "votes"- or feedback- on concepts and ideas that stood out to them for each of the three data categories – high, medium, and low risk. Participants were instructed to place their votes into three categories, defined as:

"Agree" - "This is an example of a best-practice."
"Accept" - "There's an opportunity to strengthen this."
"Disagree" - "This isn't addressing existing gaps."

High Risk Data	
Agree	• Participants agreed that, generally, high-risk data includes anything that – if compromised – could result in catastrophic harm to national security, public safety or community lifelines, grid integrity, or critical infrastructure. Examples include load flow data, black-start information, passwords, employee data, NERC CIP, and industrial usage information. • Participants also indicated that criteria for high risk data should align with, or at least not contradict, existing state, federal, or regulatory body designations. • There was agreement that risk should be narrowly defined by operational risk and the degree of impact the data could have in the wrong hands. • There was broad agreement amongst participants that there should be a vetting process and training on proper use and handling of data for requesters. • Strict data sharing protections, such as not allowing data to be downloaded onto external servers, being for view-only on-premises, and having access be need- and role-based should be implemented for this risk category. Additionally, some data, like IT/OT data, should never be shared, and this may belong in a bucket above high risk. • There was agreement that NDAs are not sufficient to protect data and that there need to be meaningful consequences for mishandling of data and breaking of agreements and legal protections for utilities sharing data via proper channels and in good faith. Additionally, it was expressed that protections need to cover ISO27001/27017. • There should be defined cyber controls for data and data sharing. • Participants called out that there needs to be mindfulness about aggregating data, as aggregating certain kinds of data to certain levels can move it into the high risk category.

Accept	• NDAs alone are insufficient to protect sensitive data. Additional, layered protection measures are necessary. • Risk can be elevated if certain data is aggregated or grouped. • Some participants thought the scope of criteria listed should be narrowed to ensure that only high risk data was included. • Stewardship/context of data. • Areas of reliability issues. • Cyber security certifications. • Vetting process – internal and external access.
Disagree	• There was disagreement that encryption of high risk data would be sufficient protection. • Some participants pushed back on there being kinds of data that would never be released in any way, stating that if the risk associated with a particular data set is mitigable with economic penalties, it should not be high risk. • If something is already public data, it cannot be high-risk. • There was pushback on the assertion that all feeder data is high risk – even if a few customers are truly high risk, not all of them should be. • Penalties and enforcement of data is mismanagement. Need to head off bureaucracy bloat (disallow share costs are low). • Some participants pushed back on the broad statement that aggregation can make data more high risk, expressing that multiple requests for low-risk data is not high risk and the need for the risks of aggregation to be more clearly defined. • When defining high risk, anything that is already public data should not be high risk and operational data needs to be more clearly defined. • Some participants expressed the opinion that PII should not be a sole criterion for classifying data as high risk, stating that some PII has low consequences, and that damages from PII release are often economic, reputational, or otherwise not operational level. • The question of how it would be decided that data has no public need, interest, or benefit and who would make that decision was raised.
Medium Risk Data	
Agree	• Overall, participants agreed that proper mitigation measures can move high risk data down to medium risk and that data availability could be expanded with proper protections in place. Similarly, aggregation of low risk data could move it into the medium risk category. • The idea of limiting the number of requests, combinations of data sets, and scale of RFIs was supported. • Generally, the idea of using potential impacts as a measure for determining risk was looked at favorably. • Participants agreed that having training requirements via a third party and a vetting process for people requesting and handling information. It was suggested that the work FERC/NERC has done to develop criteria for vendors could be leveraged. • There was agreement that harm should be considered through the lenses of material economic harm and physical harm.

	• Support was expressed for equipment types being at least medium risk, as one device could be used to gain access to the system. • Participants agreed that there are discrepancies between utilities when it comes to data availability. • There was agreement that the question of who would bear the cost (in terms of resources and personnel) of new programs needs to be discussed, and that fees paid by the requester may be appropriate. • Participants expressed that there needs to be an avenue for disagreements over request legitimacy or denied requests to be handled.
Accept	• Participants wanted more clarity on what accountability for data governance would look like. • Participants expressed that they could accept tiered vetting, but wanted clarity on how that would be developed and how it would work once implemented. • Protection measures were something accepted as a necessity, but some thought that there is more to consider about the method of sharing (encryption, secure portal). • Training for data recipients was something that was agreed upon by some, but others expressed that it needed more careful thought and that it might not be needed for all levels of risk. • Some participants called out a need for more clarity around what level of aggregation of low risk data means and how aggregation could turn low risk data into medium risk data. • While some participants said that repeat requests or requests for multiple data sets could correlate to risk, others said this would be difficult to measure and create a metric for. • Participants were generally accepting of the idea that if potential impacts can be reasonably prevented through additional protections (business agreements, legislation, etc.) then data could be shared. • The question of whether there is an acceptable amount of disruption or load loss to the industry resulting from the release of data exists. If so, what would those thresholds be?
Disagree	• Some participants disagreed that controls and protections on high risk data can move it into the medium risk category. • Again, people disagreed that NDAs are an adequate protection measure, but some went a step further and disagreed that a business agreement would be an adequate protection. • There was some disagreement on whether or not high- versus low-networked areas have bearing on risk. • The question of how 'less vulnerable' facilities or areas would be defined was asked. • Some participants wondered how protection measures would apply to a requester who might not be a developer, such as university researchers or interest groups. • Some participants disagreed that training on data governance was necessary unless the requester would be accessing an internal enterprise system via VPN.
Low Risk Data	

Agree	• There was broad agreement that data in this category tends to be things that are already publicly available or easily available upon request (such as a customer requesting their own data). • Participants agreed that noting requester information is a distinguishing characteristic for low- versus 'no'-risk. • Because administrative hurdles can be time-consuming and expensive, it may be reasonable to make certain very low risk data publicly available. • There was agreement that automation, when possible, is a good way to reduce burdens for low risk data.
Accept	• Participants did not place anything in this category.
Disagree	• Some participants disagreed that low risk data is publicly available data, and that publicly available data is actually a separate category from low risk.

APPENDIX B: August 2025 After Action Report

Minnesota Grid Security Study: Data Sharing Mechanisms Workshop

After Action Report

August 2025

Minnesota Department of Commerce
Jessica Burdette
jessica.burdette@state.mn.us

Converge Strategies
Jonathon Monken
jmonken@converstrategies.com

Table of Contents

Executive Summary

On 11 August 2025, the Minnesota Department of Commerce ("Commerce") convened stakeholders involved in Docket No. E-999/CI-20-800 (*In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data*) for an in-person workshop focused on developing a proposed structure for a standardized data request process. A total of 24 participants, representing 12 Minnesota state offices, utilities, non-profit organizations, and private energy infrastructure developers, attended the workshop, which was facilitated by Converge Strategies, LLC ("Converge").

During this workshop, participants discussed:

- Prerequisites to submitting a data request application
- Information that should be included in a standard data request
- Reasonable timelines for data request application review
- How denied applications and appeals should be handled and the potential role of state agencies in that process, based on existing legislative rules

The Data Sharing Mechanisms workshop was the second in a series of three workshops designed to inform the creation of a standard grid data sharing framework. This After Action Report (AAR) summarizes key findings from the workshop, but does not provide final recommendations regarding Docket 20-800. The third workshop will build on these findings to continue developing the Minnesota Grid Data Sharing Framework.

Following this workshop, Converge hosted a virtual outbrief for parties who were unable to attend the workshop in person. A similar outbrief will be held after the third workshop to share the discussions and outcomes with interested parties.

Key Findings

The workshop encouraged attendees to consider what a state-wide, standardized data request process could look like. Throughout the day, workshop participants alternated between small-group discussions focused on building the application process and large-group consensus-building conversations, where groups reported on their small-group discussions and highlighted points of agreement or disagreement. The diagram in Figure 1 below was used to guide the facilitated discussions.

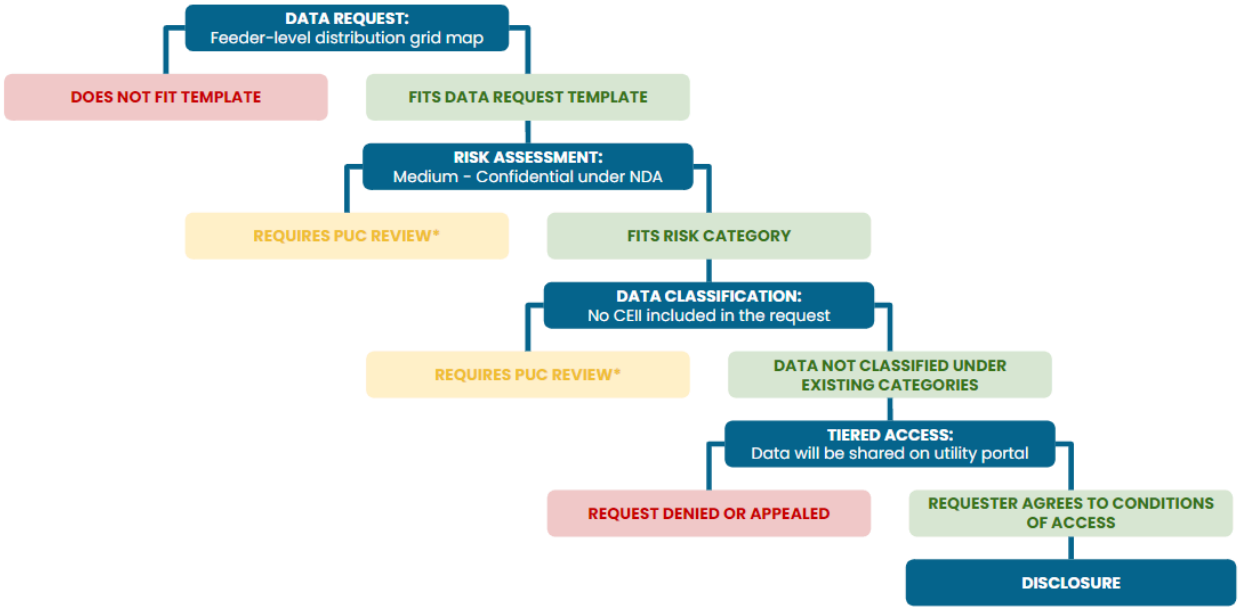


Figure 1: Example of Feeder Level Data Request and Sharing Process

Key takeaways from the discussions are summarized briefly below; more detail is available in subsequent sections and in the appendix.

Pre-Application Process. Workshop participants were asked to consider the steps requesters should have to take before submitting a data request application. Participants focused on two primary options. First, requesters could be required to undergo a background check, to be performed by a third party and evaluated by the utility. This would result in a pass/fail outcome, determining whether the individual or organization is eligible to submit a data request application. Alternatively, requesters could be required to complete a preliminary application, which could include information like the requester's name, organization (if applicable), additional personnel requiring access to the information (if applicable), and a project description and justification for the request.

Building a Standard Application. Participants discussed the standard request template concept and identified the information that is essential to help utilities evaluate risk as they receive requests. Essential information broadly included whether anyone other than the applicant would need access to the data (including third parties), a clearly articulated need and justification, data type (e.g. equipment, load, capacity), validation of a passed background check (source TBD), and the period of time the requester would need access to the data in order to fulfill their requirements. Some 'nice to have' information included the requester's plans to develop public-facing derivative products from the data or whether they planned to input it into an AI, information about their data handling and data security practices, the geographic locations associated with the data, and the time period the data originates from (e.g. the last twelve months, the last three years).

Application and Request Timeline. Participants agreed that the most important aspects of the application request process are clear, consistent communications and shared expectations between requesters and utilities. While the timeline for reviewing and fulfilling a request may be impacted by the risk level of the requested data, participants agreed that a

general guideline of three months or 90 days is reasonable for a utility to complete their review of an application. Due to concerns around communications, secure data sharing, and appropriate data control, some participants suggested developing a portal or tracker through which requesters can monitor progress on their request and utilities can share data.

Role of the State and Working Group. The final activity focused on what an appeals process for denied applications might look like, and what role, if any, the state might play in that process. Participants agreed that a denied request should be accompanied by clear, criteria-based reasoning and an invitation for further discussion. They also agreed that a formal appeals process should be a last resort, and that utilities and requesters should make every good-faith effort to resolve disputes without escalation. Two primary ideas for a formal appeals process emerged - a utility-led process, or a process that uses the MNPUC's existing complaints process. The utility-led process was discussed as the primary method for appeals, with the MNPUC process being exercised during 'extreme' situations such as an inability to reach consensus between the requester and utility.

Working Group Background

Following Xcel Energy's 2019 Hosting Capacity Analysis (HCA) Report (Docket No. E002/M-19-685), the Minnesota Public Utilities Commission ("PUC") initiated orders to address concerns around the electrical distribution grid and customer data security between July 2020 and June 2023, culminating in the establishment of a working group. These working groups met during a series of workshops from July to September 2024.

In Summer 2024, and in response to the June 2023 order, Converge was hired to provide services and recommendations to the Commission regarding open topics in the docket. Converge reviewed infrastructure security policies and risk assessment frameworks, researched cyber and physical security risks to grid infrastructure and supply chain vulnerabilities, conducted interviews with stakeholders involved in the docket to gather insight on the current status of grid data sharing, and provided recommendations for the structure and content of future workgroups.

Converge wrote a report ("Minnesota Commerce Grid Data Sharing Report") on those efforts and submitted it to the PUC for an open comment period in November 2024. The PUC accepted the report in February 2025 and directed the working group to continue and provide recommendations for a secure data sharing process for DER interconnection.

Timeline

Converge will lead stakeholders through a series of three workshops to inform a standard grid data sharing framework for Minnesota:

- **Data Protection Capabilities:** Focus on developing data protection categories and criteria for categorizing data based on level and type of risk.
- **Data Sharing Mechanisms:** Focus on developing a structure for a standardized data request process based on best practices.
- **Use Case Analysis:** Focus on validating the data sharing framework developed in previous workshops by developing 6-8 use cases of sample grid data requests.

Following each workshop, participants will have the opportunity to provide comments on the workshop AAR to ensure that the conversations are accurately reflected. Additionally, each workshop will have a virtual outbrief for those who cannot attend in person and are interested in updates. While clarifying questions and comments are welcome in the AAR review period and virtual outbrief, they are not an opportunity for parties to reinterpret previous comments or add new considerations. Workshop activities will follow the timeline below:

Topic	Event	Date
Data Protection Capabilities	*Workshop (Complete)*	*July 7, 2025*
	Virtual Outbrief (Complete)	July 18, 2025; 10-11AM CT
	Report Comment Period (Complete)	July 24 - August 4, 2025
Data Sharing Mechanisms	*Workshop (Complete)*	August 11, 2025
	Virtual Outbrief (Complete)	August 22, 2025; 11AM-12PM CT
	Report Comment Period	August 27 - September 8, 2025
Use Case Analysis	Workshop	October 6, 2025
	Virtual Outbrief	October 17, 2025; 11AM-12PM CT
	Report Comment Period	October 22 - November 5, 2025
Final Report	Final Report Comment Period	January 9 - 22, 2026

Summary of Working Group 2: Data Sharing Mechanisms

Objectives

The goal of the Data Sharing Mechanisms workshop was to develop a structure for a standardized data request process based on best practices. To achieve this goal, this workshop had three objectives:

1. Discuss the differences in grid data sharing application processes across workgroup stakeholders.
2. Develop a proposed pre-application vetting standard that ensures the accessibility and security of grid data sharing in the state.
3. Develop a proposed structure for a standardized data request process, based on best practices, to create consistency across the state.

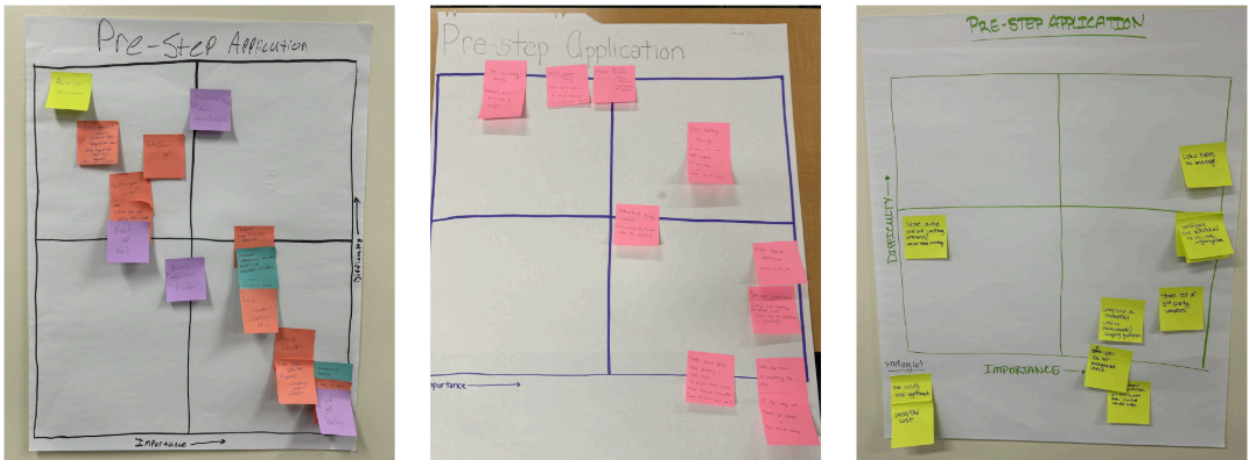
Participants

The Data Sharing Mechanisms workshop convened a total of 24 participants from 12 state offices, utilities, non-profit organizations, and private energy infrastructure developers:

- Minnesota Attorney General's Office
- Minnesota Public Utilities Commission
- Minnesota Department of Commerce
- Minnesota Information Technology Services (MNIT)
- Minnesota Solar Energy Industries Association (MnSEIA)
- U.S. Solar
- R Street Institute
- Fresh Energy
- Dakota Electric Association
- Minnesota Power
- Otter Tail Power
- Xcel Energy

Pre-Application Process Small Group Activity

For this activity, stakeholders were assigned to small groups with varied representation from utilities, developers, non-profit organizations, and representatives from Minnesota security and regulatory agencies. Each group worked to define the steps that prospective data requesters should take before submitting an application by thinking through the importance (i.e., information required to assess applicants) and difficulty (i.e., relevance or ability to extract and utilize the requested information) of potential vetting requirements.



The small groups then shared their ideas with the large group and Converge facilitated a discussion where participants asked questions, provided feedback, and worked to build consensus on the importance and difficulty of potential vetting requirements. Two main ideas took shape and are discussed below. See Attachment A for full notes from the activity.

Background Check

Some participants thought that the most important initial step is to conduct a background check to establish whether the requester (i.e., individual or organization) has a history of bad actions or associations with threat actors (e.g. domestic violent extremist groups or foreign governments). In their view, beginning the process with a background check, conducted by a vetted and approved third party, is the most efficient option, as neither the requester nor the utility would spend significant resources upfront providing information for or reviewing an application. Figure 1, shows a potential pre-application process whereby requesters pass both a background check and the utility's internal risk assessment process.

Figure 2: Potential Background Check Process

Preliminary Application

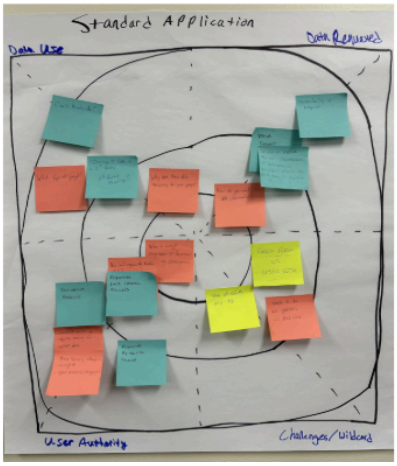
Other participants preferred an abbreviated version of the data request application. The most important fields to include are:

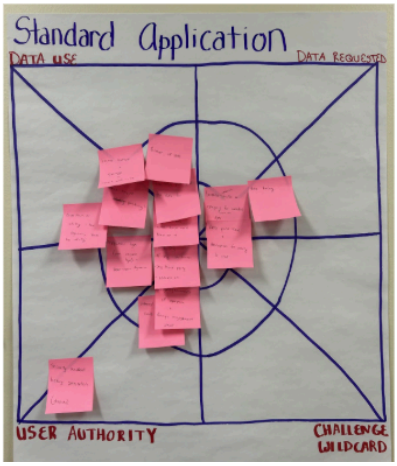
- Individual requester's name.
- Requester's company or organization (if applicable).
- Anyone else who would need access to the data (including third parties).
- Project description and justification.
- Requester's preferred method/medium of accessing data.

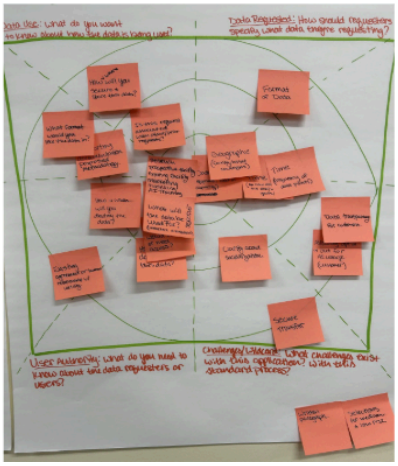
Participants also suggested providing an informational sheet to applicants, which would give an overview of the application process and data risk categories. This would help set requesters' expectations about how their application will be assessed.

Standard Application Small Group Activity

This activity focused on what information utilities need from requesters to thoroughly review a data request. In small groups, Converge facilitated a "What's on Your Radar?" activity, where participants brainstormed and categorized potential application questions as 'essential' (the center of the radar), 'nice to have' (the inner circle of the radar), and 'luxury' (the outer radar ring).







The activity emphasized the importance of data security, ease of use, and overall navigability of the application. The groups then reconvened for a large group discussion. Points of general agreement are captured below. See Attachment B for full notes from the activity.

Essential

Participants agreed that the standard application should strike a balance between providing the utility with enough information to perform a risk analysis without being overly burdensome for the requester. The large group discussion resulted in these five data request fields being categorized as essential for the risk analysis process:

- If anyone beyond the initial requester will be using the data, including third parties.
- A demonstrated need or justification for the data.
- Data type (e.g. equipment, load, capacity).
- Validation of a passed background check.
- Period of time the requester needs the data for.

Nice to Have

If the following items would not be overly burdensome, utility participants indicated that they could assist in the risk analysis process:

- If the data will be used in derivative products, especially if those products will become public.
- Data handling and sharing practices and policies of the individual or organization.
- If the data will be utilized by Large Language Models and other AI tools.
- If there will be future recurring requests related to the immediate request.
- Timing considerations for the requester's project.
- Geographic location associated with the data.
- Time period associated with the data (e.g. the last twelve months, the last three years).
- Type of user (e.g. researcher, developer).
- Country of origin.
- Countries of operation.
- Internal security certifications and policies.
- Data retention and destruction policies.

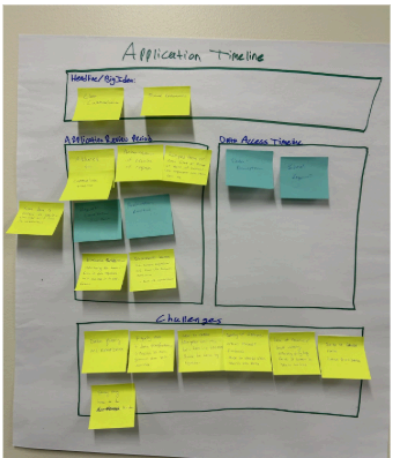
Luxury

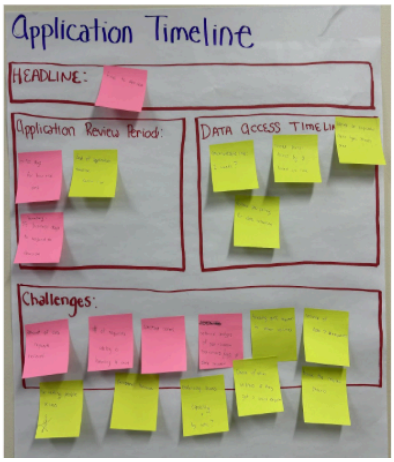
In an ideal process, the following items could be useful to utilities, but are likely too burdensome for a standardized, statewide request process:

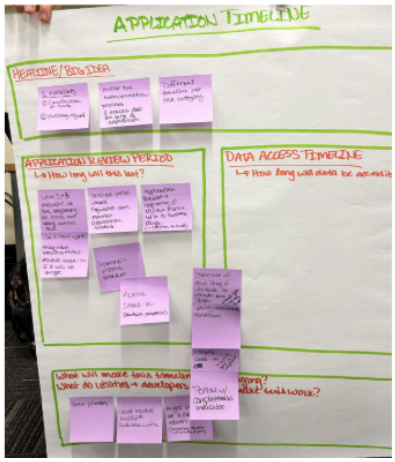
- Cloud analysis.
- The format and granularity of the data the requester is looking for.
- Requester's preferred method of data access, storage, and transmission.
- An attestation related to the requester's and organization's history of security incidents.
- Supporting documentation for the project.
- Any existing agreement or business relationship with the utility.

Application Timeline Small Group Activity

The third activity focused on defining a reasonable and realistic timeline for application processing and data request fulfillment. Discussion started in small groups before transitioning to the large group. Participants were asked to determine a reasonable timeframe for reviewing and fulfilling a data request, considering factors such as the risk level of the data, technical or operational challenges, and the requested duration of access. The discussion was divided into four sections: MainIdea, Application Review Period, Data Access Timeline, and Challenges.







A summary of each discussion is provided below. See Attachment C for full notes from the activity.

Main Idea

Participants agreed that clear, consistent communication and shared expectations between data requesters and utilities should be hallmarks of the process, regardless of the timeline. Some participants suggested that there are two distinct timelines to consider in the data sharing process – the application evaluation/risk assessment timeline and the request fulfillment timeline. This distinction was made because participants agreed that application evaluation/risk assessment should be completed within 90 days of submission, while request fulfillment could vary widely based on the risk level of the request, as discussed in workgroup one.

Application Review Period

Participants acknowledged that since this is a new process, timeline expectations should be generous yet reasonable. The timeline could be altered in the future, as the process becomes more established and understood. Overall, state, developer, and utility representatives deemed that a 90 day review period was a reasonable amount of time in which to review an application and determine which risk category it falls into (low, medium, or high, as discussed in Workgroup #1, *Data Protection Capabilities*), given that the following were part of the process:

- An automated receipt of submission.
- Acknowledgement of request within ten business days of submission.
- Point of contact designated by both the utility and the requester.
- Opportunity for open communication about pending requests, alternatives, and clarifications.
- Consistent touch-points and updates on application status.
- Six months to a year for application time-out (e.g. a non-response from a requester to a utility request for additional information or engaging in a discussion about mitigations).

Utility participants were concerned that tracking application status and communicating with applicants would become resource-intensive. In response, the concept of a portal with a status monitoring feature received positive feedback, though it could be costly.

Data Access Timeline

The data access timeline refers to how long a requester can have access to data. Participants acknowledged that these timelines could vary depending on the requester, data type, and risk level of the data. Regardless of access time, all parties will be expected to follow the data retention policies of the utility from whom the data was obtained. However, participants noted that enforcing data access would be difficult, if not impossible, if data is physically handed over to requesters. This is not a concern for certain kinds of low risk data, but could be a significant challenge for data in higher risk categories. Two potential solutions were proposed:

- A downloadable link that expires after a set amount of time.
- A portal with login credentials that expires after a set amount of time.

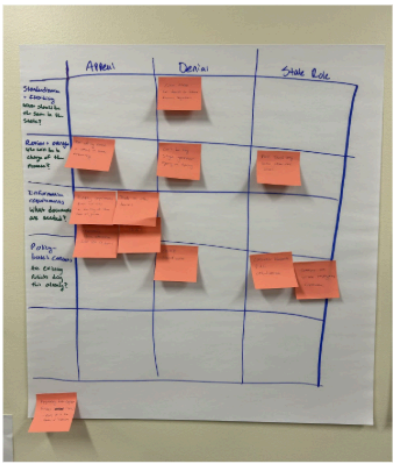
Challenges

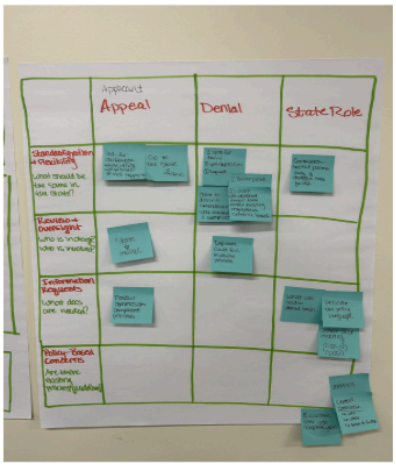
Additional potential challenges associated with the application timeline are summarized below:

- Data quality controls and data transformation can be time-consuming, expensive processes. The question of who bears the financial and administrative burden was a primary concern, with some participants suggesting that the cost-causer should pay.
- Utilities of all sizes were concerned about the potential number of requests and their ability to absorb a potential increase in workload. Some utilities may not have the ability to hire additional staff or create a dedicated team to fulfill data requests, meaning that existing employees would take on this work in addition to their full-time jobs. Furthermore, a dedicated data request team may still need input from other business units, depending on the nature of a request.
- Turnover at utilities and requester organizations was considered a hurdle due to the need to re-train and re-vet personnel.
- Enforcing data access is difficult if data is physically handed over to requesters.
- Maintaining awareness of unusual requests and suspicious requesters – within and between utilities – was seen as important, yet potentially difficult to standardize.
- Prioritizing requests was a potential sticking point, as it speaks to issues of equity and fairness. A prioritization framework could help with this challenge.
- Developing an appeals process for denied applications, as well as potential time limits for submitting an appeal.

Role of the Working Group and State Small Group Activity

The final activity once again included small group discussion, followed by a read-out and discussion with the full group. Participants considered what role state agencies, utilities, and requesters might play in an appeals process. They discussed how application disputes should be communicated, how the process would remain fair, and whether there are any existing procedures or policies that might inform the process.





A summary of the discussion is provided below. See Attachment D for full notes from the activity.

Denial of Request

If a data request application is denied, participants agreed that clear reasoning should be provided to the requester. This could constitute an email with the following components:

- Clear, criteria- and policy-based reasoning for the denial, citing the established risk tiers (low, medium, or high, as discussed in workgroup 1) and any applicable state or federal regulations.
- An offer to further discuss the request and possible alternatives or risk mitigations.

Utilities suggested that they should keep records about each requester to track the number and type of data requests a single entity makes. This information could help identify potential security issues arising from aggregation of data by a single party.

Appeal of Denial or Decision

Participants broadly agreed that requesters have the right to ask for clarification on a denial and expect a timely answer. Two primary appeals processes were suggested:

- An internal process, where the denied requester appeals to the utility, and the utility handles the process, relying on general counsel and Subject Matter Experts (SMEs).
- An external process utilizing the existing PUC complaints process.

Those who favored early PUC involvement – with no utility-hosted appeal process – noted potential unfairness with a utility reviewing its own decision to deny an application and that the review may be perfunctory as the utility may be unlikely to reverse its initial decision. Those who favored an internal, utility-owned process believed that discussions between the requester and utility should solve most issues, with only extreme circumstances requiring intervention from the PUC. Regardless, workshop participants agreed that utilities and requesters should make every effort to resolve disputes through discussions and mitigation efforts before entering an official appeals process.

Role of the State

While any individual has the right to file a complaint with the PUC at any time (as long as it complies with Rule 7829.1700) and that the PUC should have a role in the appeals process as it relates to this data sharing framework, there was acknowledgement that the PUC is over-burdened and should only be asked to review highly-contested, high-importance cases. Participants from state agencies pointed out that the Consumer Advocate, the Interconnection Ombudsperson, and the Commissioner of Commerce also have the authority to review such cases.

Participants agreed that the party seeking appeal should initiate the process and provide justification for the appeal. Additionally, there was general agreement that utilities should provide the following:

- Specifics on what led to the denial, including policies or statutes that the request violated.
- Information on previous requests made by the appealing party, if they demonstrate that the request in question constitutes a higher risk level based on data the appealing party has already received.

Utility participants noted that there are pre-existing policies that an appeal process must account for. For instance, Minnesota Statute 13.37 outlines general non-public data, and all Complaints must comply with Rule 7829.1700. Additionally, utilities expressed that if fulfilling a data request would violate CIP-014 or similar policies, they would not be able to discuss specifics in a public forum and would request moving to a closed-door session.

Function of Application Process

The purpose of a standard application process is to streamline and improve the application experience for both requesters and utilities. A well-defined process may even alleviate some of the concerns about the financial and administrative burden of data sharing by making the process more efficient. An important component of the process is a common data request application across all utilities. From the requesters' perspective, the common application provides clear expectations of the required information and assurance that the process will be similar regardless of which utility they request data from. From the utility's perspective, each application field helps them interpret grid and personal/organization risk. Table 1 below provides examples of how the application fields should be used to determine risk.

Table 1: Grid Versus Personal Risk Interpretations In Grid Data Request Applications

Grid Risk	Personal Risk
• Requested data points are protected by external policies making them unsharable (e.g., national security, Critical Energy Infrastructure Information (CEII), NERC Critical Infrastructure Protection (CIP), etc.). • Requested data points are individually categorized as low risk, but reach higher risk when aggregated. • Requester's background poses some legitimate risk (e.g., company is owned or operated by foreign entity, no prior history in the energy sector, etc.). • Requester asks for extra information that is normally irrelevant to typical or similar data requests. • Requester's project is inappropriately sited (e.g., too big, too small, or not needed in a portion of the grid).	• Requester has personal or organizational history of cybersecurity incidents, or is unwilling to comply with reasonable cybersecurity protections. • Requester's project poses business risk to the utility, including connecting resources normally installed by the utility or providing energy to utility customers. • Requester does not sufficiently disclose how data will be used or stored, and by whom. • Requester has submitted multiple, simultaneous requests, especially without prior notice to utility. • Requester asks for data (in a specific format or type) that the utility does not keep data in (i.e., data not in digestible format).

Attachment A: Pre-Step Application Small Group Activity

An *Importance/Difficulty Matrix* is a visual tool for prioritizing features by plotting them on a two-dimensional grid. The horizontal axis represents the importance of that feature, and the vertical axis represents the relative difficulty of implementing the feature. This activity helped participants think through the pre-application process and how a requester is vetted prior to submitting a data request application.

Group 1

Quadrant	Requirement
High Importance, Low Difficulty	• Participants agreed that verifying the identity of the requestor will be critical. • Requestors should include the name of their company and information on the project they are requesting data for. • Requestors should list all others who will be using the requested data.
High Importance, High Difficulty	• Participants would like to include an acknowledgement form or other form of consent for recompense for misuse/disclosure of data. • Participants would like to be able to assess the security of the requestor's organization, including understanding internal data protection policies and cybersecurity program maturity.
Low Importance, Low Difficulty	• There should be guards against frivolous, high-frequency requests [borderline with high/low].
Low Importance, High Difficulty	• Participants wanted to understand why requestors were requesting that data, and potentially show proof of need. • There should be disclosure of relevant authorities governing data/energy/infrastructure security. Additional legislation may be needed • Existing discovery protocol. • Requestors should be subject to OSINT research, including for past cyber incidents.

Group 2

Quadrant	Requirement
High Importance, Low Difficulty	• Requesters should specify their preferred data access method. • Requesters should detail the justification for why they need certain data, but there are concerns that review of this is subjective.

	• An information sheet about data tracking and risk levels should be provided so requesters know ahead of time what they're asking for. • Names of the people who will be using the data, along with any third parties should be provided.
High Importance, High Difficulty	• There should be data handling training required, but there were questions about who would enforce this. • Requesters should send security-related certifications or self-attest to training. • Review of the pre-application would likely be done by the utilities, but there may be personnel constraints. • The purpose of the pre-step application should be to triage review in order to define expectations and make a profile of the requester.
Low Importance, Low Difficulty	• N/A
Low Importance, High Difficulty	• Participants preferred the state to handle the pre-application process, but utilities could too. • There should be a standard process handled by the utility. • The initial query should pull basic information that allows requesters to analyze the costs and benefits of their request.

Group 3

Quadrant	Requirement
High Importance, Low Difficulty	• Third-party verification via background check was seen as essential to vetting potential applicants (individuals and organizations). Utility participants indicated that they use these kinds of services regularly and have existing vendor relationships. • Utility members expressed the importance of clarifying that the third party vendor does not make the decision about whether an individual 'clears' the background check – that responsibility would lie with the utility from whom the individual or entity is requesting information. • Maintenance of a website-hosted list of third-party vendors by the state for data requesters to utilize was posed as something that would be helpful for requesters and an important security component. • Having a reasonable period of time for the validity of a verification/background check was seen as an essential security measure. Three years was posed as an amount of time that seemed reasonable from a security and requestor convenience perspective.
High Importance, High Difficulty	• Creating a new process may require utilities to hire additional employees to handle the additional work. While it is important to have sufficient personnel, getting approval and funding for those positions was identified as a significant challenge.

Low Importance, Low Difficulty	• The state owning the initial vetting process was placed in this quadrant because utility participants were of the opinion that this was not something necessary for the process to run smoothly, as they have significant experience vetting individuals and organizations.
Low Importance, High Difficulty	• Blank.

Attachment B: Standard Application Small Group Activity

"What's on Your Radar?" is a design thinking activity where participants use a concentric-circle diagram to plot ideas according to their importance, with ideas closer to the center receiving higher priority. This activity helped participants categorize the information utilities are seeking from data requesters as 'essential,' 'nice to have,' and 'luxury'. The goal was to identify what a utility must know in order to evaluate risk and review data request applications, while maintaining a simple and navigable request process.

Group 1

Quadrant	Essential	Nice To Have	Luxury
Data Use What do you want to know about how the data is being used?	• N/A	• Utilities would like to understand why the data requested is necessary for the requestor's project.	• Cloud analysis. • Requestors should detail the specific type of project the data they are requesting is for. • Requestors should disclose if the data will be shared with a 3rd party.
Data Requested How should requesters specify what data they are requesting?	• N/A	• The data should be delivered in a usable format so that screenshots are not required to capture it.	• Requestors should share the data format and granularity they require.
User Authority What do you need to know about the data requesters or users?	• Understanding who exactly will be using the data, such as if it is just the requestor, or if it will be used by individuals across their organization or 3rd party consultants, is essential.	• Requestors should share if the data will be used in derivative products, especially those that may become public. • It's important to know requestor data handling and sharing policies.	• A consent form to take cybersecurity training for certain data types. • Information on requestor security practices, including cyber awareness programs, encryption, and data retention policies.
Challenges/ Wildcard	• N/A	• The application should be as generic as possible to enable widespread use. • Participants were concerned that	• N/A

		requestors may input the data into LLMs and AI tools, which could compromise it. This should be disclosed and/or warned against in the application. • Application questions should tease out if the requested data poses risks to the broader grid or to individuals.	

Group 2

Quadrant	Essential	Nice To Have	Luxury
Data Use What do you want to know about how the data is being used?	• Requesters should justify why they are making the request, and the utility can determine the data they need based on that.	• The application should ask if the requester will be making future or recurring requests. • The application should ask what format the data is in and how long the requester needs access to it for.	• The utility should provide a dynamic form. • Requesters should specify their preferred method of data access, storage, and transmission.
Data Requested How should requesters specify what data they are requesting?	• N/A	• Requesters should specify any timing-related considerations related to their request. • Requesters should specify the location or time of the data they need. • Requesters should specify the datapoint name and description.	• N/A

User Authority What do you need to know about the data requesters or users?	• The form should capture the requester's name, if others in their broader organization will have access to it (and if so, their names), and any third parties that may have access to the data.	• The form should capture what type of user is requesting data. • Requesters should detail their countries of origin and/or countries of operation, and sign a foreign engagement attestation form. • Requesters should share internal security certifications and policies.	• Requesters should sign an attestation related to their history of security incidents, if applicable.
Challenges/ Wildcard	• N/A	• N/A	• N/A

Group 3

Quadrant	Essential	Nice To Have	Luxury
Data Use What do you want to know about how the data is being used?	• Knowing what the data will be used for is essential for risk screening. Ideally, there would be a checkbox – options such as research, prospective facility, existing facility, marketing, modelling, AI – and a short written description.	• Whether or not a request is associated with another request (part of the same project). This was seen as a signal to requesters that utilities are monitoring how many and what kinds of requests an individual or entity is making.	• Knowing where and how the requester will secure and store data. • What format the requestor would like the data in. • Supporting documentation for their project that provides insight into what they plan to do with the information so the utility can know if the format of the data will be useful.
Data Requested How should requesters specify what data they are requesting?	• Knowing the data type – such as equipment, load, or capacity data – is an essential risk screening question.	• Knowing the geographic area that the requested data covers is important for security screening and knowing if the data is available. • Knowing the time period the requester is interested in is important for request fulfillment. For instance, data that is older than utility data	• The format the requester would like the data to be in was considered a luxury, as it may or may not matter, depending on the format the utility keeps the data in.

		retention policies is unlikely to be available. • Understanding the frequency of data points the requester is interested in (e.g. fifteen-minute intervals, monthly, annual, etc.) is important for request fulfillment, as data may not exist at a certain interval.	
User Authority What do you need to know about the data requesters or users?	• Validation that the requestor completed and submitted a background check to the utility and that it passed analysis. • Knowing if the requester is the only individual who would have access to the data or if others in their organization would also need/have access is an important security question, as additional individuals may need to be verified. • Knowing if the requester needs the data for a specific period of time, indefinitely, or on a certain cadence so that proper mitigations can be put in place.	• Assuming that data is handed over to the requester, how and when will the requester/recipient of the data destroy the data.	• Whether or not the requester has an existing agreement or business relationship with the utility.
Challenges/ Wildcard	• Gaining clarity from a requester on how or if they plan to socialize the data and controlling that could be a challenge if data is physically handed over to an entity. • Ensuring secure transfer of data could be a challenge. • As AI becomes a more prevalent tool, requesters may be looking to train an AI with utility data or use it to analyze utility data. Utility participants envision two challenges with this. First, they may receive requests from customers wanting to know if their data was used in AI-related endeavors. The second is that they foresee a time when they need to offer an option for customers to opt-out of their data being used by AI. This would add a layer of complexity to providing data to requesters.		

Attachment C: Application Timeline Small Group Activity

A *Concept Poster* helps guide and organize thoughts around a developing process. In this *Concept Poster*, participants outlined a reasonable timeline for processing applications and fulfilling data requests. This timeline will help set requester expectations for the application review period.

Group 1

Question	Answer
Headline/Big Idea	• Having clear communication and shared expectations that are met by both parties is more important than adhering to a specific timeline.
Application Review Period How long will this last?	• Regardless of the length of timeline, it should be clearly communicated early on and adhered to. • Acknowledgement of request receipt should be made shortly after it's submitted. • There should be an assigned person at each step of the review process or a general point of contact who the requestor can reach out to. • There should be several "stage gates": acknowledgement of application receipt, communication of request completion timeline, and application review. • There should be an evaluation period that provides an opportunity for the requestor and the utility to discuss options if the data requested isn't available or is in a different format than what was requested. • There should be a review for discrepancies between the pre-application requestor and the person who submits the application. • Some data is needed on specific timelines or it loses its usefulness.
Data Access Timeline How long will data be accessible?	• Stage gate: data acceptance.
Challenges	• Data quality, normalization, and transformation may pose issues or be required, particularly if the requested data isn't available. Any costs associated with this should be borne by the requestor. • Studies may have to be re-done in order to provide data, which increases costs for the utility. • Should requestors want to appeal a decision, it should be required to do so within a specific time period. • There are questions on how to deal with a lack of resources and staff capacity, especially at smaller utilities. These problems will become more acute during busy periods or summer/holidays when staff are out of office. • There is a question about how requests will be prioritized and in what order they will be completed. What is fair and what is efficient?

Group 2

Question	Answer
Headline/Big Idea	• What does the timeline to a decision look like?
Application Review Period How long will this last?	• Participants thought that a 90 day review period for low risk data requests was reasonable. • Six months to a year was viewed as a reasonable timeline for application time-out. • Establishing a boundary, such as 15 business days, for responses to a decision was discussed (i.e., issue decision by utility and 15 days for requester to respond).
Data Access Timeline How long will data be accessible?	• Participants brought up that the amount of time that data is accessible for could vary based on the requester, the data type, internal data controls/retention policies, and the access area. • Two ideas for controlling access were proposed – providing a downloadable link that is time-limited and utilizing a portal, to which the requester would have access for a pre-set amount of time. • It was also brought up that all data retention policies need to be followed first.
Challenges	• The number of data requests received could pose a challenge to evaluating and fulfilling requests, especially if there are multiple at one time. • Constant communication with requesters could be a challenge for utilities who do not have personnel dedicated to evaluating and fulfilling data requests. • Additionally, personnel turnover at both utilities and organizations requesting data could prove to be challenging from both an evaluation and security perspective. • Re-vetting people based on circumstances and needs could be logistically challenging. • Enforcing access capabilities once data is provided could be difficult. • There should be a process for utilities to share and discuss the requests they have received so that utilities can be aware of strange requests or if an entity is making multiple requests at multiple utilities. • Tracking the review process without dedicated personnel or some kind of software could prove challenging.

Group 3

Question	Answer
Headline/Big Idea	• Participants identified two timelines in the application process – data request classification and request fulfillment. • Mirroring the framework of the interconnection process, where there are three tracks depending on the size and type of the application, was seen as a potential model. • Participants noted that it is likely that the risk category a request falls into would impact the request fulfillment timeline.
Application Review Period How long will this last?	• As this would be a new process that may need iteration, utility and industry representatives felt that an application receipt and beginning of review notice within ten business days (in addition to the automated submission response) and an overall review period of up to three

	months was reasonable. • Parties envisioned that there would be opportunities for dialog between the requester and the utility during this period with an expectation for timely response to queries. • Open communication and active check-ins during this stage were something developers placed value on. This led to parties discussing the benefits of a hosted portal where requesters can monitor the status of their application and receive updates.
Data Access Timeline How long will data be accessible?	• Group 3 discussed this as being a difficult thing to control, especially if data is physically handed over to a requestor. • The concept of a hosted portal again came up, as it would allow viewing, but not possession of the data, and access could easily be withdrawn after a specified period of time.
Challenges	• New processes can be challenging as they are utilized and refined. • Utility participants pointed out that multiple business units could have a role in evaluating and fulfilling requests, which slows down and complicates the process. • Additionally, utilities may not have the resources to create a team dedicated to data request evaluation and fulfillment. Therefore, these tasks would be performed by existing employees in addition to their regular, full-time jobs, which presents time and resource challenges.

Attachment D: Role of the State Small Group Activity

The *Creative Matrix* is an activity that helps facilitate discussion and organize thoughts around a concept or process that has multiple components and considerations. For this *Creative Matrix*, workshop participants discussed what role the State of Minnesota may have in adjudicating disputes over denied data applications and what information would need to be communicated with an emphasis on fairness and timeliness.

Group 1

	Appeal	Denial	State Role
Standardization and Flexibility What should be the same throughout the state?	• N/A	• If an appeal is denied, the reason for the denial should be clearly communicated so that requestors can successfully request data in the future and avoid continued missteps	• N/A
Review and Oversight Who is in charge? Who is involved?	• Participants agreed that if a utility reviews its own decision, it may seem perfunctory to a requestor, who would not expect that the utility would reverse their own decision.	• No single government agency can provide review and oversight alone, because the different expertise of different agencies will be required to effectively provide review and oversight for energy security issues.	• The PUC is already overburdened and should only review the small percentage of cases that are "close calls" or have heightened importance.
Information Requests What documents/information are needed?	• Utilities should report information on previous requests for appeal. This could help determine whether a single requestor has been making frivolous appeals, if there is a specific part of the application process that has tripped up	• Utilities should share information on previous denials, which would provide insight into whether requestors are making frivolous appeals, a particular stage of the application process is posing issues, or if utilities are	• N/A

	requestors, or other information that may be valuable for evaluating both an appeal and the process writ large. • Utilities should share which step of the application process led to the initial denial.	overzealously denying requests.	
Policy-Based Concerns Are there existing policies/guidelines?	• MN statute 13.37 defines general non-public data. • The existing regulatory data request process may be illustrative, and parts of it useful, for designing a new appeals process.	• Existing frameworks like CEII and classifications (i.e. Secret, Confidential, etc.) will be instructive and offer a clear reason for denial of certain requests.	• Several entities already exist to adjudicate these issues, including the PUC, the Consumer Advocate, and the Interconnection Ombudsperson. • The Commerce Commissioner can initiate investigations.

Group 2

	Appeal	Denial	State Role
Standardization and Flexibility What should be the steam throughout the state?	• Justification for the appeal. • Appeals can only happen on disputed items and as an option of last-resort. • Parties should discuss the issue to try to provide reasonable mitigations, such as sanitization of data or partial data access.	• Utilities should provide clearly defined justification for a denial (e.g., policy, etc.). • When able, utilities should provide reasonable mitigations as part of denials.	• It was brought up that any complaints can only happen if they meet Rule 7829.1700. • The view that the state should step in when an entity is looking to appeal multiple denied requests.
Review and Oversight Who is in charge? Who is involved?	• The internal legal team with support from SMEs. • The regulatory compliance team.	• The individuals or teams who initially reviewed the application. • General Counsel team.	• Utility participants thought that there should be a 'blacklist' of bad requesters (e.g., don't follow data protection guidelines, erroneous requests,

			etc.) that the PUC maintains. Utilities would report bad requesters to the PUC for addition to the list, and any MN utility could access the list at any time. Developer participants expressed reservations about the prospect of utility-determined lists with few guiding structures. • The idea that the MN Fusion Center could get involved to issue security notifications related to bad requesters was floated.
Information Requests What documents/information are needed?	• Evidence of why the denied party wishes to appeal their case.	• A clear timeline for the appeal process needs to be set. 90 days was suggested as a potentially reasonable amount of time. • Any historic issues with the requester need to be tracked and presented, such as too many requests or rising risk level due to aggregation. • Again, a clear justification for why the request was denied was very important to developer representatives.	• N/A
Policy-Based Concerns Are there existing policies/guidelines?	• Developer representatives were concerned about the success rate of appeals.	• N/A	•

Group 3

	Appeal	Denial	State Role
Standardization and Flexibility What should be the steam throughout the state?	• Participants agreed that requesters can ask for clarification, which the utility will provide. If the requester is still unsatisfied, they can utilize the MNPUC complaints process.	• Group 3 identified two points where denial might happen – during the pre-application verification and during request evaluation. • Participants agreed that for the first denial situation, a standardized email message would be appropriate. For the second situation, a more personalized email that offers an explanation of denial that conforms with existing regulations and is criteria-based would be better. • Additionally, the more personalized email explaining request denial should offer further discussions to find alternatives.	• Participants agreed that the MNPUC has a role to play in settling disputes that cannot be resolved through dialog, utilizing the existing complaints process.
Review and Oversight Who is in charge? Who is involved?	• There was agreement that if a situation escalates to using the MNPUC complaint process, the MNPUC is then in charge of oversight.	• Utilities found it difficult to say who at their organization would oversee this process, as a single request could involve multiple business groups and could fail multiple policies.	• MNPUC
Information Requests What documents/information are needed?	• All items typical in a formal Commission complaint investigation.	• N/A	• Requesters would be responsible for submitting the initial complaint petition. • Utility representatives said they would be willing to provide at least the information that was provided in the denial email and the language of the

			• policy that they determined the request violated. • Utility representatives said that in some cases, such as a request that would violate a CIP-14 or DOD policy, they would not be able to provide any information in a public forum or filing. Instead, they would request a closed-door meeting.
Policy-Based Concerns Are there existing policies/guidelines?	• N/A	• N/A	• In addition to the existing MNPUC complaints process, it was raised that utilities will need to adhere to existing standards, such as CIP-014 and DOD regulations.

APPENDIX C: October 2025 After Action Report

Minnesota Grid Security Study: Use Case Analysis Workgroup

After Action Report

October 2025

Minnesota Department of Commerce
Jessica Burdette
jessica.burdette@state.mn.us

Converge Strategies
Jonathon Monken
jmonken@converstrategies.com

Table of Contents

Executive Summary

On 6 October 2025, the Minnesota Department of Commerce ("Commerce") convened stakeholders involved in Docket No. E-999/CI-20-800 (*In the Matter of a Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data*) for an in-person workgroup focused on validating and refining the data sharing framework developed in Workgroup Sessions 1 and 2, by developing use cases based on sample grid data requests. A total of twenty-three participants, representing twelve Minnesota state offices, utilities, non-profit organizations, and private energy infrastructure developers, attended the workshop, which was facilitated by Converge Strategies, LLC ("Converge").

During this workshop, participants discussed:

- Use cases (scenarios) that tested the Grid Data Sharing Framework draft outcomes form Workgroup Sessions 1 and 2.
- Areas of convergence and divergence in the Grid Data Sharing Framework draft.

The Use Case Analysis workgroup session was the last in a series of three, which were designed to inform the creation of a standard grid data sharing framework. This After Action Report (AAR) summarizes key findings from the session, but does not provide final recommendations regarding Docket 20-800.

Following this workgroup session, Converge hosted a virtual outbrief for parties who were unable to attend in person. A similar outbrief was held after the two previous sessions to share the discussions and outcomes with interested parties.

Key Findings

Attendees were encouraged to treat the use case scenarios as an opportunity to test the draft Grid Data Sharing Framework and clarify what factors and mitigations would cause risk levels to the system to increase or decrease, while considering the suitability and feasibility of data protection measures. Throughout the day, participants alternated between small group discussions, focused on evaluating the risk of various use case scenarios, and large group consensus-building conversations, where participants reported on their small group discussions and highlighted points of agreement or disagreement.

Key takeaways from the discussions are summarized briefly below; more details are available in subsequent sections and in the appendices.

The Role of Business Agreements. Workgroup participants agreed that all data-sharing should be accompanied by a business agreement (e.g. NDAs, data sharing agreements). However, while it was agreed that NDAs would likely be required in most data-sharing situations, they may not lower the risk level of sharing data based on the information being requested. More robust business agreements, like data sharing agreements, could be used in addition to or lieu of NDAs. If the terms of a data sharing agreement were sufficiently robust and tailored to individual situations, they could decrease the risk to the system of sharing data to an acceptable level, especially when combined with other mitigation strategies. The

content and format of agreements also provides an opportunity for stakeholder alignment with the creation of a standardized template for NDAs/Data Sharing Agreements.

Risk Evaluation Lens. Evaluation of the risk level of the components of a data request (described on p. 9) revealed several methods to evaluate risk and a variety of risk drivers. Participants agreed that for the purposes of the Grid Data Sharing Framework, the risk level of requests should be evaluated based on risks to security, the integrity and reliability of the distribution grid, and public safety. Corporate and business risks were deemed out-of-scope for this effort.

Mitigation Options are Dynamic. There is rarely a single mitigation that will effectively protect shareable data. Rather, the mitigation options discussed by participants (listed on p. 9-10) are flexible, scaleable, and can be layered depending on the risk level of the request. This approach would provide structure and consistency, while still providing flexibility for stakeholders.

Vetting Requesters is Essential. To ensure the safety and reliability of the grid, it is critical that requesters (individuals and companies/organizations) be vetted. All individuals who will handle the data should undergo a background check to verify that they are who they say they are, are connected to the company/organization they claim to be from, and don't have anything in their history that could pose a security risk. Companies/organizations should undergo vetting to ensure they are legitimate, are legally able to do business in Minnesota, and do not have ties to foreign entities of concern.

Secure Sharing Methods. Secure sharing and storing of data is an important mitigation method. However, this becomes challenging to assess and keep consistent when requesters have differing capabilities. Participants agreed that a secure portal could be the simplest, and most uniform method of sharing data.

Details Matter. The granularity of requested data, the number of years requested, and the intention of a requester to make the data public in the form of a report or derivative product all have a significant impact on risk level. Additionally, while the reason for the request was not a comparatively significant driver of risk, alignment between it and the requester's mission and/or request offers a point of triangulation—if a project is grossly out of alignment with the requester, it could be a red flag. Data being used for specific and finite projects also impacts risk, as well as if data would be put into a Large Language Model (LLM), as LLMs can aggregate disparate data, potentially compounding risk.

Working Group Background

Following Xcel Energy's 2019 Hosting Capacity Analysis (HCA) Report (Docket No. E002/M-19-685), the Minnesota Public Utilities Commission ("PUC") initiated orders to address concerns around the electrical distribution grid and customer data security between July 2020 and June 2023. This culminated in the establishment of a working group. This working group met during a series of workshops from July to September 2024.

In response to the June 2023 Order, Converge was hired in Summer 2024 to provide services and recommendations to the Commission regarding open topics in the docket. Converge reviewed infrastructure security policies and risk assessment frameworks, researched cyber

and physical security risks to grid infrastructure and supply chain vulnerabilities, conducted interviews with stakeholders involved in the docket to gather insight on the current status of grid data sharing, and provided recommendations for the structure and content of future workgroups. Converge wrote a report ("Minnesota Commerce Grid Data Sharing Report") on those efforts and submitted it to the PUC for an open comment period in November 2024.

The PUC accepted the report in February 2025 and directed the working group to continue and provide recommendations for a secure data sharing process for DER interconnection.

Timeline

Converge led stakeholders through a series of three workgroup sessions to inform a standard grid data sharing framework for Minnesota:

- **Data Protection Capabilities.** Focused on developing data protection categories and criteria for categorizing data based on level and type of risk.
- **Data Sharing Mechanisms.** Focused on developing a structure for a standardized data request process based on best practices.
- **Use Case Analysis.** Focused on validating the data sharing framework developed in previous workshops by developing use cases of sample grid data requests.

Following each workgroup session, participants had the opportunity to provide comments on the AAR to ensure that the conversations were accurately reflected. Additionally, each session had a virtual outbrief for those who could not attend in person and were interested in updates. While clarifying questions and comments were welcome in the AAR review period and virtual outbrief, they were not an opportunity for parties to reinterpret previous comments or add new considerations. Workgroup activities followed, and will continue to follow, the timeline below:

Topic	Event	Date
Data Protection Capabilities	*Workgroup (Complete)*	*July 7, 2025*
	Virtual Outbrief (Complete)	July 18, 2025; 10-11AM CT
	Report Comment Period (Complete)	July 24 - August 4, 2025
Data Sharing Mechanisms	*Workgroup (Complete)*	August 11, 2025
	Virtual Outbrief (Complete)	August 22, 2025; 11AM-12PM CT
	Report Comment Period (Complete)	August 27 - September 8, 2025
Use Case Analysis	*Workgroup (Complete)*	October 6, 2025
	Virtual Outbrief (Complete)	October 17, 2025; 11AM-12PM CT
	Report Comment Period	October 22 - November 5, 2025
Final Report	Final Report Comment Period	January 9 - 22, 2026

Summary of Working Group 3: Use Case Analysis

Objectives

The goal of the Use Case Analysis workshop was to validate and refine the draft Grid Data Sharing Framework developed in Workgroup Sessions 1 and 2. To achieve this goal, this workgroup session had four objectives:

1. Test the draft Grid Data Sharing Framework developed in Workgroups 1 and 2 with use cases based on sample grid data request scenarios.

2. Understand the conditions that would cause risk levels to increase or decrease, and how that impacts grid data sharing outcomes.

3. Evaluate the draft Grid Data Sharing Framework, including the application, to determine the suitability and feasibility of its requirements for stakeholders.

4. Clarify which aspects of the draft Grid Data Sharing Framework stakeholders were in agreement on, and around which points there was less clarity.

Participants

The Use Case Analysis workgroup session convened a total of twenty-three participants from twelve state offices, utilities, non-profit organizations, and private energy infrastructure developers:

- Minnesota Attorney General's Office
- Minnesota Public Utilities Commission
- Minnesota Department of Commerce
- Minnesota Information Technology Services (MNIT)
- Minnesota Solar Energy Industries Association (MnSEIA)
- Citizen's Utility Board
- Clean Energy Economy Minnesota
- U.S. Solar
- R Street Institute
- Fresh Energy
- Dakota Electric Association
- Minnesota Power
- Otter Tail Power
- Xcel Energy

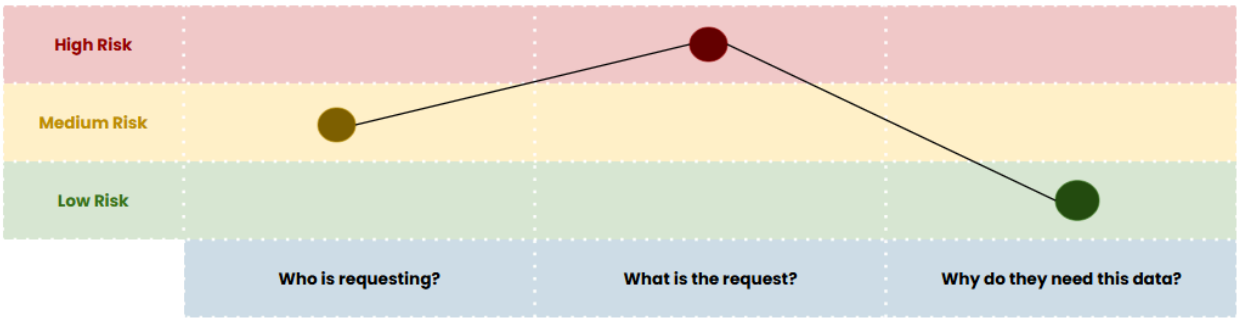
Use Case Risk "Curve" Development

For this activity, stakeholders were assigned to small groups with varied representation from utilities, developers, non-profit organizations, and representatives from Minnesota security and regulatory agencies. Each group was given a use case scenario, which they could modify, if desired. Stakeholders were asked to work together to determine the relative risk level—high, medium, or low—of the following elements of the use case:

- **Who.** The individual making the data request, the organization they were from (if applicable), as well as any relevant third parties (if applicable).
- **Request.** What data the requestor is asking for, including, but not limited to, data type(s), corresponding geographic footprint, and data age.
- **Why.** The reason or project the requestor is making the data request for.

The relative risk level of each element was plotted on a chart to develop the risk "curve," where the highest level of risk determined the overall risk level of the use case. *Figure 1: Use Case Risk "Curve" Example,* below, provides an example where the requester is a medium-level risk, the data being requested is a high-level risk, and the reason the requester wants the data is a low-level risk, resulting in an overall high-level risk.

Figure 1: Use Case Risk "Curve" Example



Once the relative risk curve of the use case was determined, stakeholders were asked to discuss and apply the following mitigations (which were identified in Workgroup session 1) to the situation in an effort to bring down the security risk of sharing the data:

- NDAs
- Attestations
- Business Agreements
- Requester Vetting
- Enforceable Accountability Mechanisms (e.g. penalties, legal protections for breaking agreements or terms of use)
- Data Access Time Limits
- View-Only Capabilities (i.e. non-downloadable, secured portals)
- Data Encryption
- Data Handling Training
- Cybersecurity Guidelines/Training
- Background Checks
- Data Scrubbing/Sanitization
- Data Aggregation (in some cases, to obscure customer or system details)
- Secure Portal
- On-Site Viewing of Data

This activity was done twice—once with a low-risk use case and once with a medium-risk use case. A summary of the discussion is provided below. See Attachment A for full notes from the activity.

Low-Risk Use Case

Each group was given a use case scenario, which they could modify if desired. While the scenario might not have represented an overall low system-level risk, the goal was to apply mitigations that would bring the risk of sharing grid data down to a low-risk level, as defined in Workgroup Session 1.

Group 1

Group 1's first use case was:

- **Who.** Community Power, a Minnesota-based non-profit.
- **Request.** Historical data on locational outages in the metro area.
- **Why.** To assess distribution system reliability and equity impacts.

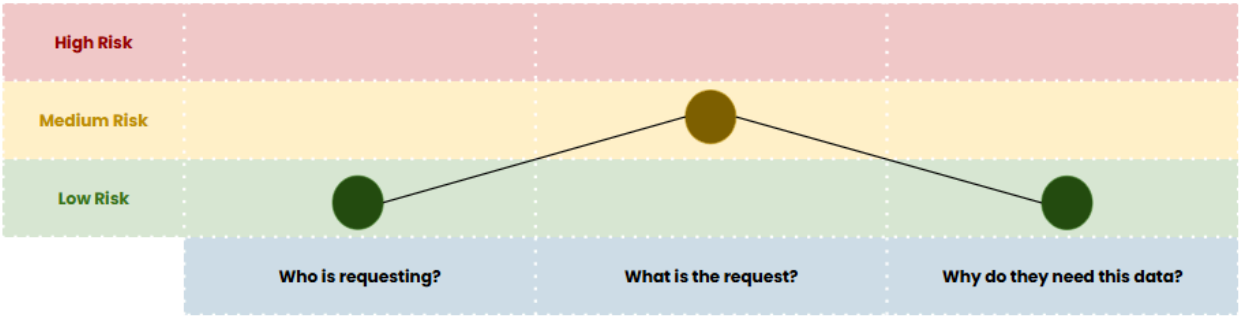
Who. The discussion of the risk level of the 'who' centered around not only the requesting organization, but the individual making the request. Broadly, it was decided that the risk level of the requester organization would depend somewhat on the level of familiarity the utility had with the requestor. For instance, the requester would be low risk if the organization was known in the industry and/or to the utility and if there was some familiarity with them and their work. However, the risk level could rise if the individual making the request could not be tied to the organization they claimed to be from. Ultimately, the group deemed the 'who' in this case to be a low-risk requester.

Request. Whether the request would be low- or medium-level risk depended on the granularity of the data, the number of years the data was being requested for, and if it included the current year, as trends that could expose vulnerabilities become more apparent as more data is provided. It was concluded that in a situation like this, if the data did not include the current year, it would pose a lesser risk. However, for purposes of this activity, the group decided that the request would be categorized as a medium-level risk, due to the potential granularity being asked for.

Why. Participants noted that the 'why' matched the requester's organizational mission. While this in and of itself does not lower risk, the converse – a mismatch between the requesting organization's mission and the request – could be cause for alarm. However, utility representatives noted that some specific elements of this data request might not be collected by the utility at this time, which would make it unavailable, unless the requester was willing to pay for its collection.

Risk Curve. Based on this discussion, the overall request was categorized as a medium-level risk and is shown in *Figure 2: Group 1 Low-Risk Use Case Risk "Curve"* below.

Figure 2: Group 1 Low-Risk Use Case Risk "Curve"



Mitigations. The security of the data was the most important factor when it came to applying mitigations. Utility members in this group said that the utility would need to be comfortable with the requester's security protocols. While this could be a subjective determination, it was suggested that a secure portal could be used for the requester to access the data if the utility was uncomfortable with their security protocols. It was also agreed that an NDA or some other kind of agreement would be needed, and that the kind of agreement should be appropriate to the overall risk level of the data being shared to the grid. Given that those mitigations were applied, the group did not see any reason why a data request similar to this one could not be shared, provided that the individual, their organization, and any third parties involved passed background checks and verification.

Group 2

Group 2's first use case was:

- **Who.** MN Center for Energy and Environment (CEE), a Minnesota-based non-profit. They plan to work with graduate students at the University of Minnesota who are doing a capstone project.
- **Request.** Data on areas with limited redundancy.
- **Why.** To study potential areas for siting microgrids.

Who. As with Group 1's first use case, there were multiple people and entities involved that needed to be evaluated. Since the organization was well-known to utilities, the group deemed it to be a low-risk requester. However, there was ambiguity about the risk posed by the University of Minnesota students, mostly driven by whether or not the students would know how to properly protect and use the data being requested. There was also discussion regarding their legal liability (i.e., if they would be covered under MNCEE's agreement with the utility or if they required separate ones). Ultimately, this was categorized as a medium-level risk.

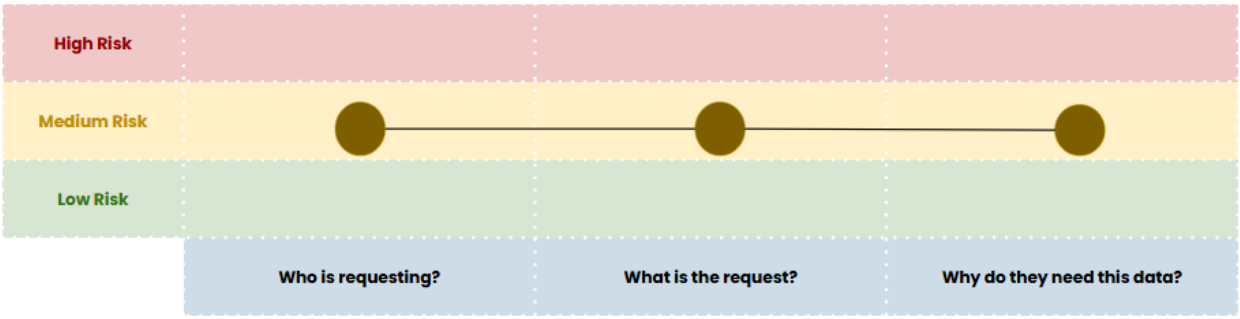
Request. The students' project requires data on areas with limited redundancy for the utility's entire system. This was concerning due to the volume of the request and because having this level of data in a public forum presents a significant risk to the grid by publicizing its weakest points. It should be noted that the group clarified that the age of this data would not matter, because even if they provided the students with data from five years ago, there are some parts of the system that may not have changed since then, making the data technically

current. However, due to the varied nature of this data (being about specific parts of the system and not all), the group categorized the request as a medium-level risk.

Why. The group questioned whether or not the students needed this data to achieve their stated purpose and if they could accomplish their project with publicly available data. The group also determined they would need to know how the students were going to use the data and present their findings. It was assumed that based on real-life experience, the students would publicly present and publish their findings on their university's public portal. Therefore, the group categorized the project justification as a medium-level risk.

Risk Curve. Based on this discussion, the overall request was categorized as medium-level risk and is shown in *Figure 3*: *Group 2 Low-Risk Use Case Risk "Curve"* below.

Figure 3: Group 2 Low-Risk Use Case Risk "Curve"



Mitigations. The group concluded that a case like this could likely be mitigated to a low-level risk. This would involve requiring access through a secure utility portal. There would also need to be legal protections, including some form or combination of NDA, attestation, and/or business agreement with the non-profit and the university, including language about how the data can and cannot be used. In a real-life situation, it would need to be determined whether the students would enter into an NDA via their university, via the NDA with MNCEE, or directly with the utility. There was also discussion about the amount of scrubbing that may be needed in a case like this to make the risk to the grid more decidedly low-level, and whether that would make the data less useful to the students.

Group 3

Group 3's first use case was:

- **Who.** Contractor working on behalf of a Tribal Government in Minnesota.
- **Request.** Data on daytime minimum load, peak load, and load shape for the past three years.
- **Why.** To design a microgrid.

Who. The group discussed at length the relationship between the contractor, the Tribal Government, and the utility, and how that informs risk. Utility representatives said that the relationship between the contractor and Tribal Government would have to be officially confirmed and documented before moving forward, and that even if there was a good relationship between the utility and the tribe, it would be the contractor that would drive the risk level. For purposes of the exercise, the group decided that the 'who' of this use case would

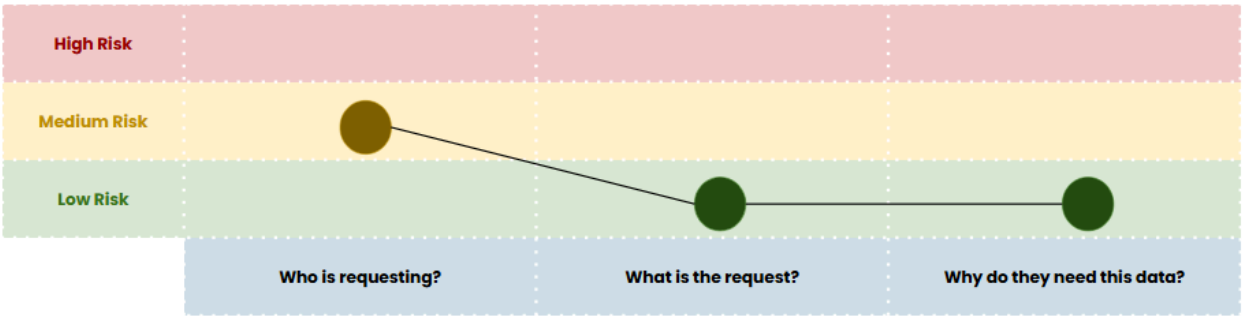
be classified as a medium-level risk, as there might not be a prior relationship between the contractor and utility.

Request. The request itself was deemed to be a low-level risk for two reasons 1) the data belongs to the Tribe, so they are entitled to use it, and 2) because some of the information being requested is publicly available. However, utilities noted that load shape data may be difficult to provide, as it might not be available.

Why. The group agreed that the stated project posed a low-level risk to the system, as the data will be used for a discrete and finite project.

Risk Curve. Based on this discussion, the overall request was categorized as medium-level risk and is shown in *Figure 4: Group 3 Low-Risk Use Case Risk "Curve"* below.

Figure 4: Group 3 Low-Risk Use Case Risk "Curve"



Mitigations. The group agreed that no matter what the overall risk a request posed to the system, an NDA or similar agreement would be needed, even if it didn't re-categorize the risk to the system to a low-level risk. For this particular example, the group agreed that to bring the risk to an acceptably low level, there would need to be a business agreement between the utility and the contractor and a data release consent form signed by the Tribe. The group also agreed that a secure portal would be the safest way to share the data, given that they don't know the cybersecurity capabilities of the contractor and that it would be difficult to assess that.

Medium-Risk Use Case

Each group was given a use case scenario, which they could modify if desired. While the scenario might not have represented an overall medium system-level risk, the goal was to apply mitigations that would bring the risk of sharing grid data down to a medium-risk level, as defined in Workgroup Session 1.

Group 1

Group 1's second use case was:

- **Who.** A Minnesota-based solar developer.
- **Request.** Peak load values for three substations in Minnesota, one of which is regulated under NERC CIP-014.

- **Why.** To assess feasibility, cost, and impact of a solar + storage facility for a municipality.

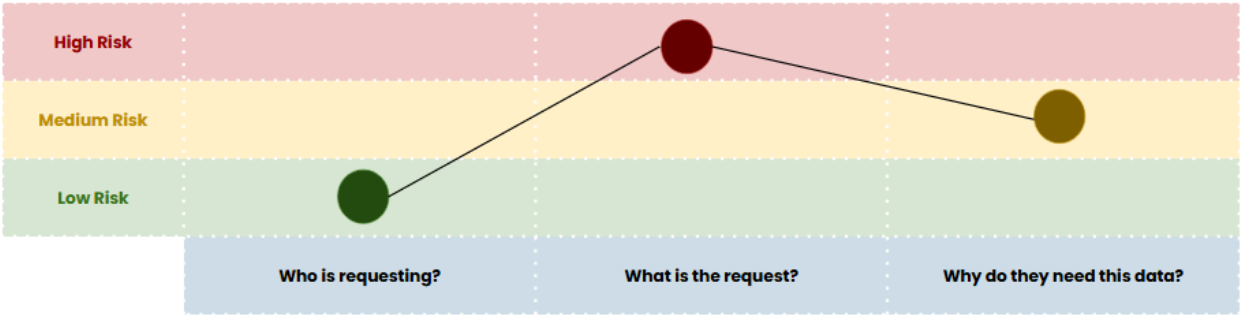
Who. Based on the assumption that a Minnesota-based solar developer would be unlikely to have ties to foreign entities, the group classified them as a low-level risk. However, there was discussion around the importance of vetting both the requesting organization and individual requester, including background checks for anyone who would be handling the data, for due diligence.

Request. The request itself spurred discussion about how to appropriately address data requests that include information on sites regulated under NERC CIP-014[13]. This included debate on whether the request could even be partially fulfilled, as simply omitting the data from the CIP-014 substation, but providing data on the other two substations, could reveal its criticality. There was also uncertainty around whether there would be other security-related designations placed on the CIP-014 substation and if the language of CIP-014 itself precluded sharing of any data related to the site.[14] Ultimately, the group decided to classify this request as a high-level risk.

Why. Because the location of the project – in front of or behind the meter – would impact the visibility the utility had into its impacts on the grid, the group classified the 'why' as a medium-level risk. The risk associated with asset ownership was also discussed, as a municipality may have an obligation to make certain data public, which could increase risk to the grid by increasing visibility.

Risk Curve. Based on this discussion, the overall request was categorized as a high-level risk and is shown in *Figure 5: Group 1 Medium-Risk Use Case Risk "Curve"* below.

Figure 5: Group 1 Medium-Risk Use Case Risk "Curve"



Mitigations. For this use case, the group agreed that an NDA would not lower risk (as NDAs do not ensure long-term compliance), and that overall, there were no mitigation strategies that could result in this situation being a low-level risk to the system. A medium level of risk,

[13] NERC CIP-014 – Physical Security requires responsible entities "[t]o identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within and Interconnection."

[14] Section 6.4 (p. 7) of Reliability Standard CIP-014-3 states that "Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure." The "unaffiliated third party reviewer" refers to the entity selected by the utility to perform the certification of the Requirement R1 risk assessment.

however, could potentially be achieved if the following were utilized: cybersecurity guidelines and training for the requester, a business agreement or other legal agreement that is stronger than an NDA, and scrubbing data to a minimally acceptable level so that all three substations appear the same.

Group 2

Group 2's second use case was:

- **Who.** A California-based solar developer.
- **Request.** Feeder information at a discrete site – daytime minimum load, peak load, and load shape over the last two years
- **Why.** Exploring interconnection of a solar array >1MW (modeling, cost analysis, and design).

Who. Based on the assumption that the solar developer is legally allowed to operate in Minnesota, the group classified them as a low-level risk. However, there was discussion around the legal effectiveness of potential NDAs or business agreements if the developer experiences some sort of security issue involving the grid data outside of Minnesota.

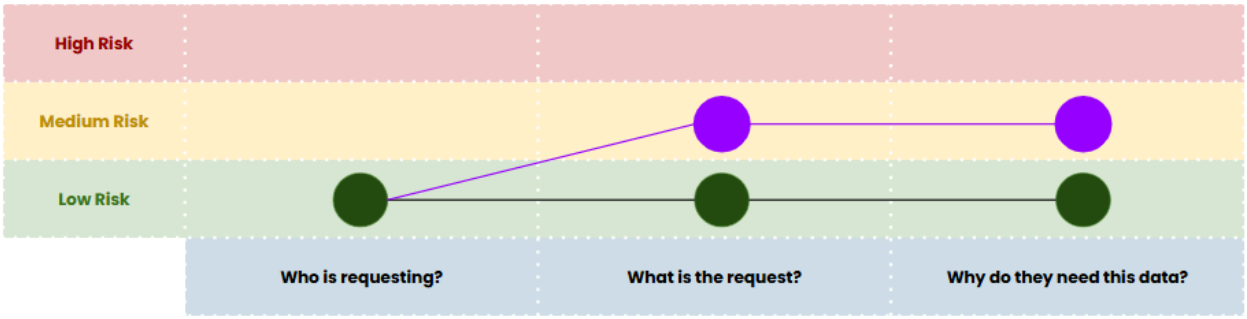
Request. The group decided that, depending on how the situation was viewed, it could be a low- or medium-level risk. This request was ultimately categorized as a low-level risk because the requester is looking for data at a single location, negating aggregation concerns (marked in black in Figure 5). Much of the data request is already public data, leaving the utility to only provide the load shape and peak load data. However, it was noted by the group that load shape can be used to analyze energy use patterns for customers along a feeder. If there is little data to show, this could potentially reveal what type of customer (e.g., an industrial plant) is on the feeder. As a thought exercise, the group envisioned a situation where the request could become a medium-level risk (marked in purple in Figure 6). In this case, the location of the data requested became a major factor (e.g. the same data for a single area, multiple areas across the utility's service territory, or the same request for multiple feeders). This would prompt concerns about data aggregation and violating the 15/15 rule, because as the number of feeders increases, it starts to paint a more complete picture of the system. [15]

Why. The data requested seemed odd to the group because of the age of the data being requested. Utility group members were also concerned that outdated data might mislead the developer's findings. However, the group acknowledged that they cannot dictate or adjudicate why a requester wants specific data (i.e., their project justification). Therefore, this was categorized as a low-level risk. Under the thought exercise, there was concern about the ability of the data to be aggregated and provide the developer with a more complete picture of the system, regardless of the data's age.

Risk Curve. Based on this discussion, the overall request was categorized as a low-level risk and is shown in *Figure 6: Group 2 Medium-Risk Use Case Risk "Curve"* below in green; as part of the thought exercise, this request would be categorized as a medium-level risk when shown in purple.

[15] Minnesota Public Utilities Commission (PUC) Docket No. E,G-999/CI-12-1344.

Figure 6: Group 2 Medium-Risk Use Case Risk "Curve"



Mitigations. The group said that either a secure portal or data encryption would be the preferred method of providing this information. Like with the previous case (group 2's low-level risk case), the group wanted to include either an NDA, business agreement, or attestation to the data's use as part of disseminating this data. This feature was remarked upon as being 'the bare minimum' for all non-public data requests. Despite the low-level risk of the data, the group believed that requiring data handling training should also be 'the bare minimum.'

Group 3

Group 3's second use case was:

- **Who.** Tesla (myriad business groups and contractors).
- **Request.** Distribution system capacity data.
- **Why.** Assess potential sites across the Twin-Cities metro area, Duluth, Rochester, and the highways in-between for public charging.

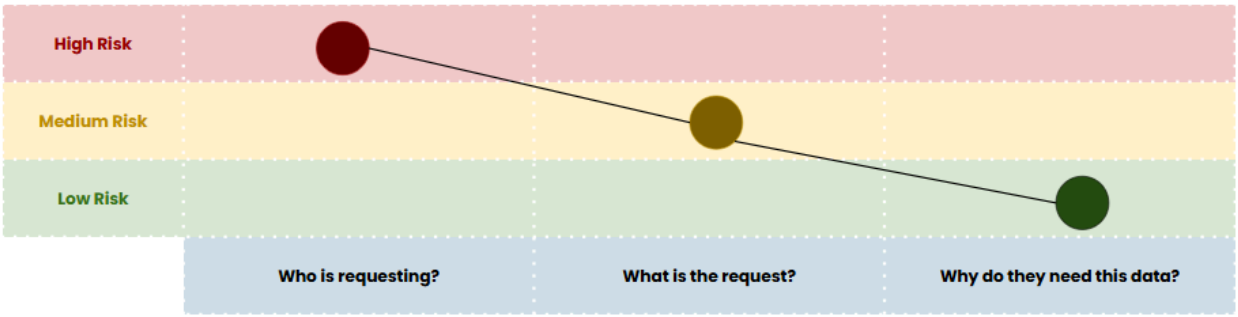
Who. The group classified this requester as a high-level risk for two reasons. First, giving more people access to the data (myriad business groups and contractors) increases risk because it increases 1) the opportunities for the data to be mishandled and 2) targets for nefarious cyber activity. Second, companies that have a global footprint, and therefore store some of their data outside the U.S., are inherently more risky.

Request. The group decided that the requested data poses a medium-level risk. Although the data in question covers a large geographic area, it could be aggregated in such a way that it would decrease visibility into the system.

Why. As long as the project would not exceed what the utilities involved can serve, the group decided that it would be a low-level risk because it is related to natural load growth and corresponds with the request and the requestor.

Risk Curve. Based on this discussion, the overall request was categorized as a medium-level risk and is shown in *Figure 7: Group 3 Medium-Risk Use Case Risk "Curve"* below.

Figure 7: Group 3 Medium-Risk Use Case Risk "Curve"



Mitigations. The group agreed that NDAs alone would not provide meaningful mitigation in this case. To bring the risk to the system down to a medium-level, a business agreement that included language precluding data storage outside the U.S. would be needed, as well as a secure captive portal through which to access the data. If the data was viewed on-site and sanitized, it could be a low-level risk. However, it was unclear to the group if that would render the data useless for the requester.

High-Risk Use Case Development

For this activity, stakeholders stayed with their small groups and developed a use case that would present a high-level risk to the system, which they believed could not be mitigated to a medium- or low-level security risk. Once the use case was created, stakeholders discussed the mitigation options available and what impacts, if any, they would have on the risk of sharing the data.

A summary of the discussion is provided below. See Attachment B for full notes from the activity.

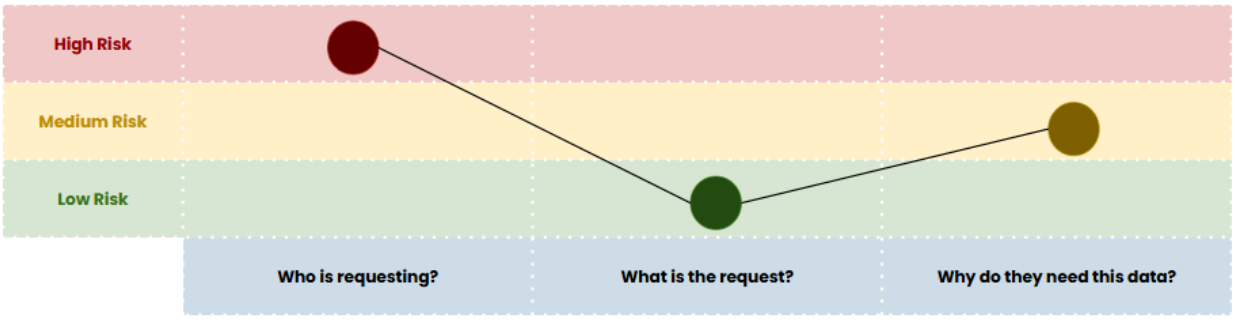
Group 1

Figure 8: Group 1 High-Risk Use Case Risk "Curve" below shows the risk levels of the elements of the high-level risk use case that Group 1 developed.

Group 1's final use case was:

- **Who.** An AI company.
- **Request.** Feeder capacity, daytime minimum load, performance data, reliability data.
- **Why.** Develop a tool for predictive maintenance.

Figure 8: Group 1 High-Risk Use Case Risk "Curve"



Who. The group had concerns that an AI company may be trying to informally approximate energy systems—especially if they submitted similar requests to multiple utilities—even if this is not their stated objective. The main issue identified was a lack of distrust with AI and uncertainty around the overall scope of the project without a clearly defined trigger for enhanced mitigation.

Request. The group concurred that the highest risk from a request like this comes from unknowns, because similar data requested from multiple utilities could be aggregated and used to create a functional model of larger energy systems. Participants noted that neither utilities nor the PUC currently have a mechanism to offer visibility into requests made to multiple utilities, making it difficult to accurately assess risk.

Why. The group agreed that to accurately gauge risk to the system, they would need to understand if the product developed with this information would be sold and the questions the requester intended to put into the Large Language Model (LLM). However, it was acknowledged that this may be proprietary information.

Mitigations. In this case, the group agreed that mitigations such as the requester agreeing to only use the data in private and/or proprietary LLMs, a robust cybersecurity assessment, time-based access, and NDAs or a data sharing agreement would not decrease the risk to the system. The group was unsure if any of the mitigations available could decrease the risk this case poses to the system to a medium- or low-level risk, and thought that this could be an example of a situation that may need PUC intervention and guidance. However, there was also an acknowledgment that this use case does not necessarily present a clear 'trigger' for enhanced mitigation and PUC intervention, given the uncertainty at play.

Group 2

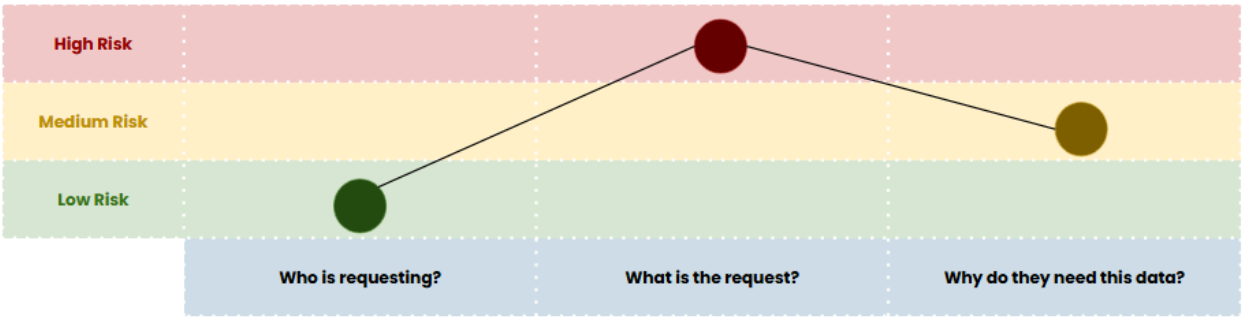
Figure 9: Group 2 High-Risk Use Case Risk "Curve" below shows the risk levels of the elements of the high-level risk use case that Group 2 developed.

Group 2's final use case was:

- **Who.** A DER company with internal engineering capabilities.
- **Request.** Full service territory load flow models.

- **Why.** Perform an internal analysis on the grid for interconnection siting purposes using their own model.

Figure 9: Group 2 High-Risk Use Case Risk "Curve"



Who. With this use case, the group said that it would be important for the company, the individual making the request, and all engineers who would use the data to undergo a background check. This would not reduce risk, but it would confirm that the business is legitimate and that neither it, nor its employees, have anything in their backgrounds that would increase the risk to the grid, should this information be shared with them. However, because the requester is a DER company, they were categorized as a low-level risk.

Request. The group deemed this request a high-level risk because the request involves providing all the data the utility has about its system, including line and load data. The group acknowledged that this data request introduces some proprietary/business concerns, but that the security risk to the grid and to society of providing this data outside of the company was their greatest concern.

Why. It was assumed by the group that the requester intends to use the information to ultimately "get ahead" of the traditional interconnection process. The group acknowledged that, within reason, they cannot tell requesters what they can or cannot do with the data they're given. However, the group categorized this as a medium-level risk for two reasons. First, the developer might not know how to properly analyze or manipulate the data in their model, which can mislead their efforts in DER siting. This prompted concerns that the developer might waste its own time if their projections are wrong and they have to restart their siting process. Second, the security concern of how the data is used (e.g., use of AI, data breaches, etc.) remained.

Mitigations. The group was adamant it would be impossible to mitigate this use case to a lower risk level, even if NDAs, secure portals, and scrubbing and aggregation were utilized. This evolved into a discussion about the vast resources necessary – for both utilities and developers – to properly manage in-person viewing of data, prompting questions about its feasibility and usefulness. From a utility perspective, this would require significant personnel time, which not all utilities have. For example, supervision of this would likely need to be done by an engineer or cyber security manager; some utilities remarked that they are either short-staffed, or that that role in question was too valuable on other tasks to be utilized in this way for long durations, which could create inequity and inconsistency in the data sharing process across the state. Developer representatives pointed out that if they cannot manipulate the data in real time, they may not get all their questions answered in a single

visit and would have to make multiple trips to the utility, which would increase the burden on the developer and utility alike.

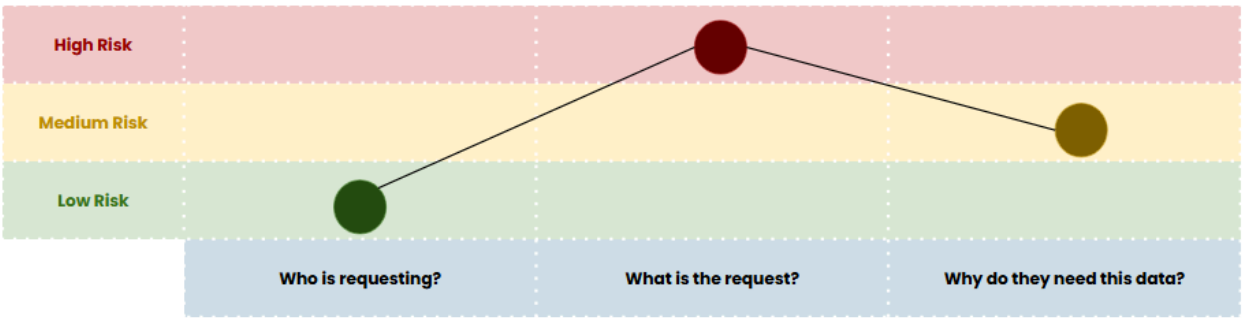
Group 3

Figure 10: Group 2 High-Risk Use Case Risk "Curve" below shows the risk levels of the elements of the high risk use case that Group 3 developed.

Group 3's final use case was:

- **Who.** Minnesota-based grid-scale developer.
- **Request.** Bulk electric system data, including generation plants, large transmission, load flow (both peak and minimum flow), an 8760 model, line capacities, hosting capacity, existing generation, geographic locations of feeder routes, and substations and their ratings.
- **Why.** Looking for potential operational risks with distribution-scale batteries.

Figure 10: Group 2 High-Risk Use Case Risk "Curve"



Who. Although a Minnesota-based grid-scale developer would likely be a low-risk level entity, the group agreed that it was still important for the company, the individual making the request, and anyone who may handle data (e.g. other employees, contractors) should undergo a background check. Additionally, the company should be vetted to ensure they don't have concerning ties (e.g. owned or partially owned by foreign entities) or past data security-related incidents.

Request. The group thought that, taken all together, the data encompassed in this request would be classified as a high-level risk because of the visibility it would give into the workings and vulnerabilities of the system. However, the group did agree that if substations and their ratings were the only data points requested, the request would be classified as a medium-level risk.

Why. Because the project states that the requester would be looking for potential operational risks, the group agreed that this could identify vulnerabilities on the system that could pose a significant level of risk, should the information or the project output fall into the wrong hands. However, assuming the company is legitimate and all personnel properly vetted, they are doing due-diligence before seeking approval for building distribution-scale batteries, which protects the system. For these reasons, the group classified the project as a medium-level risk.

Mitigations. As with the other use cases discussed in Workgroup 3, the group agreed that an NDA alone would not lower the risk level of this case from a high-level risk. However, upon reflection, they decided that a business agreement plus access through a secure portal and data scrubbing/sanitization could potentially bring the risk to the system to a medium-level risk, depending on the level of scrubbing/sanitization. There was additional discussion about whether on-site viewing – which could potentially lower the risk even further – would even be useful to the requester, due to the volume of the request and the scope of the project.

Areas of Agreement and Dispute

This large-group activity focused on identifying areas of agreement and disagreement within the draft Grid Data Sharing Framework. A summary of the discussion is provided below. See Attachment C for full notes from the activity.

Areas of Agreement

Following are items that stakeholders agreed were important components or concepts of a Grid Data Sharing Framework:

- A way for utilities to communicate with each other about requests to know if the same request is being made of each of them, as the same request of multiple utilities from the same requester could be a risk indicator.
- When evaluating risk, the emphasis should be on security risk, grid risk, and public safety, not on corporate or business risk.
- A clarifying meeting between utility and requester early in the evaluation process is important, as it could streamline the process.
- If publicly available data is part of a request, it should be provided up-front, and then the utility should work on evaluating the rest of the request.
- NDAs will likely be part of most requests, regardless of other mitigations; having a template would increase efficiency and speed.
- A data sharing agreement of some kind is required for all requests; the kind of agreement (e.g. NDA) and terms and conditions will be determined by the risk level of the data being requested.
- There needs to be a "pressure valve" or "off ramp" at each stage of the process to improve efficiency and reduce the time needed to complete requests
- Mitigation options are flexible, scalable, and can be layered.

Areas of Dispute

- Whether a scoping meeting or a pre-application is more beneficial to assessing risk and ensuring requesters are asking for the right data for their project.
- The question of the cost of implementing the Grid Data Sharing Framework and who will pay.
- What is the goal of the background check? What constitutes a red flag? What are utilities looking for?
- Should a background check happen before a request is submitted or as part of the request? Who is responsible for conducting the background check?
- There is a cost to in-person data viewing, and it's unclear if this is valuable to a requester.

- Can a request be denied due to technical feasibility?
- There needs to be a timeline for each stage of the process that is reasonable and proportionate to the task.
- The usefulness of data after certain mitigations are applied can be reduced.
- Does declining one part of the request decline the entire request?
- Is CIP-014 an automatic no?
- How data sharing in CIP-014 scenarios or other data sharing rules (scalability) would look.

Attachment A: Use Case Risk Curve Development

Low Risk

Group 1

Use Case Scenario

Who. Community Power, a Minnesota-based non-profit.
Request. Historical data on locational outages in the metro area.
Why. To assess distribution system reliability and equity impacts.

Use Case Risk Curve

	Who	Request	Why
High	• N/A	• N/A	• N/A
Medium	• The request increases in risk if the individual has no online footprint or can't be tied to the organization they are requesting data for. • The organization being registered with the state is a plus but does not bring the risk level down. However, the absence of registration could heighten risk.	• More years of data requested means more risk, because you can start to see trends, like component degradation over time. • It may be possible to see connections to critical infrastructure.	• The threat of outages is higher in economically depressed areas. • Data on equity could reflect poorly on the utility, thereby impacting its bottom line. This is corporate risk however, not security risk.
Low	• The organization is known in the industry and/or to the utility. There is familiarity with their work. • The requesting organization has documented participation in related processes or requests.	• The risk really depends on the granularity of the requested data. • Raw data may be less risky. • This kind of data is often publicly available, although it depends on the utility. • If the data doesn't come to the current year, it is less risky.	• The utility may not have equity data, resulting in higher costs to collect the data the requester is looking for. • The reason the organization is requesting this data is aligned with their mission, which is a green flag.

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• N/A	• N/A	• N/A
Medium	• N/A	• N/A	• N/A
Low	• Understanding the requesting organization's security protocols is important. • The email of the requester should be associated with their organization. It may be necessary to confirm that they work there. • This would require a preliminary application. • It's important for the utility to be able to assess the anticipated intensiveness of the request workload. • It's important to memorialize the request and save it in case it's needed in future proceedings.	• Understanding 3rd party access is crucial. • It is essential to understand if the data will be made public, either in a derivative form or attached as an appendix. • There needs to be more clarity provided on the requested data granularity. • The utility should neither over nor under gather data. It is important to understand exactly what the requester needs.	• The utility needs to have a level of comfortability with the requester's security protocols. • NDAs would be required if the data is more granular. • If the requester has poor security protocols, a hosted portal or additional NDA language may be required. • Confidential (or other classification levels) markings may be required on documents.

Group 2

Use Case Scenario

Who. MN Center for Energy and Environment (CEE), a Minnesota-based non-profit.
Request. Data on areas with limited redundancy.
Why. To study potential areas for siting microgrids. They plan to work with graduate students at the University of Minnesota who are doing a capstone project.

Use Case Risk Curve

	Who	Request	Why
High	• If it was a developer, there is an economic interest.	• N/A	• N/A
Medium	• The risk level of University of Minnesota students depends on how they use the data. • A key question is if the students understand	• Having so much data about vulnerability presents an aggregation concern. • Redundancy is seasonally and	• How the information will be displayed matters. For example, if the capstone project will be published publicly.

	• how to use data and disclose it. • An agreement may be needed with the university to protect data.	structurally fluid. • The location of the data impacts the risk level. • There is a question of whether they need this data specifically, or if their project could be completed using publicly available data. • The data requested could be for areas with a risk for long outages. • There may be a need for additional criteria or specifics from the requester.	
Low	• The organization itself is low risk.	• This would require some data farming.	• N/A

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• N/A	• N/A	• N/A
Medium	• N/A	• N/A	• Too many mitigations limits the project capability.
Low	• N/A	• Whether the requested data is practical (real-time) or procedural (old data) impacts the risk and mitigation required.	• Requiring access through a secure portal mitigates risk. • Data access time limits may be needed. • Data scrubbing may be needed. • Some form of NDA, attestation, and/or business agreement may be needed. As part of it, there should be a required statement on how the data is used. • There is a question of whether the NDA covers the students or just the school or organization.

Group 3

Use Case Scenario

Who. Contractor working on behalf of a Tribal Government in Minnesota.
Request. Data on daytime minimum load, peak load, and load shape for the past three years.
Why. To design a microgrid.

Use Case Risk Curve

	Who	Request	Why
High	• N/A	• N/A	• N/A
Medium	• Whether or not there is a prior relationship with the contractor impacts risk.	• N/A	• N/A
Low	• The Tribal government has a good relationship with the utility, lowering risk. • The individual requesting data has passed a background check.	• Because the data impacts only the Tribal community, the risk is lower. • The data "belongs" to the Tribe - they are entitled to have it. • Daytime minimum load data is publicly available for the substation. • Load shape data may be difficult to provide.	• The requester is the one who benefits from the data. • The data will be used for discrete and finite projects.

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• N/A	• N/A	• N/A
Medium	• N/A	• N/A	• NDAs are needed in most situations, although they may not reduce the overall risk of the request.
Low	• N/A	• N/A	• There should be a data release consent document with the Tribe. • A business agreement is needed. • Data encryption is needed. • A secure portal can be required to access the data.

Medium Risk

Group 1

Use Case Scenario

Who. A Minnesota-based solar developer.
Request. Peak load values for three substations in Minnesota, one of which is regulated under NERC CIP-014.
Why. To assess feasibility, cost, and impact of a solar + storage facility for a municipality.

Use Case Risk Curve

	Who	Request	Why
High	• N/A	• Participants needed to know more information about how NERC CIP-011 applied to low-impact substations. • If a substation is designated under NERC CIP-014, it likely has additional security-related designations as well. • The data from the NERC CIP-014 substation is probably CEII and largely unshareable. • Omitting data on the one NERC CIP-014 substation while providing data on the other two may identify its criticality.	• N/A
Medium	• N/A	• Peak load values at the non-NERC CIP-014 substations are still medium risk because that data can be exploited.	• Who would own and operate the proposed facility matters (i.e.. whether it is municipally owned or not). • Whether the project would be behind the meter or not could also impact risk.
Low	• It would be important to know how long this organization has been around, or perhaps more importantly, if their employees are known in the industry.	• N/A	• N/A

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• Understanding if the company has a track record of NDA violations and/or cyber incidents. If they do, the request becomes much higher risk.	• If the municipality will own the project, they may be obligated to disseminate the data publicly. Understanding if and how they will share the information is essential.	• An NDA does not bring down the risk level. • An NDA may have a negative effect: if communities get wind of it, it may become a bigger deal. • There must be a way to ensure long-term compliance.
Medium	• N/A	• Data granularity, peak capacity, and transformer information matter to the risk level.	• Cybersecurity guidelines and training are a must-have. • A business agreement or other legal agreement that is stronger than an NDA is probably necessary. • It may be possible to scrub data to a minimally acceptable level so that all three substations appear the same, and data can be provided for all of them.
Low	• N/A	• N/A	• N/A

Group 2

Use Case Scenario

Who. A California-based solar developer.
Request. Feeder information at a discrete site – daytime minimum load, peak load, and load shape over the last two years
Why. Exploring interconnection of a solar array >1MW (modeling, cost analysis, and design).

Use Case Risk Curve

	Who	Request	Why
High	• N/A	• N/A	• N/A
Medium	• N/A	• If multiple feeders are asked for, this may raise risk and the utility could stop sharing the data due to the 15/15 rule and aggregation	• This could be used to determine customer type. • Aggregating the same data on a different feeder vs. aggregating

		• concerns. • The location of the request impacts risk: whether it is one area or multiple areas spread out.	different data on the same feeder impacts risk. • This could give a bad actor the ability to aggregate data and plan attacks.
Low	• Participants assumed the company is legally allowed to operate in Minnesota.	• Load shape can be used to infer patterns of use for customers if there are few customers on a feeder. • A single feeder does not present an aggregation concern, so if a single location is requested, this helps limit risk.	• Providing 2-year old data may mislead them.

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• N/A	• N/A	• N/A
Medium	• N/A	• N/A	• Secure portal.
Low	• There is a question around what type of background check is appropriate and what flags may be. There are privacy concerns. • Is this being tracked across the utility?	• N/A	• Attestations, NDAs, and/or a business agreement may be needed. • A secure portal or data encryption could mitigate risk. • Data handling training reduces risk, and may always need to be required.

Group 3

Use Case Scenario

Who. Tesla.
Request. Distribution system capacity data that will be shared amongst myriad business groups and contractors.
Why. Assess potential sites across the Twin-Cities metro area, Duluth, Rochester, and the highways in-between for public charging.

Use Case Risk Curve

	Who	Request	Why
High	• The fact that the data will be shared with many business groups raises the risk. • Data being shared with contractors raises the risk. • The requester may put the data into AI. • The requester has a global footprint and may store data outside the U.S.	• N/A	• N/A
Medium	• N/A	• The data requested covers a large geographic area. • The data is aggregated, which carries less risk in this scenario.	• N/A
Low	• N/A	• N/A	• The request is related to natural load growth. • The reason for the request matches up with the requester.

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• N/A	• N/A	• NDAs are required but will not lower risk.
Medium	• N/A	• N/A	• A business agreement that includes language precluding data storage outside the U.S. is needed. • A secure captive portal will be required to access data.
Low	• N/A	• N/A	• To reduce risk to the lowest possible level, the data will either have to be accessed via an on-site viewing or it will have to be aggregated/scrubbed/sanitized.

Attachment B: High Risk Use Case Development

Group 1

Use Case

	Who	Request	Why
High	• An AI company.	• N/A	• The company may be trying to approximate energy systems by making requests to many utilities, although this would not be their stated goal. • The main issue is that there is distrust and uncertainty, but not a clear trigger for enhanced mitigation.
Medium	• N/A	• N/A	• They may be looking to develop a sellable tool, such as one on predictive maintenance or a database.
Low	• N/A	• The data requested may be low risk, including feeder capacity, daytime minimum load, performance data, or reliability data.	• N/A

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• N/A	• N/A	• The requester should agree to only use the data in private/proprietary LLMs, if any. • A robust cybersecurity assessment is necessary, but AI safeguards are still nascent and may not sufficiently mitigate risk. • Time-based access with proof of data deletion would be required.

			• NDAs should be carefully crafted so that they do not prevent utilities from talking to one another. • There should be a data sharing agreement. • Because there is currently no way for a utility to crosscheck requests with other utilities, a request like this is subject to the data owners' best judgement.
Medium	• N/A	• The utility needs to understand if the data or a product it's used for will be sold. • The utility would want to know the questions being input into LLMs, although the requester may say this is proprietary.	• There could be PUC visibility on all requests, although this could be burdensome. • New mitigations may be needed/present as possibilities as more information comes to light. • This type of request may have to be taken to the PUC.
Low	• N/A	• N/A	• N/A

Group 2

Use Case

	Who	Request	Why
High	• N/A	• They are requesting a full service territory synergy map (load flows). • They are looking for all load and line data.	• N/A
Medium	• N/A	• N/A	• They would like to perform an internal analysis on the grid for siting purposes. • They would like to be efficient in the process (interconnection).
Low	• A distributed energy resource company with internal engineer capabilities.	• They are looking for one area's line model with no loads. • If it's wrong, they have to redo the process.	• Whether the data is historical or not doesn't matter, as the system doesn't always change.

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• Background checks are required but won't reduce risk. • There could be a criteria-based background check with a yes or no and no additional specifics given to the utility.	• N/A	• In-person view-only capabilities may be required. • However, in-person viewing may require high resourcing, as someone would have to be there supervising. • There would have to be limits on what the requester brings in and takes out. • There should also be limits on how the utility helps the requester during an on-site visit, perhaps limited to only a basic Q+A. • NDAs would be needed but may not reduce risk. • There should always be a data handling or viewing agreement and/or an NDA. • A secure portal could be used. • Data should be scrubbed and sanitized. • Feeder data could be aggregated so that it is load only, with no lines, and is a static model. • If costs "don't add up" then we can't give up
Medium	• N/A	• N/A	• N/A
Low	• N/A	• N/A	• N/A

Group 3

Use Case

	Who	Request	Why
High	• N/A	• The request is for bulk electric system data. • The data requested includes generation plants, large	• N/A

		transmission, load flow (both peak and minimum flow), and an 8760 model. The risk of this and the bulk electric system data could likely not be mitigated. • The requested data also includes line capacities, hosting capacity, and existing generation. • The requester is looking for geographic locations of feeder routes, as well as substations and their ratings.	
Medium	• N/A	• Substations and ratings may be medium risk rather than high if alone.	• The requester is completing a project on distribution-scale batteries • They are looking for potential operational risks.
Low	• The requester is a Minnesota-based grid-scale developer.	• N/A	• N/A

Mitigations

	Background Check/Pre-App	Application	Additional Mitigations
High	• N/A	• N/A	• NDAs are required but would not lower the risk level.
Medium	• N/A	• N/A	• A business agreement could reduce some risk. • Having the requester access data through a secure portal may lower risk. • Data scrubbing or sanitization could be required to reduce risk.
Low	• N/A	• N/A	• On-site viewing of data would lower risk. • Aggregating the data would reduce risk.

Attachment C: Areas of Agreement and Dispute

Areas of Agreement	Areas of Dispute
• A way that utilities can communicate with each other about requests to know if the same request is being made of each of them is a good idea.. • There should be an emphasis on security risk, grid risk, and public safety, not on corporate or business risk. • A clarifying meeting between utility and requester early in the evaluation process is important. • Publicly available data should be released early on if it is part of a request, and then the utility should work on the rest. • NDAs will likely be part of most requests, regardless of other mitigations - how much of them can be templated? • A data sharing agreement is required. • There needs to be a "pressure valve" or "off ramp." • Mitigation options are flexible, scalable, and can be layered. • Is there some interaction with the MNDIP process?	• Whether a scoping meeting or a pre-application is more beneficial. • The question of the cost of implementing the Grid Data Sharing Framework and who will pay. • What is the goal of the background check? What constitutes a red flag? What are utilities looking for? • Should a background check happen before a request is submitted? • There is a cost to in-person data viewing, and it's unclear if this is valuable to a requester. • Can a request be denied due to technical feasibility? • We need a process timeline, and are unsure of the numbers for it. • The usefulness of data after certain mitigations are applied can be reduced. • Does declining one part of the request decline the entire request? • Is CIP-014 an automatic no? • How data sharing in CIP-014 scenarios or other data sharing rules (scalability) would look.