September 30, 2021

Will Seuffert
Executive Secretary
Minnesota Public Utilities Commission
121 7th Place East, Suite 350
Saint Paul, Minnesota 55101-2147

RE: **Comments of the Minnesota Department of Commerce, Division of Energy Resources**
Docket No. E999/CI-20-800, Docket No. E002/M-19-685

Dear Mr. Seuffert:

On April 30, 2021, the Minnesota Department of Commerce's (Department) consultant, Synapse Energy Economics, Inc. (Synapse), provided a report entitled *Hosting Capacity Analysis and Distribution Grid Data Security* (Report). The Report offers recommendations on Xcel's hosting capacity analysis and distribution grid data security, in response to both the Minnesota Public Utilities Commission's (Commission) July 31, 2020 Order in Docket No. E002/M-19-685 and to the Commission's Notice issued in the Commission Investigation on Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data in Docket No. E999/CI-20-800.

On June 7, 2021, the Department and Synapse submitted an Addendum to the Report (Addendum). The Addendum made various corrections to the Report.

Attached to this letter is a final version of the Report that includes the corrections detailed in the Addendum. Both the Department and Synapse are available to answer any questions that the Commission may have in this matter.

Sincerely,

/s/ MATTHEW LANDI
Rates Analyst

ML/ja
Attachment

Hosting Capacity Analysis and Distribution Grid Data Security

(MPUC Docket Nos. E999/CI-20-800 and E002/M-19-685)

Prepared for Minnesota Department of Commerce

September 30, 2021

Prepared by:

Shannon Liburd
Elijah Sinclair
Tim Woolf
Cheryl Roberto

Synapse
Energy Economics, Inc.
617.661.3248 | www.synapse-energy.com

Acknowledgements

Synapse would like to thank Professor Emeritus Vicki Bier, of the University of Wisconsin Madison, and Associate Professor Tony Cox, of the University of Colorado Denver, for providing their time, guidance, and feedback on the application of the Risk-Benefit Framework. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of Professors Bier and Cox.

CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

Executive Summary

The Minnesota Department of Commerce, Division of Energy Resources (Department) retained Synapse Energy Economics, Inc. (Synapse) in 2021 to support its exploration of privacy and security issues related to Minnesota utilities' hosting capacity analyses (HCA) and distribution grid data. As with other jurisdictions looking ahead to grid transformation, Minnesota seeks to balance the data access needed to support distributed energy resource (DER) uptake with maintaining a secure grid that protects the privacy of customers.

Utilities develop hosting capacity maps to support market-driven, DER deployment. The maps provide an early indicator to project developers seeking areas within the utility service territory where DER additions may contribute the greatest value. By signaling these locations, utilities reduce the possibility of developers having to pay high system upgrade costs to interconnect DERs. However, the amount of system data displayed in hosting capacity maps varies across states. Utilities must balance the need to share this information for the benefit of the public with the potential for grid and customer security threats from bad actors, who could potentially use this same information to launch an attack.

Synapse provided technical support at two stakeholder workshops hosted by the Department as part of the Minnesota Public Utilities Commission's Docket No. E999/CI-20-800. The topic of the first workshop was costs/risks and benefits of public access to grid data, and the topic of the second workshop was sensitive information sharing and classification. Based in part on these workshops, Synapse developed its assessment of the current state of the industry as well as recommendations to guide Minnesota as it continues its dialogue. Specifically, Synapse focused on:

1. the privacy and security implications of Xcel Energy's HCA report and public-facing map; and
2. the privacy and security implications of public display or access to electric distribution grid data.

Below, we provide our recommendations and then summarize our assessment. Recommendations here are not meant to comment on the appropriateness of the 15/15 standard as it relates to the Commission's ongoing proceedings in the following two dockets: the Commission's Inquiry into Privacy Policies of Rate-Regulated Energy Utilities (Docket No. E, G-999/CI-12-1344) (Docket 12-1344), and a Petition by Citizens Utility Board of Minnesota (CUB) to Adopt Open Data Access Standards (Docket No. E, G-999/M-19-505) (Docket 19-505).

<u>Synapse Recommendations</u>

As a result of Synapse's findings, we recommend the Commission take the following short-term actions:

- Allow Xcel to only redact load data when a feeder violates the 15/15 aggregation standard and require Xcel to publish on its map, and in its tabular spreadsheet, all other HCA data.

- Require Xcel to create a transparent process for third parties to access Critical Electric Infrastructure Information (CEII), on a "need-to-know" basis, with appropriate protections (e.g., non-disclosure agreements, or NDAs) in place.

- Allow Xcel to only redact feeders included in the HCA if they satisfy one or more of the following criteria: (1) connected to a dedicated customer or (2) connected to critical infrastructure or serve a critical customer.

- Require Xcel to provide more detailed rationale (e.g., beyond "security concern") for not publishing feeder and substation capacities.

In the long term, we recommend the Commission take the following actions:

- Require Xcel to provide an unblurred HCA map showing its distribution feeders, behind a verified web login portal that is open to the public (i.e., does not require an NDA).

- Encourage Xcel to consider a tiered-access approach that helps streamline access to non-public grid data and does not make requirements unnecessarily burdensome.

- Encourage Xcel to engage in a transparent, Risk-Benefit/Cost-Benefit Framework stakeholder process to help determine whether specific, sensitive grid data should be published on its HCA map, and how secure access to sensitive grid data (deemed non-public) should be provided.

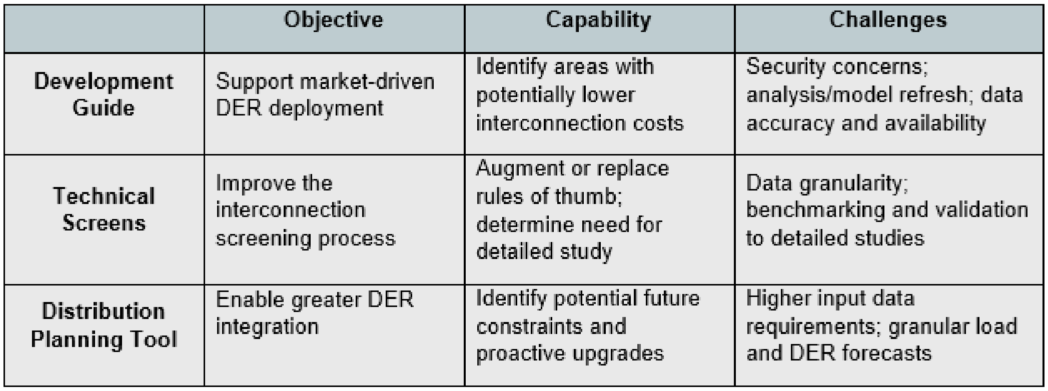
- Require Xcel to estimate the level of effort and cost to incorporate each specific piece of data in the Pre-Application Report that is currently excluded from the HCA map due to technology requirements (e.g., querying and search functionality) rather than security concerns (e.g., distance from site to substation).

These recommendations should help to balance the grid and customer security concerns and data access requirements of all parties involved.

Hosting Capacity Use Cases

"Hosting capacity" refers to the amount of DERs that can be accommodated on the distribution system on a given circuit without adversely impacting power quality or reliability and without requiring infrastructure upgrades. There are three primary applications, or use cases, for an HCA: (1) to support market-driven DER deployment by enabling developers to identify technically suitable and potentially lower-cost interconnection locations; (2) to assist with streamlining DER interconnections by improving or automating parts of the technical screening process; and (3) to enable more robust, long-term distribution system planning, providing visibility into how much DER the grid can host in future years, by identifying potential system constraints and proactive upgrades. Table ES-1 provides more details on these use cases. This report will focus on the first two use cases, using HCA maps as a (1) development guide and (2) to augment or replace interconnection technical screens (e.g., to replace the Pre-Application Report).

Table ES-1. Hosting Capacity Use Cases



	Objective	Capability	Challenges
Development Guide	Support market-driven DER deployment	Identify areas with potentially lower interconnection costs	Security concerns; analysis/model refresh; data accuracy and availability
Technical Screens	Improve the interconnection screening process	Augment or replace rules of thumb; determine need for detailed study	Data granularity; benchmarking and validation to detailed studies
Distribution Planning Tool	Enable greater DER integration	Identify potential future constraints and proactive upgrades	Higher input data requirements; granular load and DER forecasts

Source: *U.S. DOE, Office of Electricity, Integrated Distribution Planning - Utility Practices in Hosting Capacity Analysis and Locational Value Assessment, 2018, p.3.*

Protection of Sensitive Energy Information and Customer Confidentiality

Critical data is data which must be removed from the public domain to maintain its security. This may include energy information pertaining to critical customer groups or critical infrastructure. U.S. utilities are taking measures to protect customer privacy using aggregation standards and Critical Energy/Electric Infrastructure Information (CEII) criteria.

As defined by the Commission, the purpose of protecting Customer Energy Use Data (CEUD) is to prevent third parties from accessing the energy-use patterns of a specific customer and data that reveals commercially sensitive information. Regarding critical infrastructure, several federal agencies have provided guidance and regulations. At the national level, the Cybersecurity & Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) has identified 16 critical infrastructure sectors that it considers vital to U.S. security, national economic security, and national public health or safety. The energy sector is uniquely critical because it provides an "enabling function" across all critical infrastructure sectors.

To align with protecting critical infrastructure sectors, as identified by DHS, Xcel identified customers and their associated feeder(s) that, in its judgement, would warrant protection based on the criticality of the loads they serve. These critical customers fell into the following categories:

- Critical Energy Infrastructure (similar to DHS Energy sector);
- Critical Hospitals - Level 1 or 2 Trauma Centers (similar to DHS Healthcare and Public Health sector);
- Critical Data Centers (similar to DHS Communications and Information Technology sectors); and
- Critical Public Gathering Center (similar to DHS Commercial Facilities sector).

Grid Security

There are three main categories of electric system vulnerabilities which can result in the disruption of the grid's power supply. These are physical security, cybersecurity, and personnel vulnerabilities. This report only focuses on physical and cybersecurity vulnerabilities.

Physical attacks on distribution transformers, circuits (e.g., feeders), protective devices, and other distribution system assets could impact the electricity supply to critical local customers like hospitals. For governing distribution systems, over which states have authority, there are no mandatory federal standards such as the North American Electric Reliability Corporation CIP standards that apply to the bulk power system. Thus, there are varying standards of protection for distribution systems.

A recent U.S. Government Accountability Office (GAO) report for the Department of Energy (DOE) on distribution grid cybersecurity notes that U.S distribution systems are increasingly at risk from cyberattacks. As a result, threat actors can use multiple techniques to access those systems and potentially disrupt operations. However, the scale of the potential impacts of such cyberattacks on the grid's distribution systems is unclear. The GAO report states that none of the cybersecurity incidents reported in the United States have disrupted the reliability or availability of the grid's distribution systems.

Grid and Customer Security and Customer Confidentiality Discussion

The Commission's July 31, 2020 Order required Xcel to further discuss grid and customer security issues related to the public display or access to grid data, including distribution grid mapping, aggregated load data, and critical infrastructure in a proceeding that includes additional parties, experts, and utilities. It also required Xcel to separately evaluate and justify each privacy and security concern and to provide a full description and specific basis for withholding any information in its 2020 HCA.

Xcel provided comments in its 2020 HCA on the main grid and customer security and confidentiality issues related to the public display or access to grid data. This included distribution grid mapping, aggregated and peak load data, and critical infrastructure. To address these concerns, Xcel continues to: (1) remove certain feeders from the heat map to protect critical infrastructure; (2) protect customer privacy by applying the 15/15 standard; (3) treat the peak substation transformer load and peak feeder load data as non-public in the Tabular Results; and (4) blur exact feeder lines in the heat map.

We discuss each of these security and confidentiality controls in turn.

Xcel uses 15/15 Standard to Redact Feeder from HCA Map	
Xcel's Justification	**Synapse Recommendation**
Publicly disclosing feeders which violate the 15/15 standard could compromise customer confidentiality.	Only load information should be redacted from the feeder when the 15/15 standard is violated.

The Commission should allow Xcel to only redact load data and require it to publish all other HCA data on its map when the application of the 15/15 standard calls for the redaction of CEUD to protect customer privacy. This recommendation is based on stakeholder requests to have HCA results and non-CEUD information made available on the HCA map under such circumstances, how other electric utilities appropriately balance providing HCA results and feeder locations while not revealing customer privacy (e.g., redact only feeder load profile) on their maps when similarly applying the 15/15 standard, and Xcel's prerogative to redact feeders from its map that violate CEII and critical customer group screens.

Peak Substation Transformer & Peak Feeder Load Confidential	
Xcel's Justification	**Synapse Recommendation**
Load is security information. Publishing this information could aid bad actors in planning a serious attack. It could also compromise the privacy or confidentiality interests of large or critical infrastructure customers.	Apply a Risk-Benefit Framework (Section 4.2) to weigh risk vs. public benefit of publishing information.

There are competing claims about the value of this information to DER developers and the risks associated with publicly providing it. A Risk-Benefit Framework, as proposed in Section 4.2, should be applied to help determine whether substation and feeder peak loads should be publicly provided as requested by the Commission. This framework will help to weigh the need for this information by a diverse group of DER developers (e.g., storage, electric vehicle, and solar) against the customer and grid security risks of publishing it.

Xcel Redacts Feeders to Protect Critical Infrastructure Sectors	
Xcel's Justification	**Synapse Recommendation**
Feeders are not shown on HCA Map to align with protecting critical infrastructure sectors.	• Create a transparent process on how third parties can access CEII.

Given the importance of protecting critical infrastructure and customer groups, Xcel's approach of excluding a feeder from its HCA map when it is connected to critical infrastructure, as defined according to its five critical infrastructure categories, seems reasonable. However, to increase the transparency of the process with the public, Xcel should specify in greater detail the types of customers that are considered critical, grid-dependent customers, which fall outside of its five critical infrastructure categories. Xcel should also create a transparent process for how third parties can access CEII, on a “need-to-know” basis, with appropriate protections (e.g., an NDA) in place.

Public Display of Distribution Lines on HCA Map	
Xcel’s Justification	**Synapse Recommendation**
An unblurred HCA map would make the grid unnecessarily vulnerable to attack and would jeopardize customer security and confidentiality.	Xcel should unblur its HCA map because: • Hosting capacity maps generally show feeder lines. • Knowing the distribution line locations provides significant value to DER developers. • Location of information on distribution facilities is likely already in the public domain. • Various tools are available to help map distribution lines. • A bad actor can conduct reconnaissance by visual observation of distribution line connections. • Focusing on strengthening the grid’s physical and cybersecurity defenses, and increasing grid resiliency, is more effective at deterring attackers than concealing information. • Distribution systems are generally lower value targets relative to transmission systems.

In general, publicly available hosting capacity maps of U.S. electric utilities leading in this space show the distribution system feeder lines at increasingly granular levels of detail (e.g., sub-feeder level). Xcel provides hosting capacity results at the sub-feeder level, but this granularity is lost because the actual feeders are blurred on Xcel’s hosting capacity map. Hosting capacity maps should be sufficiently detailed to be useful to stakeholders. There is significant benefit to developers of knowing the locations of distribution lines to optimally site DERs. Xcel frequently gets requests from its developer community to show its feeder lines on the HCA map, and in a recent developer survey, all the participants said that Xcel’s current HCA map requires more detailed information to be useful.

Detailed maps of the U.S. power system were once readily available in the public domain and on the Internet and many can still be found. Bad actors could also use publicly available resources such as Google Earth to map distribution lines, or they could simply locate a critical facility and visually trace the power lines emanating in either direction to plan an attack. Rather than focusing on concealing grid data on the locations of feeders and substations, the utility should focus on bolstering its physical and cybersecurity defenses in case of an attack, and on enhancing the reliability and resiliency of the grid. Doing so could deter would-be adversaries from attacking by reducing or removing the perceived benefits that an adversary associates with an attack. Additionally, investments in measures aimed at limiting or denying adversary success serve a broader purpose of improving mission resilience to power disruptions resulting from natural disasters, operator error, or equipment failures.

HCA Integration with Pre-Application Report

Xcel should clearly justify the security concerns it has regarding revealing substation and feeder thermal capacities given the tangible benefits to DER developers of having that information. A Risk-Benefit Framework could assist in balancing the risks of publishing substation and feeder capacities and peak loads against the public benefits.

Frameworks for Assessing Inclusion of Grid Data in HCA Map

Risk-Benefit Framework

The Risk-Benefit Framework is used to semi-quantitatively determine the risk to a critical asset (e.g., substation) due to revealing sensitive information about it (e.g., on an HCA map) over a one-year period. It helps estimate the probability of an attack and the resulting consequence if the attack were successful. Based on the expected value of the risk, it can be categorized as a low, moderate, or significant risk. The risk level for each critical asset evaluated would then be compared to the value of revealing information about the same asset to the public.

Cost-Benefit Framework

The Cost-Benefit Framework could be used to compare the costs and benefits to the public/ratepayer of publicly revealing specific grid information. The benefits would include the incremental customer and societal benefits of making the information public and the costs would include the costs to the utility of providing this information and of defending against a better-informed attack. A net public benefit would inform whether the specific grid information would be made public.

Deciding Which Framework to Apply

In general, the Risk-Benefit Framework should be applied first to determine the overall level of risk to an asset from revealing information about it. The Cost-Benefit Framework can supplement it, adding more details about the actual cost of providing the information when there is an incremental labor cost to doing so (e.g., HCA map enhancements such as formulas and search functionality). If there is no risk involved with providing specific information, then the Cost-Benefit Framework should be used instead since it primarily focuses on weighing the economic costs versus the benefits.

Framework Limitations

Every framework or model has its limitations, and it is important to acknowledge them. However, it is unacceptable to state that there are myriad undefined threats or attack vectors that exist, and consequently, no sensitive grid information should be revealed on an HCA map. Using a risk-based framework helps stakeholders gain a shared understanding of the information under consideration and to discuss risk more tangibly.

Models for Information Sharing

There are different approaches for sharing grid information with third parties. Utilities in different states share grid data in a variety of ways, including through their HCA maps and interconnection processes. A tiered-access approach is one way to selectively share sensitive data on a “need-to-know” basis. A web portal with different levels of access is one way to implement this approach. Investor-owned utilities in Minnesota, New York, New Hampshire, and California either use, or plan to use, a tiered-access framework to effectively share data with third parties. Xcel should consider using a tiered-access approach to share additional HCA information with the public.

1. Introduction

In this era of electric utility transition, utilities will be responsible for optimizing all cost-effective energy resources, regardless of size or ownership. Hosting capacity maps can be used by utilities to support market-driven distributed energy resource (DER) deployment. These maps provide early indicators to project developers looking to identify areas within the utility service territory where DER additions may contribute the greatest value and/or cause the least negative impact to the operation of the grid. By signaling these locations, utilities facilitate the optimization of DER deployment. Hosting capacity maps can also help the utility streamline its DER interconnection process, thereby reducing an expense and barrier to DER deployment. Utility approaches for implementing hosting capacity maps vary from static maps of constrained areas with limited system data to dynamic maps that provide additional system data at each location. The amount of system data displayed in hosting capacity maps varies. It depends upon the balance each state's regulatory framework has established between the utility's grid security concerns around making data public and the public interest benefits of advancing a flexible, reliable, and resilient grid through cost-effective DER deployment. Examples of potentially sensitive data include the location of sensitive loads and critical energy infrastructure.

1.1. Background

On July 31, 2020, the Minnesota Public Utilities Commission (Commission) issued its Order in Docket No. E002/M-19-685. Among other things, the order requested that the Commissioner of Commerce seek authority from the Commissioner of Management and Budget to incur costs for specialty services to (a) provide a recommendation on privacy and security in the next hosting capacity report proceeding and (b) participate in related analysis and stakeholder engagement. The Commission requested further development of issues surrounding customer privacy and system security in the context of Northern States Power Company's (d/b/a Xcel Energy) hosting capacity map and whether its 2020 Hosting Capacity Analysis (HCA) report complied with the Commission's directives in its orders in Docket Nos. E002/M-18-684 and E002/M-19-685. On October 30, 2020, the Commission opened a Commission Investigation proceeding related to grid and customer security issues in Docket No. E999/CI-20-800.

In February 2021, the Minnesota Department of Commerce, Division of Energy Resources (Department) retained Synapse Energy Economics, Inc. (Synapse) to provide technical expertise for regulatory proceedings before the Commission on issues related to:

1. the privacy and security implications of Xcel Energy's HCA report and public-facing map; and
2. the privacy and security implications of public display or access to electric distribution grid data.

1.2. Report Overview

This report provides insight regarding distribution grid and customer security as it pertains to sharing sensitive information on hosting capacity maps. It focuses on the current state of the industry and provides recommendations to help guide the ongoing discussion on HCA and distribution grid data security in Minnesota.

Hosting capacity maps are useful information-sharing tools for different stakeholders that need access to distribution grid data. However, balancing the public benefits associated with sharing specific types of sensitive grid data with the corresponding risks can be challenging. This report reviews grid data security and related customer energy use privacy practices and standards in the United States. We draw from these best practices to provide a recommendation based on our findings in the context of the state of Minnesota. Moreover, the report investigates the application of risk- and cost-based frameworks for determining a path forward for securely sharing sensitive hosting capacity map data for the public good in Minnesota.

A summary of each chapter of the report is as follows:

- Chapter 1 provides background on the Commission-ordered proceedings related to Docket No. E002/M-19-685. It also gives an overview of the report and discusses the two workshops that helped inform the study.

- Chapter 2 highlights the various applications of hosting capacity maps and discusses how several states are using them to accelerate DER deployment and to help modernize the grid.

- Chapter 3 provides an in-depth review of the types of sensitive information, motivations for and methods to protect this information. It assesses the current industry standards for sharing distribution system information. The chapter specifically discusses customer energy use data and critical energy infrastructure information in the context of hosting capacity, reviews grid security vulnerabilities and threats, and offers examples of how to balance the risks with the public benefits of publishing distribution system data. Finally, it applies these findings to Minnesota to inform the final recommendations.

- Chapter 4 discusses two frameworks that can be used to compare the incremental benefit and risk/cost of releasing specific grid data. It first describes and evaluates the Risk-Benefit Framework, which can be used to measure and compare the risks and benefits of incremental data release. It then offers the Cost-Benefit Framework, which is a systematic approach for comparing the costs and benefits of alternative options. Electric utilities use both methods to optimize internal resource investment decisions and to justify these decisions to regulators and stakeholders.

- Chapter 5 reviews models for information sharing. After providing an overview of the types of data-sharing models, this chapter benchmarks industry standards and then offers a recommendation for the Commission to consider.

- Chapter 6 provides final recommendations to the Commission.

- Chapter 7 concludes the report and highlights points for future discussion.

In summary, this report examines grid security and customer confidentiality issues as they pertain to hosting capacity maps, develops frameworks and models to implement risk-based sharing of sensitive data, and provides recommendations for application in Minnesota. It surveys industry practices, explains the risks of sharing distribution grid data, and lays out frameworks and models that can be used to measure and expand the usefulness and variety of data shared on hosting capacity maps.

1.3. Workshops

Although not required by the Commission's Order, the Department hosted stakeholder workshops on March 17 and March 31 to discuss and better understand issues related to electric distribution system data privacy and security. The topic of the first workshop was costs/risks and benefits of public access to grid data. The topic of the second workshop was sensitive information sharing and classification.

The objectives of the workshops were two-fold:

1. to convene a stakeholder forum to discuss grid security and customer confidentiality issues related to the public display of grid data; and
2. to create a framework to balance (a) grid security and customer privacy concerns associated with public access to grid data with (b) the public interest.

In Workshop 1, national security expert Dr. Paul Stockton[1] presented a statement on behalf of Xcel Energy on grid security risk scenarios and specific attack vectors that adversaries can employ; Xcel Energy presented on its current grid security and resiliency efforts; the Interstate Renewable Energy Council (IREC) presented on the benefits of public access to grid data; and Synapse presented on risk-based classification of data and risk-benefit and cost-benefit frameworks. In preparation for the first workshop, the Department sent a survey to members of the public to better understand the usefulness of Xcel Energy's hosting capacity map and the public benefits of certain grid data for, among other applications, identifying potential project sites for DER interconnection. The survey results informed the workshop discussion. Fifty-two people participated in the first workshop.

In Workshop 2, Synapse expanded on the risk/cost-benefit frameworks discussed in Workshop 1, presented on classification criteria for Critical Electric Infrastructure Information (CEII), discussed hosting capacity map security and confidentiality considerations by comparing utility HCA map practices nationally, and reviewed different models for data sharing. Fifty-four people participated in the second workshop.

[1] Dr. Paul Stockton provides strategic advice to industry and government clients on critical infrastructure resilience and national security. He chairs the Grid Resilience for National Security Subcommittee of the Department of Energy's Electricity Advisor Committee.

There was robust participation from the Minnesota utilities in both workshops but participation from DER developers was limited. While the number of developers attending was sufficient to conduct the workshops, it can be a goal to increase developer participation in future discussions.

The Department posted a written summary of both workshops, including presentation materials, to the Commission's electronic docket filing system. Developers or others that were unable to attend can review these materials.

2. Hosting Capacity

2.1. Hosting Capacity Use Cases

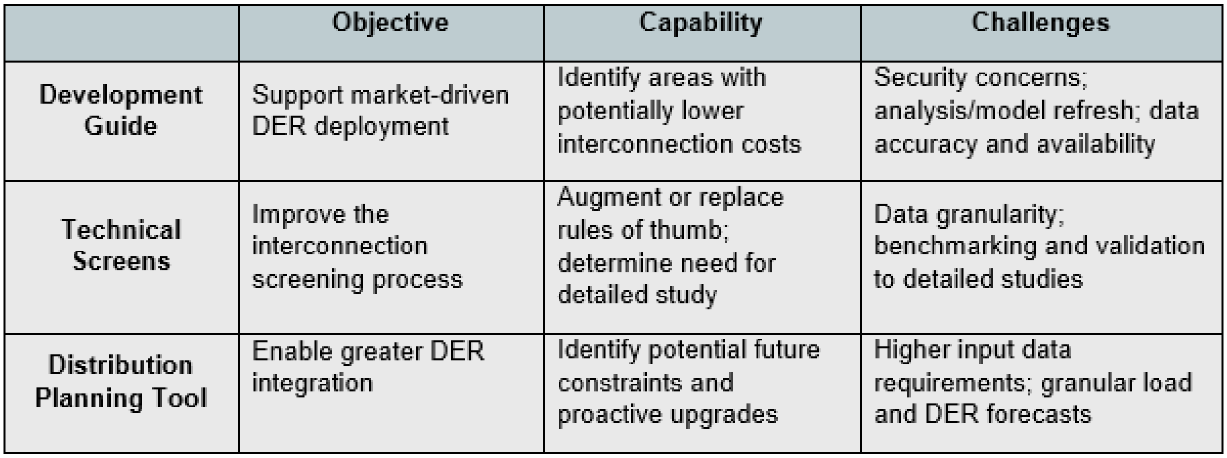
Hosting capacity refers to the amount of DERs that can be accommodated on the distribution system on a given circuit without adversely impacting power quality or reliability and without requiring infrastructure upgrades.[2] Hosting Capacity Analysis is a useful tool for assessing the locational value of DERs at increasing levels of penetration on the grid. Hosting capacity maps, a visual representation of an HCA, can be used to transparently share information between regulators, developers, electric customers, and utilities. This results in more efficient and economical DER deployment on the grid.[3]

There are three primary applications, or use cases, for an HCA: (1) to support market-driven DER deployment by enabling developers to identify technically suitable and potentially lower-cost interconnection locations; (2) to assist with streamlining DER interconnections by improving or automating parts of the technical screening process; and (3) to enable more robust, long-term distribution system planning, which provides visibility into how much DER the grid can host in future years by identifying potential system constraints and proactive upgrades. Table 1 summarizes the main HCA use cases.

[2] Electric Power Research Institute (EPRI). 2020. *Defining a Roadmap for Integrating Hosting Capacity in the Interconnection Process.* p. 3. https://www.epri.com/research/programs/108271/results/3002020010.

[3] Stanfield, Sky and Stephanie Safdi. 2017. *Optimizing the Grid: A Regulator's Guide to Hosting Capacity Analyses for Distributed Energy Resources.* Interstate Renewable Energy Council (IREC). p. 1. https://irecusa.org/wp-content/uploads/2017/12/Optimizing-the-Grid_121517_FINAL.pdf.

Table 1: Hosting Capacity Use Cases



	Objective	Capability	Challenges
Development Guide	Support market-driven DER deployment	Identify areas with potentially lower interconnection costs	Security concerns; analysis/model refresh; data accuracy and availability
Technical Screens	Improve the interconnection screening process	Augment or replace rules of thumb; determine need for detailed study	Data granularity; benchmarking and validation to detailed studies
Distribution Planning Tool	Enable greater DER integration	Identify potential future constraints and proactive upgrades	Higher input data requirements; granular load and DER forecasts

Source: U.S. DOE, Office of Electricity, Integrated Distribution Planning - Utility Practices in Hosting Capacity Analysis and Locational Value Assessment, July 1, 2018, p.3.

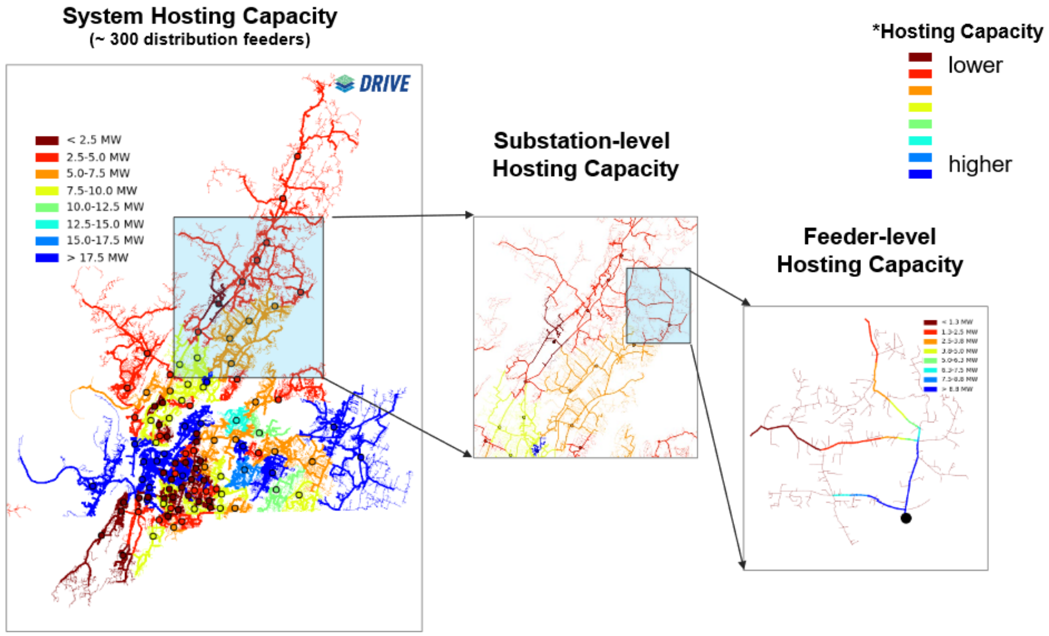
2.1.1. Hosting Capacity as a Development Guide

Some utilities are using hosting capacity maps to help energy developers identify optimal locations for interconnecting DERs on the distribution system to minimize project costs. Developers can face considerable uncertainty around the costs of interconnecting DERs.[4] Connecting DERs to capacity-constrained circuits may require system upgrades, resulting in higher interconnection costs and potentially an uneconomical project.

Hosting capacity maps give an indication of how much generation can be added to a circuit or feeder before it reaches its capacity, or other limitations that reduce its ability to reliably serve electric customers. With these insights, developers can identify locations where the circuits have capacity to accommodate additional DERs, without triggering a system upgrade. Figure 1 provides a color-coded illustration of a system's hosting capacity at both the substation and feeder levels. Hosting capacity information can also be provided at the sub-feeder or line segment level. Feeders with lower hosting capacity (e.g., red lines) may require system upgrades to overcome circuit constraints. However, hosting capacity maps only provide a snapshot of the distribution system at a given point in time and are not meant to replace a detailed system interconnection study for a particular site.

[4] U.S. DOE. 2018. *Office of Electricity, Integrated Distribution Planning - Utility Practices in Hosting Capacity Analysis and Locational Value Assessment*. p. 11. https://static1.squarespace.com/static/5b736be575f9eeb993c4d5f1/t/5b8f4055032be49d0ccfd2bf/1536114780361/ICF+DOE+Utility+IDP+FINAL+July+2018+%28003%29.pdf.

Figure 1: Hosting Capacity Illustration



Source: Jeff Smith, Methods, Applications, Opportunities and Challenges, EPRI. MPSC Distribution Planning Stakeholder Meeting, June 27, 2019, p.4.

Hosting capacity maps generally inform the early stages of DER project development, enabling developers to more efficiently allocate their time and resources to focus on the most promising sites. Providing developers with this high-level distribution system view could also help accelerate the interconnection process by channeling applications to the grid locations where they are most likely to be quickly approved,[5] reducing interconnection queue backlogs, and making more efficient use of utility resources.

2.1.2. Hosting Capacity as an Interconnection Technical Screen

The utility interconnection process is intended to maintain grid safety and reliability, and it determines whether and how a DER can connect to the distribution system.[6] However, ambitious new state and federal policies, growing customer demand, and steadily declining prices are accelerating DER growth and increasing the volume of interconnection applications. Utilities are finding it difficult to keep pace. Thus, it is becoming increasingly important for utilities to carry out interconnection processes efficiently and effectively.[7] Figure 2 shows that an interconnection application must pass through several stages of evaluation before receiving approval.[8] The process often includes a set of technical screens that

[5] Stanfield, Sky and Stephanie Safdi. 2017. *Optimizing the Grid.* p. 8.

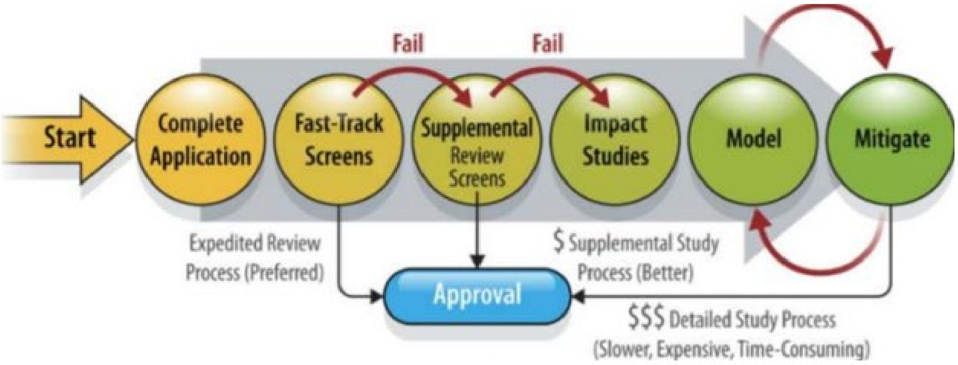
[6] U.S. DOE. 2018. *Utility Practices in Hosting Capacity Analysis and Locational Value Assessment*. p. 16.

[7] Ibid.

[8] Ibid.

evaluate whether the application can receive fast-track status allowing an application to bypass some or all the additional supplementary technical screens or the detailed study process.[9]

Figure 2: Interconnection Screening Process


Fail
Fail
Start
Complete Application
Fast-Track Screens
Supplemental Review Screens
Impact Studies
Model
Mitigate
Expedited Review Process (Preferred)
Approval
$ Supplemental Study Process (Better)
$$$ Detailed Study Process (Slower, Expensive, Time-Consuming)

Source: NREL, Emerging Issues and Challenges in Integrating Solar with the Distribution System, May 2016.

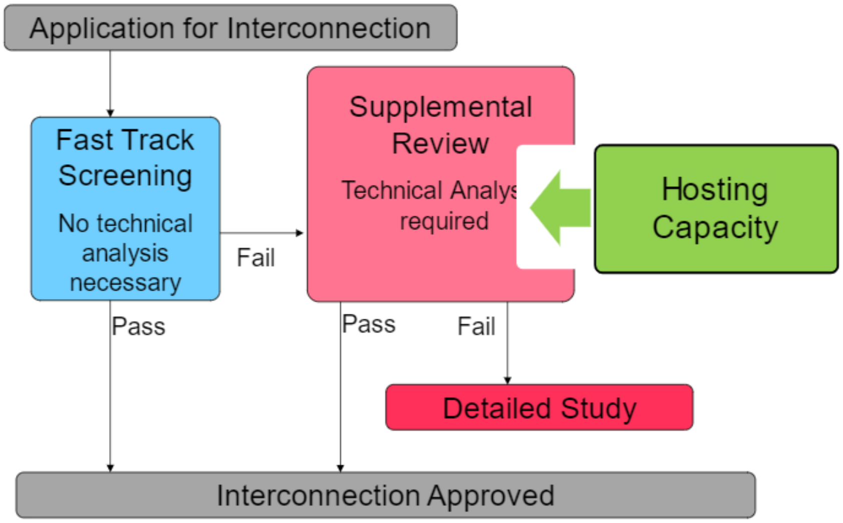
As shown in Figure 3, hosting capacity is being used as a means to either inform or supplant some fast track and supplemental review screens, though it cannot replace a detailed system impact study.[10] With frequent hosting capacity analysis updates (e.g., monthly), utilities can move toward more automated and streamlined interconnection processes, enabling them to balance higher volumes of interconnection applications more efficiently with the need to complete detailed interconnection studies. However, for many DER applications, the hosting capacity analysis and maps are a sufficient proxy for the technical screens employed by the utility.[11]

[9] Ibid.

[10] EPRI. 2020. *Defining a Roadmap for Integrating Hosting Capacity in the Interconnection Process.* pp. 5, 8.

[11] U.S. DOE. 2018. *Utility Practices in Hosting Capacity Analysis and Locational Value Assessment*. p. 18.

Figure 3: Hosting Capacity Analysis Can Assist in Interconnection Screening



Source: Jeff Smith, Methods, Applications, Opportunities and Challenges, EPRI. MPSC Distribution Planning Stakeholder Meeting, June 27, 2019, p. 24.

2.1.3. Hosting Capacity Analysis for Long-Term Planning

HCA can be used as a tool for long-term, integrated distribution system planning. In the other two use cases, hosting capacity is evaluated in the context of current system conditions. In this use case, HCA is used to plan for future scenarios with higher levels of DER penetration and load growth. This is especially important considering progressive DER adoption policies that accelerate the use of electric vehicles and energy storage. This type of forecasted hosting capacity could enable utilities to proactively assess the need for system upgrades in anticipation of DER growth, consider the potential to utilize DERs to defer or avoid planned capital upgrades (e.g., non-wire alternatives), and optimize the deployment of DERs on the grid in support of system reliability and resiliency.

2.2. Current State of the Industry

2.2.1. Overview

Hosting capacity maps are currently available from a relatively small number of utilities. However, the maps are becoming an increasingly important tool for project developers looking to interconnect DERs to the distribution system and to industry advocates and regulators who want to increase the amount of DERs deployed on the grid for the public good. Currently, at least ten states require utilities to produce hosting capacity maps: California, Colorado, Illinois, Massachusetts, Nevada, Minnesota, New York, Maryland, New Jersey, and Connecticut. [12] Several other states are having regulatory discussions about

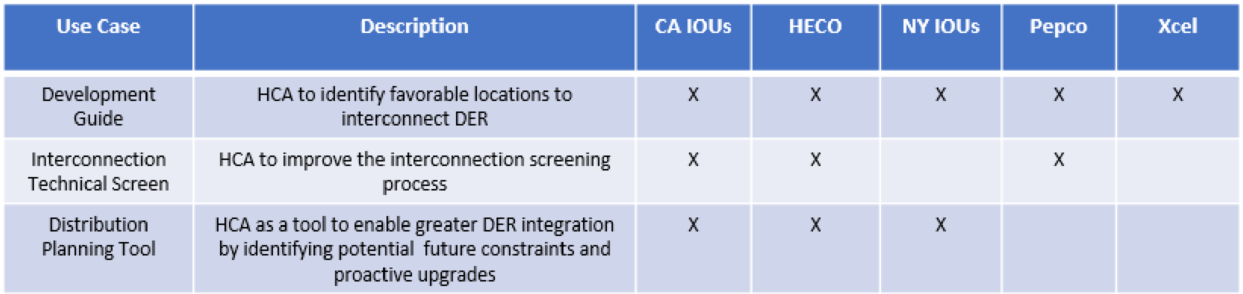
[12] Driscoll, William. June 16, 2020. "Solar hosting capacity maps must be accurate to be useful." pv magazine. Available at: https://pv-magazine-usa.com/2020/06/16/solar-hosting-capacity-maps-must-be-accurate-to-be-useful/#:~:text=Seven%20states%20now%20require%20utilities,represents%20IREC%20in%20state%20proceedings; and

requiring hosting capacity analyses, or improving existing ones, including Kentucky, Michigan, New Mexico, New Hampshire, Ohio, Oregon, and Vermont .[13] The following sections provide an overview of how leading utilities are applying HCA and compare the types of information being made publicly available in hosting capacity maps.

2.2.2. Utility Applications of Hosting Capacity Analyses

Across the United States, electric utilities are using hosting capacity maps for different applications. Table 2 provides a snapshot of how Xcel Energy, Potomac Electric Power Company (Pepco), Hawaiian Electric Company (HECO), and the California, and New York investor-owned utilities (IOU) are currently applying HCA on distribution systems. The following sections will discuss this in greater detail.

Table 2: Utility Hosting Capacity Analysis Benchmark



Use Case	Description	CA IOUs	HECO	NY IOUs	Pepco	Xcel
Development Guide	HCA to identify favorable locations to interconnect DER	X	X	X	X	X
Interconnection Technical Screen	HCA to improve the interconnection screening process	X	X		X	
Distribution Planning Tool	HCA as a tool to enable greater DER integration by identifying potential future constraints and proactive upgrades	X	X	X		

Source: Lisa Schwartz, Lawrence Berkeley National Lab, Distribution Planning Regulatory Practices in Other States, Oregon Public Utility Commission Webinar, May 21, 2020, p. 40 (Synapse modified).

2.2.3. HCA Development Guide Case Study

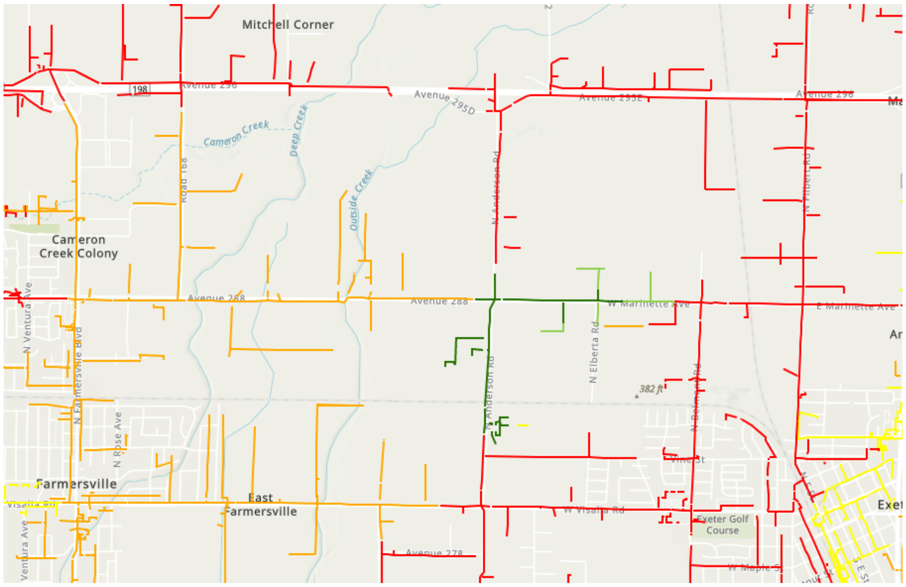
Some utilities are using hosting capacity maps to support DER developers. The California IOUs published their first hosting capacity maps called Integration Capacity Analysis (ICA) maps, in 2015 to provide an indication of hosting capacity across their systems.[14] Figure 4 provides an example of Southern California Edison's (SCE) hosting capacity map. Developers are provided with online access to the maps, which indicate the amount of DERs that can be added at each location without substantial system upgrades. The maps display information—such as load profiles, hosting capacity, total distributed generation on a feeder (existing and queued), and related grid information—at the substation, feeder, and sub-feeder (line section) levels. The maps also indicate where violations due to thermal, voltage, protection, or operational (e.g., reverse power flow) limitations could arise.

Driscoll, William. September 20, 2021. "IREC guide aims to help states deploy solar hosting capacity maps." pv magazine. Available at: https://pv-magazine-usa.com/2021/09/20/irec-guide-aims-to-help-states-deploy-solar-hosting-capacity-maps/.

[13] Ibid.

[14] U.S. DOE. 2018. *Utility Practices in Hosting Capacity Analysis and Locational Value Assessment*. p. 11.

Figure 5: SCE Integration Capacity Analysis Map



Source: https://ltmdrpep.sce.com/drpep/

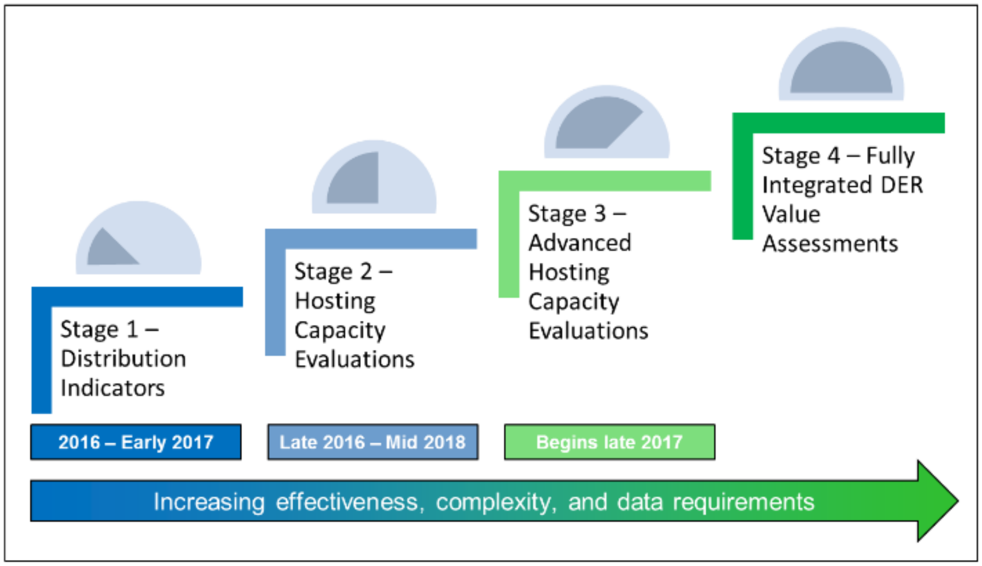
Several other utilities have published similar maps of their service territories. In New York, efforts to develop hosting capacity maps arose as part of the state's *Reforming the Energy Vision* (REV) proceeding, and in 2015 the New York Public Service Commission (NY PSC) required the utilities to include hosting capacity efforts in their Distributed System Implementation Plans (DSIP).[15] The Joint Utilities of New York[16] (JU) outlined four stages (Figure 6) in the development of their hosting capacity maps, with each stage adding greater granularity and data requirements, and increasing in computational complexity as modeling tools evolved.[17] This phased approach allows the JU to incorporate stakeholder feedback to help inform the prioritization of specific hosting capacity map enhancements that add the most value to developers.

[15] Stanfield, Sky and Stephanie Safdi. 2017. *Optimizing the Grid.* p. 35.

[16] The Joint Utilities are comprised of Central Hudson Gas and Electric Corporation, Consolidated Edison Company of New York, Inc. (Con Edison), New York State Electric & Gas Corporation, Niagara Mohawk Power Corporation d/b/a National Grid (National Grid), Orange and Rockland Utilities, Inc. and Rochester Gas and Electric Corporation.

[17] U.S. DOE. 2018. *Utility Practices in Hosting Capacity Analysis and Locational Value Assessment*. p. 13.

Figure 6: Joint Utilities Hosting Capacity Roadmap


Stage 1 – Distribution Indicators
Stage 2 – Hosting Capacity Evaluations
Stage 3 – Advanced Hosting Capacity Evaluations
Stage 4 – Fully Integrated DER Value Assessments
2016 – Early 2017
Late 2016 – Mid 2018
Begins late 2017
Increasing effectiveness, complexity, and data requirements

Source: Electric Power Research Institute ("EPRI"), Defining a Roadmap for Successful Implementation of a Hosting Capacity Method for New York State, June 2016, p. 5.

Currently, the JU is in Stage 3 of their roadmap and continues to add new functionality and upgrades to their hosting capacity maps based on stakeholder feedback. Some of these upgrades include an increased HCA refresh rate and a separate map layer focused on a load-based hosting capacity analysis.[18]

In Minnesota, Xcel provides an HCA heat map, which shows locations that may be more favorable for developers planning to interconnect DERs to the grid.

2.2.4. HCA Interconnection Technical Screen Case Study

Where DER penetration is high, like in Hawaii and California, the use of hosting capacity to inform DER interconnection technical screens has gained traction.[19] Hawaiian Electric Company (HECO) has implemented this approach and reports that use of hosting capacity for interconnection screening has substantially increased the amount of rooftop systems that they could fast-track.[20] California IOUs have also used hosting capacity information to inform and improve the Rule 21 interconnection[21] process to help expedite the interconnection of DERs. In 2020, the California Public Utilities Commission (CPUC) ordered the California IOUs to incorporate "Integration Capacity Analysis (ICA) results into the

[18] Joint Utilities of New York. "Hosting Capacity Stakeholder Webinar." November 19, 2020, p. 7. Available at: https://jointutilitiesofny.org/sites/default/files/JU%20Hosting%20Capacity%20Stakholder%20Session%20-%20November%202020.pdf.

[19] U.S. DOE. 2018. *Utility Practices in Hosting Capacity Analysis and Locational Value Assessment*. p. 18.

[20] Ibid.

[21] California Public Utilities Commission (CPUC). "Rule 21 interconnection." Available at: https://www.cpuc.ca.gov/Rule21/.

interconnection process to: (1) determine where and when existing circuits can accommodate additional distributed generation without requiring distribution upgrades and (2) allow interconnecting resources to export up to those limits."[22]

Washington, DC-based Pepco also uses the results of its HCA to help streamline the interconnection process in its service territory.[23] In combination with its Heat Map, which gives an indication of how much generation is currently installed and pending installation on a feeder, Pepco's HCA results allow a customer to analyze a point of interconnection to approximate the amount of remaining feeder capacity compared to the active and pending solar photovoltaic (PV) generation in the queue.[24] This provides a more accurate representation of the feasibility of interconnection at a particular location. However, all applications for interconnection still require a full review. Figure 7 provides an example of Pepco's hosting capacity map.

In Hawaii, HECO has an integrated interconnection queue for all areas, including those that currently exceed available hosting capacity, and customers can check the status of their interconnection application online.[25] HECO is also beginning to apply hosting capacity results for interconnection process automation and the development of the Fast Track process.[26]

[22] Kim, Anne Y. 2021. *California's Grid Modernization Report to the Governor and Legislature*. CPUC. p. 40.

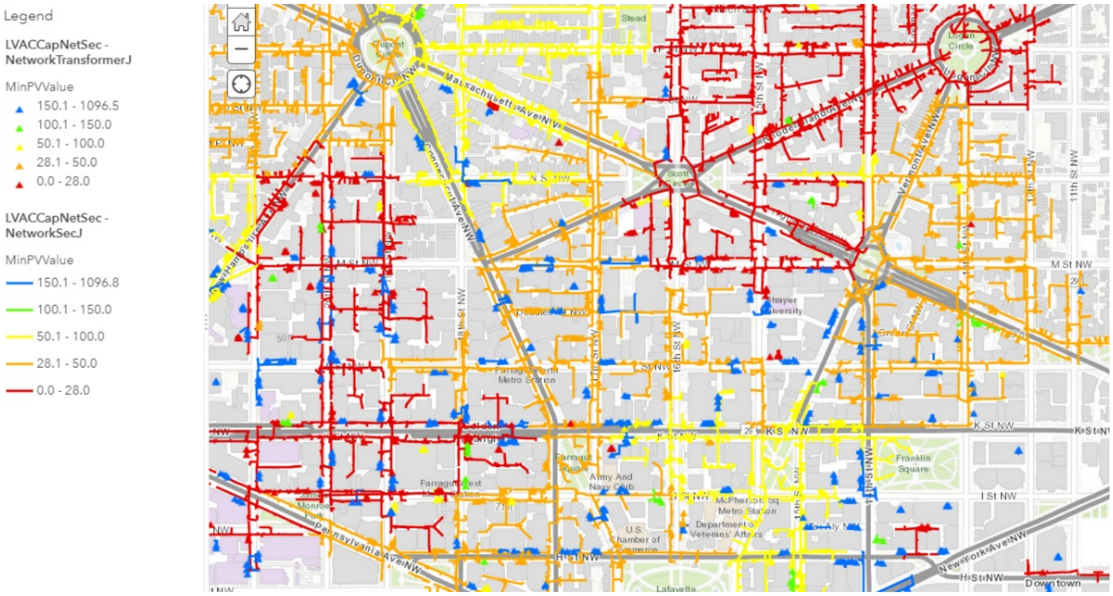
[23] Stanfield, Sky and Stephanie Safdi. 2017. *Optimizing the Grid.* p. 41.

[24] Potomac Electric Power Company. "Heat Map." Available at: https://www.pepco.com/SmartEnergy/MyGreenPowerConnection/Pages/HeatMap.aspx.

[25] Schwartz, Lisa. "Distribution Planning Regulatory Practices in Other States, Oregon Public Utility Commission Webinar." Lawrence Berkeley National Lab presentation for the U.S. Department of Energy's Office of Electricity, Transmission Permitting and Technical Assistance. May 21, 2020. p. 39. https://eta-publications.lbl.gov/sites/default/files/schwartz_puc_regulatory_practices_opuc_20200521.pdf.

[26] The Hawaiian Electric Companies. 2017. *Modernizing Hawai'i's Grid for Our Customers*. p. 29. https://www.hawaiianelectric.com/documents/clean_energy_hawaii/grid_modernization/final_august_2017_grid_modernization_strategy.pdf.

Figure 7: Pepco Hosting Capacity Map



Source: https://www.pepco.com/SmartEnergy/MyGreenPowerConnection/Pages/HostingCapacityMap.aspx.

In Minnesota, while Xcel does not currently utilize hosting capacity results in its interconnection process, it has investigated doing so, and it continues to improve its HCA to align with interconnection screens where possible.[27]

2.2.5. HCA Distribution Planning Case Study

In California, the IOUs are planning to use hosting capacity information as an input into their system planning processes to identify when and where capacity upgrades are needed on the distribution system in response to various DER growth scenarios.[28] They also proposed using the HCA results to help guide sourcing and procurement of DER solutions with additional locational granularity in the future.[29]

In Stage 4 of the New York JU's hosting capacity roadmap, the maps will be used to conduct fully integrated hosting capacity and value evaluations; they will indicate areas where DERs can bring additional value to the grid and identify ways to increase system hosting capacity. These fully integrated value assessments will help utility planners identify the locations where the deployment of DERs has the highest potential to reduce the overall net cost of operating the system.[30] A long-term goal of the JU is

[27] EPRI. 2020. *Defining a Roadmap for Integrating Hosting Capacity in the Interconnection Process.* p. 13.

[28] Pacific Gas and Electric Company (PG&E). 2016. *California Distribution Resources Plan (R.14-08-013) Integration Capacity Analysis Working Group Final ICA WG Report.* Appendix to Final ICA WG Report. p. 8. https://drpwg.org/wp-content/uploads/2016/07/ICA-WG-Final-Report.pdf.

[29] Ibid.

[30] Joint Utilities of New York. 2016. *Supplemental Distributed System Implementation Plan*. pp. 56-57.

developing the valuation methods and tools necessary for achieving the objectives of this stage.

In Hawaii, HECO is using its HCA in the planning process to assess potential system upgrades due to DER growth forecasts. Simultaneously, it is assessing portfolios of DERs to further optimize hosting capacity.[31]

2.2.6. Hosting Capacity Map Comparison Across Advanced Utilities

Publicly available hosting capacity map data can be beneficial to a variety of stakeholders including regulators, local governments, non-profits, electric customers, entrepreneurs, and DER developers. Some of the types of information that DER developers find useful include hosting capacity criteria violations, substation and (sub)feeder location and data, load profile (monthly and hourly), distributed generation (in queue and connected), and system upgrade cost estimates at specific locations given technical constraints. Utilities vary in the type and level of detail of grid data which they publish in their hosting capacity maps. Table 3 below compares the types of HCA grid data shown by states with utilities that are leading in the development of hosting capacity maps.

[31] The Hawaiian Electric Companies. 2017. *Modernizing Hawai'i's Grid for Our Customers*. p. 29.

Table 3: Hosting Capacity Map Comparison Across Advanced Utilities

Hosting Capacity Map System Data	States with Advanced Practices						
	California	D.C., DE, MD, NJ	Hawaii	Mass.	Minnesota	Nevada	New York
Solar PV HCA Availability	✓	✓	✓	✓	✓	✓	✓
Load HCA Availability	✓					✓	*
HCA Refresh Date	✓		✓	✓	✓	✓	✓
Substation Name	✓			✓	✓	✓	
Substation Location	✓				✓	✓	✓
Substation Bank Capacity	✓			✓			✓
Substation Peak Load	✓					✓	✓
Substation Load Profile	✓					✓	
Substation DG Connected/In Queue	✓				✓		✓
Substation Total DG	✓						✓
Feeder ID	✓	✓		✓		✓	✓
Circuit map layout (Feeder location)	✓	✓		✓		✓	✓
Heat map layout (No Feeder location)			✓		✓		
Feeder Capacity	✓			✓			
Feeder Peak Load	✓			✓		✓	
Feeder Load Profile	✓					✓	
Feeder DG Connected/In Queue	✓			✓	✓	✓	✓
Feeder Total DG							✓
DG Connected/In Queue Refresh Date	N/A			N/A	✓	N/A	✓
Nominal Voltage	✓			✓	✓	✓	✓
HCA Criteria Violations	✓				✓	✓	✓
Distance from feeder to substation						✓	
Impedance Data						✓	
Customer Type Breakdown	✓						

✓Indicates the data is present in the current public facing hosting capacity map.

** Indicates the data will be included in a future version of the hosting capacity map.*

"N/A" for the DG Connected/In Queue Refresh Date field indicates the same refresh rate as the rest of HCA data

California and Nevada provide the most detail on their hosting capacity maps. The California IOUs were ordered by the California Public Utilities Commission (CPUC) to provide this detailed information in support of DER developers and Nevada followed California's lead in terms of the provision of granular hosting capacity data. IOUs in these states provide both solar PV and load hosting capacity analyses to determine the incremental amount of DERs (e.g., solar PV, storage, electric vehicles) that can be accommodated on a feeder before causing a hosting capacity violation. They also both provide seasonal load profiles for the feeders. The California IOUs also provide substation load profiles. The California IOUs provide the percentage breakdown by customer type on their feeders and Nevada (NV) Energy provides other useful data on the distance from the feeder of interest to the substation along with the corresponding impedance data.

All the utilities provide the last date that the hosting capacity map was refreshed except for Pepco (e.g., Washington D.C., Maryland, Delaware, New Jersey) which updates a feeder's HCA results once per month if it has been flagged for one of the following reasons: (1) if 500kW of additional solar is approved; (2) if load on the feeder increases or drops significantly; or (3) if the feeder configuration changes. However, Pepco updates its entire hosting capacity map at least quarterly.[32]

Many of the utilities provide hosting capacity results on a nodal or line segment basis. However, Pepco provides its feeder hosting capacity results in terms of the maximum solar PV system size (in kW) given the substation transformer and feeder's hosting capacity constraints. HECO in Hawaii provides the percentage of space remaining for solar PV on the feeder as well as the total capacity output available (in kW) for customers to connect to the feeder. This is a proxy for the total distributed generation (shown in the table as DG) connected on the feeder. Additionally, all the utilities except Pepco and HECO provide nominal feeder voltage and hosting capacity violation information.

Xcel and the California and New York IOUs explicitly provide information about the existing or connected and queued distributed generation on a feeder and substation, while NV Energy only provides information about the connected distributed generation on a feeder. Pepco has a separate Heat Map, which provides pending, active, and total generation from all PV and non-PV generators.

While the California IOUs and NV Energy provide feeder load profiles that include minimum and peak loads, the New York IOUs only provide substation peak load. The California IOUs also provide the capacities of the feeders and substation banks, albeit on a separate public online map (the predecessor to the hosting capacity maps, called the PV RAM map). The New York IOUs provide the substation bank capacity. Xcel provides daytime minimum and absolute minimum loads for both its feeders and substations, but not peak load information.

Finally, all the utilities discussed here reveal their feeder lines, apart from HECO[33] and Xcel,[34] who present their hosting capacity results on a heat map. Xcel presents its HCA map as a "heat map" due to grid security concerns. HECO's locational value map (LVM) provides developers with a high-level view of approximately how much space may be available for private rooftop solar installations at a location on its primary system (e.g., not at the secondary level). While it is unclear exactly why HECO uses a heat map for its LVM, it is likely driven by its desire to maintain system reliability in the face of increasing DER penetration levels, rather than grid security concerns. Supporting evidence regarding this point are: (1) HECO does not typically have much supervisory control and data acquisition (SCADA) coverage on the

[32] Stanfield, Sky and Stephanie Safdi. 2017. *Optimizing the Grid.* p. 42.

[33] Hawaiian Electric Companies. "Oahu Locational Value Map." Available at: https://www.hawaiianelectric.com/clean-energy-hawaii/integration-tools-and-resources/locational-value-maps/oahu-locational-value-map-(lvm).

[34] Xcel Energy. "Hosting Capacity Map." Available at: https://www.xcelenergy.com/working_with_us/how_to_interconnect/hosting_capacity_map.

island, and thus primarily obtains grid data from its substations, reducing its ability to provide granular sub-feeder data and (2) HECO is careful not to reveal specific circuits that have additional hosting capacity since solar developers may heavily target them for DER interconnection. Regarding the first point, without sufficient SCADA coverage, HECO relies primarily on its substations for grid data, and cannot obtain data at the granularity necessary for a sub-feeder level HCA. Concerning the second point, Hawaii is closer than any other jurisdiction (e.g., New York or California) to experiencing the effects of high levels of DER penetration on system operations and reliability.[35] More specifically, in the near-term, it faces the dual challenge of reaching system and circuit hosting capacity levels.[36] Therefore, until HECO can modernize the grid and upgrade its infrastructure to accommodate additional generation from DERs, it does not necessarily want to advertise specific circuits where hosting capacity may be available.

NV Energy and the California and New York IOUs all reveal their feeders at the sub-feeder or line-segment level while Pepco reveals both its primary and secondary feeder locations. Additionally, all the utilities show distribution substations except HECO and Pepco. However, Pepco reveals the locations of its secondary transformers.

3. Customer Confidentiality And Grid Security

3.1. Overview

The Commission sought to elicit comments on grid and customer security issues related to the public display or access to grid data. These issues included, but were not limited to, distribution grid mapping, aggregated load data, and critical infrastructure. This section will discuss grid security and resiliency measures, how different utilities are balancing grid and customer security concerns with the release of sensitive hosting capacity map information, and the types of measures some utilities are taking to protect customer privacy using aggregation standards and CEII criteria.

3.2. Aggregation Standards and Customer Confidentiality

3.2.1. Overview of Customer Energy Use Data

As defined by the Commission, the purpose of protecting Customer Energy Use Data (CEUD) is to prevent third parties from accessing the energy-use patterns of a specific customer and data that reveals commercially sensitive information.[37] The Commission defined CEUD as "data collected from the

[35] The Hawaiian Electric Companies. 2017. *Modernizing Hawai'i's Grid for Our Customers*. Appendix C, p. 29.

[36] Ibid.

[37] Order Governing Disclosure of Customer Energy Use Data to Third Parties, Requiring Filing of Privacy Policies and Cost Data, and Soliciting Comment, Dkt. E,G-999/CI-12-1344, at 7-8 (Jan. 19, 2017) ("CEUD Privacy Order").

utility customer meters that reflects the quantity, quality, or timing of customers' natural gas or electric usage or electricity production."[38] It includes data regarding "the amount and timing of energy use and production; peak load contributions and the amount and timing of demand; and rate class."[39]

The Commission recognized that while the usefulness of this data generally increases with granularity, so does the potential for its misuse. The use cases for CEUD are numerous. Potential benefits of CEUD include helping to identify opportunities to pursue conservation, energy efficiency, and demand response programs. CEUD also helps third parties to implement these types of programs and gives policymakers the data needed to measure the effectiveness of those programs. The data may also be helpful in permitting greater use of electricity from renewable sources and reducing greenhouse gas emissions to help mitigate climate change.[40] Standards for the collection and sharing of CEUD for use by third parties should be designed to ensure that:

- Third parties may access aggregated or anonymized, disaggregated CEUD;
- The data be identified at the closest level of geographical specificity possible to maintain customer anonymity and at the finest practicable time interval;
- The utility, to the best of its ability, shall in a timely manner furnish this data in a consistent, standard format, aligned with industry best practices regarding ease of access and granularity of data; and
- Unless authorized by a customer, a third party shall not have access to any personally identifiable information (PII) for a customer.[41]

The Commission supports third parties having access to customer data if it does not violate the privacy of the individual without their consent.

Some risks that electric utilities face when sharing CEUD include:

- liability for the improper disclosure of their data and potential privacy violations;
- a damaged reputation should information be misused;
- administrative costs associated with organizing and transferring the data; and

[38] Id., p. 6.

[39] Minnesota Public Utilities Commission (MPUC). *Order Adopting Open Data Access Standards and Establishing Further Proceedings*. Dockets 12-1344/19-505, (November 20, 2020). Open Data Access Standards, p.1.

[40] Id., p. 3.

[41] MPUC. *Order Adopting Open Data Access Standards and Establishing Further Proceedings*. Dockets 12-1344/19-505, (November 20, 2020). Open Data Access Standards, p. 1.

- the lost ability to profit off exclusive knowledge of the data.[42]

Customers may also be concerned about the improper use of their data if sharing it could potentially "reveal information consumers would rather keep private."[43] The risks to customers, and to some extent the utilities, can be mitigated by removing PII that would violate customer privacy.

To remove PII, utilities in Minnesota can apply both aggregation and anonymization to CEUD. The utilization of both aggregation and anonymization can reduce the risk of revealing a specific customer's energy-use habits or of his/her PII being identified. The Department defined these terms as follows:

- Aggregated CEUD - data of individual customers located in a defined geographical area, which is combined into one collective data point per time interval.
- Anonymized CEUD - data of individual customers, which has been modified sufficiently to prevent the release of PII, collected over a number of time intervals from a defined geographical area. [44]

In summary, aggregated data refers to information that is grouped, while anonymized data refers to data where PII has been removed or modified.[45] By definition, all aggregated data is also anonymized.

Having outlined what CEUD is, the standards for collecting and sharing it, the purpose of protecting it and ways to do so, and the risks associated with its unauthorized disclosure, we will now focus on the different ways to aggregate CEUD.

3.2.2. Aggregation Standards for Customer Energy Use Data

When sharing data, utilities must do their best to make sure customer confidentiality is protected. Sometimes, customers explicitly allow their data to be shared. However, when this is not the case, certain protective measures must be put in place to assure that customer data is sufficiently protected. Methods that "prevent the release of aggregated or anonymized data sets that would put privacy at risk" are known as screens.[46] The Commission required utilities to establish defined practices to protect the anonymity of CEUD before releasing it to third parties.[47] Xcel selected the 15/15 standard to

[42] University of Chicago Law School, Abrams Environmental Law Clinic. 2016. *Regulatory Guide - Freeing Energy Data.* p. 15. Available at: https://www.law.uchicago.edu/files/file/freeing_energy_data_report_abrams_environmental_clinic_june_2016.pdf.

[43] Id., p. 20.

[44] MPUC. *Order Adopting Open Data Access Standards and Establishing Further Proceedings*. Open Data Access Standards, p.1.

[45] University of Chicago Law School, Abrams Environmental Law Clinic. p. 20.

[46] Seidman, Nancy, John Shenot. "Open Data Access Standards: Approaches in Other Jurisdictions." Presentation at the Minnesota Public Utilities Commission Technical Conference. Feb 26, 2021. p. 6. https://mn.gov/puc-stat/documents/pdf_files/RAP_Seidman%20and%20Shenot_State%20Policies%20for%20Aggregated%20or%20Anonymized%20Data%20Access_MN%20PUC_2021_FEBRUARY_26.pdf.

[47] *Order Governing Disclosure of Customer Energy Use Data to Third Parties, Requiring Filing of Privacy Policies and Cost Data, and Soliciting Comment*, Dkt. E,G-999/CI-12-1344. (Jan. 19, 2017). pp. 7-8.

determine if CEUD is sufficiently aggregated to be released.[48] Under this standard, data given to requestors must be aggregated into groups of at least 15 customers with no customer comprising more than 15 percent of the load in the given dataset.[49] Table 4 provides an overview of common aggregation standards used to protect customer data. Some prioritize customer protection while others favor providing more granular data to third-party data requestors.

Table 4: Typical Aggregation Standards

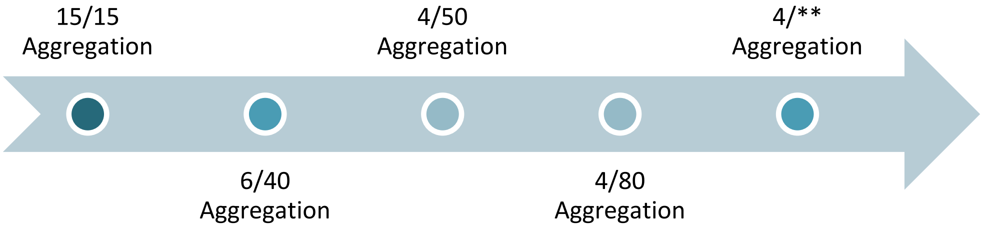
Standard	Overview	Level of Customer Privacy
15/15	Requires at least 15 customers to be included in a dataset, with no customer accounting for more than 15% of the total energy use	• High level of customer protection • Data is less granular for third-party use
6/40	Requires at least 6 customers to be included in a dataset with no customer accounting for more than 40% of the total energy use	• More customers are included, but risk of identification is higher than 15/15 standard • Data is somewhat granular for third-party use; some customers are still redacted
4/50	Requires at least 4 customers to be included in a dataset, with no customer accounting for more than 50% of the total energy use	• Lower level of customer protection • Data is more granular, and more data is included for third-party use
4/80	Requires at least 4 customers to be included in a dataset, with no customer accounting for more than 80% of the total energy use	• Lower level of customer privacy/protection • Nearly all information is included, and data is relatively granular for third-party use
4/**	Requires at least 4 customers to be included in a dataset	• Customers may be identified under some circumstances • Data is granular for third-party use; only datasets that serve less than 4 customers are not available

Most states apply the 15/15 standard to CEUD, while many of the other standards are applied to whole building energy-use data. Generally, CEUD is held to a higher standard of protection, and increasing the number of customers and decreasing the maximum percentage of total energy use leads to greater data anonymization and protection. Figure 8 portrays how changing the aggregation standard increases the data's usability while decreasing the level of protection for customers.

[48] *Xcel Energy Compliance Filing Annual Report.* Docket Nos.E,G999/CI-12-1344 and E,G999/M-19-505. (March 1, 2021), p. 4.

[49] Ibid.

Figure 8: Data Granularity for Aggregation Standards



Increasing Levels of Data Usability but Reduced Customer Protection

3.2.3. Discussion of Aggregation Standards in Minnesota

In November 2020, the Commission discussed the appropriateness of the 15/15 aggregation standard and explored the use of multiple standards to aggregate and anonymize datasets when provided to different third parties.[50] The Commission also discussed the use of a 4/50 aggregation standard for the same federal and state government entities, with the addition of "property owners or managers, so long as the CEUD requested applies only to the property the requestor owns or manages."[51] The Commission requested further expertise on topics including uniform customer access forms, segmented aggregation screens, and the refinement of contract requirements for anonymized data access.[52] The Commission continued to approve the Open Data Access standards proposed by the Citizens Utility Board which included standards for the types and format of data released.[53]

This report will focus on the application of the 15/15 aggregation standard in the context of protecting customer privacy on Xcel's hosting capacity map. The use of the 15/15 standard here is not meant to prejudice any decisions related to the access and privacy of CEUD in the context of the Commission's ongoing proceedings pertaining to its adoption of the Open Data Access Standards.

3.3. Critical Energy Infrastructure Information

3.3.1. Overview of CEII

Critical data is data which must be removed from the public domain to maintain its security. This may include information such as the location of feeders leading to critical customer groups or critical infrastructure. Several federal agencies have provided guidance and regulations regarding critical

[50] *Order Adopting Open Data Access Standards and Establishing Further Proceedings*, Dockets 12-1344/19-505, (November 20, 2020). pp. 7-8.

[51] Ibid.

[52] Ibid.

[53] Ibid.

infrastructure. At the national level, the Cybersecurity & Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS) has identified 16 critical infrastructure sectors that it considers “so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.”[54] These sectors were identified as part of Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure and Resilience and advance national policy to “strengthen and maintain secure, functioning, and resilient critical infrastructure.”[55] Table 5 lists the 16 sectors.

Table 5: DHS Critical Infrastructure Sectors

Critical Infrastructure Sectors	
• Chemical • Commercial • Communications • Critical Manufacturing • Dams • Defense Industrial Base • Emergency Services • Energy	• Financial Services • Food and Agriculture • Government Facilities • Healthcare and Public Health • Information Technology • Nuclear Reactors, Materials, and Waste • Transportation Systems • Water and Wastewater Systems

In addition to knowing which sectors to protect, it is also important to know how to protect them. Specifically, for bulk power system entities, the North American Electric Reliability Corporation (NERC) established mandatory Critical Infrastructure Protection (CIP) standards, including for the protection of sensitive data. For example, CIP-011-2, Information Protection, is structured “to prevent unauthorized access to Bulk Electric System (BES) Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.”[56] There are currently 12 CIP standards subject to enforcement which include the Physical Security Reliability Standard (CIP-014) and 11 cybersecurity standards. Table 6 provides several examples of CIP standards.

Table 6: NERC Critical Infrastructure Protection Standards

Standard	Name	Status
CIP-003-8	Cyber Security – Security Management Controls	Subject to Enforcement
CIP-004-6	Cyber Security – Personnel & Training	Subject to Enforcement
CIP-007-6	Cyber Security – System Security Management	Subject to Enforcement

[54] Cybersecurity & Infrastructure Agency. “Critical Infrastructure Sectors.” Available at: https://www.cisa.gov/critical-infrastructure-sectors.

[55] Ibid.

[56] North American Reliability Corporation. “Critical Infrastructure Protection Standards.” Available at: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

CIP-011-2	Cyber Security – Information Protection	Subject to Enforcement
CIP-012-1	Cyber Security – Communication btw. Control Centers	Subject to Enforcement
CIP-014-2	Physical Security	Subject to Enforcement

No corollary to the NERC Critical Infrastructure Protection Standards for the bulk power system exists for distribution system infrastructure.

The Federal Energy Regulatory Commission (FERC) oversees the designation of critical infrastructure. FERC Regulation 18 C.F.R. § 388.133 defines Critical Energy Infrastructure Information (CEII) as specific engineering, vulnerability, or detailed design information related to a “system or asset of the bulk-power system (physical or virtual)” in which “the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters” which:

1. Relates details about the production, generation, transmission, or distribution of energy;
2. Could be useful to a person planning an attack on critical infrastructure;
3. Is exempt from mandatory disclosure under the Freedom of Information Act (5 U.S.C. § 552); and
4. Gives strategic information beyond the location of the critical infrastructure.[57]

It is important to note that the FERC’s process for requesting CEII treatment of information only refers to an asset(s) or system(s) of the bulk power system and is not defined with respect to the distribution system. Furthermore, only the FERC can designate information as CEII.[58] Requestors who wish to designate information as CEII must explain the legal justification for such treatment according to the FERC’s criteria. For specific locational information, requestors need to justify their request and explain why the information is not already publicly known.[59] When making its determination, the FERC considers the public’s need to have access to the information to effectively participate in proceedings. In addition, the FERC provides an administrative appeal process to challenge CEII designations or disclosures and provides the opportunity for the public to request access to CEII by submitting a detailed statement of need and executing a non-disclosure agreement (NDA), limited to one calendar year.[60]

3.4. Grid Security and Resilience

[57] Federal Energy Regulatory Commission, “Critical Energy Infrastructure Information.” Available at: https://www.ferc.gov/enforcement-legal/ceii.

[58] Ibid.

[59] Ibid.

[60] Ibid.

3.4.1. *Overview of Grid Security*

A reliable electric grid is a key pillar of the nation's economic and national security, and federal government authorities, nonprofit organizations, and the electric utility industry have made significant strides towards maintaining a secure and reliable electric system. The *Energy Policy Act of 2005* included provisions to strengthen the electric grid through the introduction of mandatory reliability standards, although they are not specifically aimed at protecting the grid against terrorist attack.[61]

However, a 2013 sniper attack on Pacific Gas and Electric's Metcalf transmission substation in California marked a turning point for the U.S. electric power sector. The attack led to the NERC establishing mandatory CIP standards for the physical and cyber security of the BES in 2015.[62] The attack also prompted electric utilities across the country to reassess their grid security programs and to apply closer scrutiny to the vulnerability of critical distribution assets to various kinds of physical and cyber-attacks.

3.4.2. *Grid Security Vulnerabilities and Threats*

There are three main categories of electric system vulnerabilities which can result in the disruption of the grid's power supply. These are physical security, cybersecurity, and personnel vulnerabilities. This report will only focus on physical and cybersecurity vulnerabilities.

<u>Physical Security Vulnerability and Threats</u>

Overview

In the United States, the electric power grid consists of over 200,000 miles of high-voltage transmission lines interspersed with hundreds of large electric power transformers.[63] Once electricity is generated, it is stepped up in voltage and transported over long distances before being distributed to consumers. The major components of transmission systems are substation transformers, which step-up and step-down voltage to more efficiently transport power over long distances, transmission towers to connect high-voltage power lines, and control centers to manage the delivery of power from generation resources to the distributed system loads.[64] Figure 9 displays the operations of the U.S. electric grid.

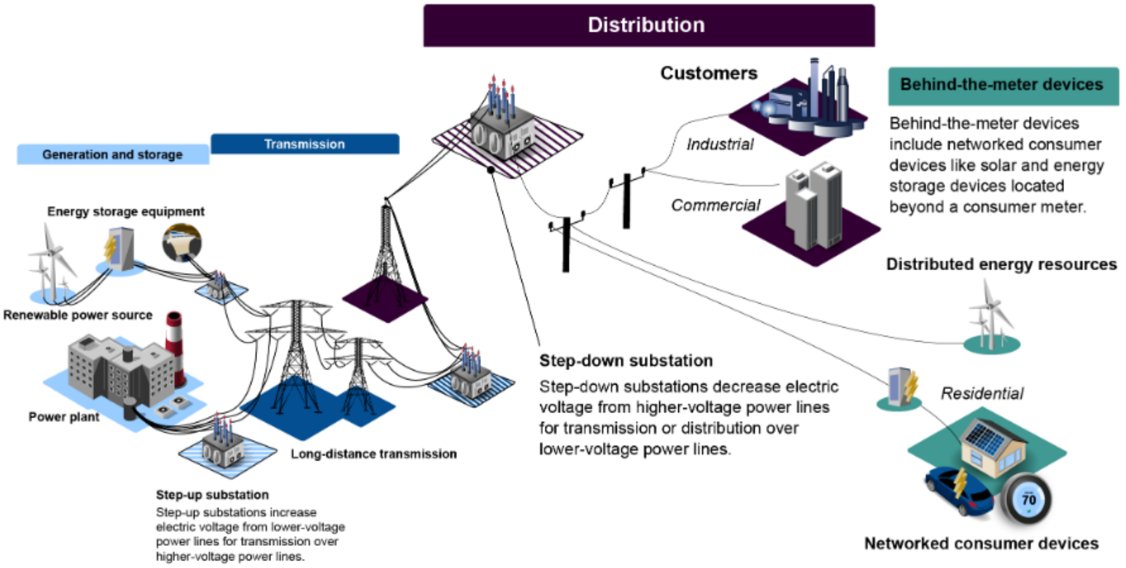
[61] National Research Council. 2012. *Terrorism and the Electric Power Delivery System Washington, DC.* The National Academies Press. p. 2. Available at: https://doi.org/10.17226/12050.

[62] Parfomak, Paul. 2018. *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?* Congressional Research Service. p. 20. Available at: https://fas.org/sgp/crs/homesec/R45135.pdf.

[63] Parfomak, Paul. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations.* p.2. Available at: https://assets. documentcloud.org/documents/1303171/2014-crs-report.pdf.

[64] Idaho National Laboratory. 2016. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*. p.10. Available at: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

Figure 9: Functions of the U.S. Electric Grid


Distribution
Customers
Behind-the-meter devices
Behind-the-meter devices include networked consumer devices like solar and energy storage devices located beyond a consumer meter.
Generation and storage
Transmission
Industrial
Commercial
Energy storage equipment
Distributed energy resources
Renewable power source
Step-down substation
Step-down substations decrease electric voltage from higher-voltage power lines for transmission or distribution over lower-voltage power lines.
Power plant
Residential
Long-distance transmission
Step-up substation
Step-up substations increase electric voltage from lower-voltage power lines for transmission over higher-voltage power lines.
70
Networked consumer devices

Source: U.S. Government Accountability Office (GAO), Electric Grid Cybersecurity, DOE Needs to Ensure its Plans Fully Address Risks to Distribution Systems, March 2021, p.6. https://www.gao.gov/assets/gao-21-81.pdf.

Transmission

To significantly impact transmission of power throughout the grid, an attacker would have to simultaneously interrupt or destroy multiple high-voltage transmission lines or high-voltage transformers.[65] Large power/high-voltage transformers, which step power down from transmission to distribution levels, are critical to the nation's power grid. These critical devices account for fewer than three percent of the transformers in U.S. substations but carry 60–70 percent of the nation's electricity.[66] The impact of extended power outages from the loss of one or more of these high-voltage transformers could disrupt electricity services over a wide area of the country and is of significant concern.[67] Risk from loss of these transformers is heightened by the lack of alternate electricity delivery paths or the lack of access to spare transformers in many transmission utilities.[68]

A 2017 report from the National Academy of Sciences (NAS) concludes: "While to date there have been only minor attacks on the power system in the United States, large-scale physical destruction of key parts of the power system by terrorists is a real danger. Some physical attacks could cause disruption in

[65] Ibid.

[66] Parfomak, Paul. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*. p.2.

[67] U.S. DOE. "Addressing Security and Reliability Concerns of Large Power Transformers." Available at: https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers.

[68] Idaho National Laboratory, p. 10.

system operations that last for weeks or months."[69] Substations and the high-voltage transformers they contain are especially vulnerable to physical attack, as well as some transmission lines where the destruction of a small number of towers could bring down many kilometers of line.[70] High-voltage transformers face several challenges which make them particularly vulnerable, including being very large, difficult to transport, typically custom-made, generally expensive (sometimes costing $3 million each[71]), and hard to replace with procurement lead times of one year or longer.[72] Most are also no longer built in the United States.[73]

High-voltage transformers are also the most vulnerable to intentional damage from malicious acts.[74] Recent domestic terrorist attacks on high-voltage transformers highlight their particular vulnerability to physical attack. The 2013 high-powered rifle assault on the 500 kilovolt (kV) transformer Metcalf substation only lasted 19-minutes but caused $15 million in damages.[75] In 2016, a similar high-powered rifle attack on a 69 kV transformer in Garkane Energy Cooperative's Buckskin substation in southern Utah reportedly left 13,000 rural customers without power for up to eight hours.[76]

Distribution

Physical attacks are not limited to the transmission system. Physical attacks on distribution transformers, circuits (e.g., feeders), protective devices, and other distribution system assets could impact the electricity supply to critical local customers like hospitals. There are no mandatory federal standards, like the NERC CIP standards which apply to the bulk power system, that are governing distribution systems, over which states have authority. Thus, there are varying standards of protection for distribution systems. However, the Metcalf attack has led to calls to not only guard against potential attacks on federally regulated, critical bulk power assets, but also to protect distribution assets under state-level purview.[77] For example, following the Metcalf incident, California lawmakers passed new legislation (SB 6991) that directed the CPUC to consider adoption of new standards and rules to address

[69] National Academy of Sciences, Engineering, and Medicine. 2017. *Enhancing the Resilience of the Nation's Electricity System*. p. 64. Available at: https://doi.org/10.17226/24836.

[70] National Research Council. 2012. *Terrorism and the Electric Power Delivery System.* p. 2.

[71] Pagliery, Jose. October 17, 2015. "Sniper attack on California power grid may have been 'an insider' DHS says." *CNN Business*. Available at: https://money.cnn.com/2015/10/16/technology/sniper-power-grid/.

[72] U.S. DOE. "Addressing Security and Reliability Concerns of Large Power Transformers." Available at: https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers.

[73] National Research Council. 2012. *Terrorism and the Electric Power Delivery System.* p. 2.

[74] Parfomak, Paul. 2014. *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations.* p. 2.

[75] Pagliery, Jose. 2015.

[76] Parfomak, Paul. 2018. *NERC Standards for Bulk Power Physical Security: Is the Grid More Secure?* p. 2.

[77] CPUC. January 2018. *Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699. CPUC staff white paper*. p. 4. Available at: https://www.cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Risk_Assessment/physicalsecurity/Final%20CPUC_Physical_Security_White_Paper_January_2018(1).pdf.

any physical security risk to the distribution system to ensure “high-quality, safe, and reliable service.”[78] Additionally, some utilities are voluntarily taking action to strengthen their distribution systems to make them more resilient to potential attacks.

Cyber Security Vulnerability and Threats

Overview

The modern grid relies heavily on high-speed communications, automation, and centralized monitoring, control, and protection of equipment. The cyber-physical systems of the electric sector include industrial control systems (ICS), which allow for synchronous, digital control of sensitive processes and the physical operations of equipment at the generation, transmission, and distribution system levels. These operations include physical functions such as the opening and closing of circuit breakers on the grid. Advances in ICS technology have resulted in advantages such as easier system operation and maintenance, and more detailed systems data. However, they have also increased the vulnerability of the systems to cyberattacks through internet or network connections from remote sites (e.g., virtual private network).[79] Any telecommunication link that is even partially outside the control of the system operators is a potentially insecure pathway into operations and a threat to the grid.[80] Figure 10 shows the typical types of cyber-attack techniques which can be used to gain access to ICS.

The most critical ICS are the supervisory control and data acquisition (SCADA) systems that gather real-time measurements from substations and send out control signals to equipment such as circuit breakers.[81] If hackers could gain access, they could manipulate SCADA systems to disrupt the flow of electricity, transmit erroneous signals to operators, block the flow of vital information, or disable protective systems.[82] Such cyberattacks would require a high level of sophistication and expertise.

[78] Ibid.

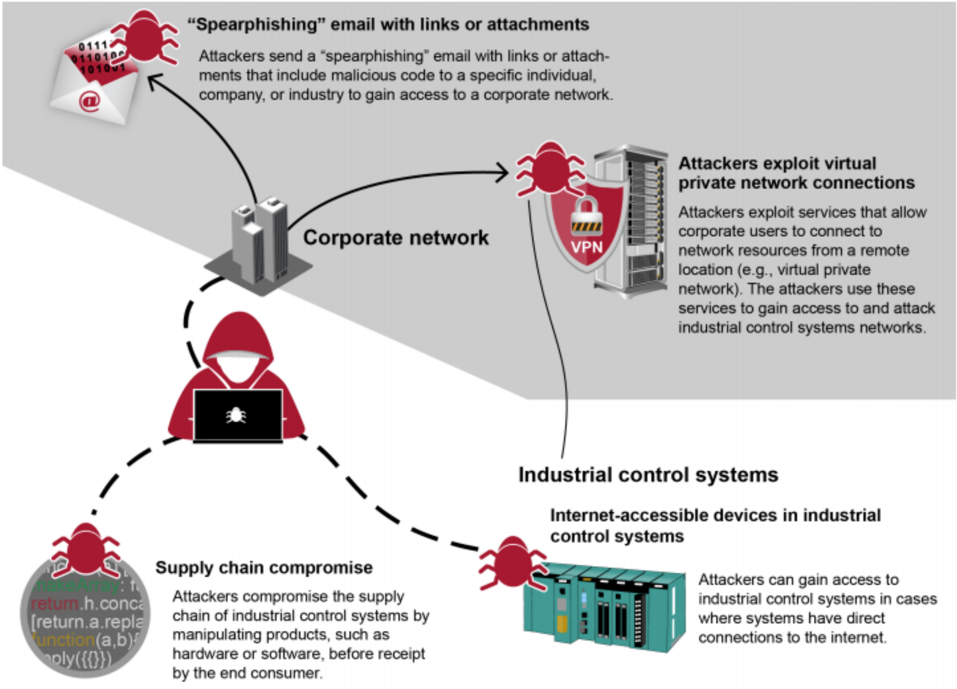
[79] U.S. Government Accountability Office (GAO). 2021. *Electric Grid Cybersecurity, DOE Needs to Ensure its Plans Fully Address Risks to Distribution Systems*. p. 13. Available at: https://www.gao.gov/assets/gao-21-81.pdf.

[80] National Research Council. 2012. *Terrorism and the Electric Power Delivery System.* p. 2.

[81] Ibid.

[82] Ibid.

Figure 10: Examples of Techniques for Gaining Initial Access to Industrial Control Systems



"Spearphishing" email with links or attachments

Attackers send a "spearphishing" email with links or attachments that include malicious code to a specific individual, company, or industry to gain access to a corporate network.

Attackers exploit virtual private network connections

Attackers exploit services that allow corporate users to connect to network resources from a remote location (e.g., virtual private network). The attackers use these services to gain access to and attack industrial control systems networks.

Internet-accessible devices in industrial control systems

Attackers can gain access to industrial control systems in cases where systems have direct connections to the internet.

Supply chain compromise

Attackers compromise the supply chain of industrial control systems by manipulating products, such as hardware or software, before receipt by the end consumer.

Source: GAO analysis of industry and federal documents. | GAO-21-81

Source: U.S. GAO, Electric Grid Cybersecurity, DOE Needs to Ensure its Plans Fully Address Risks to Distribution Systems, March 2021, p.14. https://www.gao.gov/assets/gao-21-81.pdf.

Cyber-attacks are unlikely to cause extended outages, but if well-coordinated, they could magnify the damage of a physical attack.[83] For example, a cascading power outage resulting from a physical attack on the transmission system would be aggravated, if a cyber-attacker exploited an ICS vulnerability, causing a loss of visibility into grid operations, which delayed the system operator's response time.[84] Furthermore, ICS experts note that if a threat actor can physically access a substation, there is virtually no limit to potential damage, since malware could be directly introduced to computers and devices resulting in the manipulation (e.g., protective relays), and destruction of electrical equipment.[85]

Transmission

Cyber threats to utilities responsible for transmission depend on several variables, such as network configuration within a substation, and means of communicating data.[86] Modern substations use several kinds of communication to manage local functions. Transmission substations are subject to mandatory NERC CIP cyber security standards, making unauthorized access to substation networks difficult, and

[83] Ibid.

[84] Ibid.

[85] Idaho National Laboratory. 2016. p. 11.

[86] Ibid.

likely requiring advanced skill by a threat actor.[87] However, controllers and other devices increasingly used in substation automation are often sources of numerous ICS vulnerabilities and can serve as entry points to networks. Once inside the digital operations of a substation, an attacker with the necessary skills and tools could disrupt, desynchronize, or impact data communications necessary for communications and controls causing load instability.[88] Substation networks without detection capabilities to identify intrusions and malicious data injection could allow an attacker to manipulate multiple substations over time without discovery.[89] In these networks, the risk of a coordinated cyber-attack powerful enough to disrupt a portion of the grid is greater.[90]

Distribution

A recent U.S. Government Accountability Office (GAO) report for the Department of Energy (DOE) on distribution grid cybersecurity notes that the U.S distribution systems are increasingly at risk from cyberattacks and are growing more vulnerable, in part, because their ICS connect to business networks and allow remote access.[91] As a result, threat actors can use multiple techniques to access those systems and potentially disrupt operations. However, the GAO report states that "none of the cybersecurity incidents reported in the United States have disrupted the reliability or availability of the grid's distribution systems, according to the DOE, which requires all U.S. electric utilities to report significant electrical incidents or disturbances."[92]

However, just because there has not been a cyber-attack on a U.S. distribution system does not mean one could not occur. The first confirmed cyber-attack to affect a distribution grid occurred in the Ukraine and resulted in a localized power outage in 2015.[93] Attackers launched an email phishing campaign to target IT personnel of power distribution companies and used malware to gain access to IT infrastructure.[94] They then hijacked the SCADA distribution management system (DMS) to "cause undesirable state changes to the distribution electricity infrastructure and attempted to delay…restoration by wiping SCADA servers after they caused the outage," while simultaneously preventing calls reporting power outages from reaching customer service centers.[95] The event resulted in a 3- to 6-hour outage that left more than 230,000 customers without electricity.[96]

[87] Ibid.

[88] Ibid.

[89] Ibid.

[90] Ibid.

[91] U.S. GAO. 2021. p. 2.

[92] Id., p. 22.

[93] Idaho National Laboratory, p. 11.

[94] Ibid.

[95] Ibid.

[96] Ibid.

Several energy utility companies stated that physical attacks on energy distribution machines are much more effective at taking out the power grid than a computer hack and are easy to pull off.[97] However, cyber-attacks on distribution systems could also have a significant impact if they reach the bulk power system. The GAO report notes that the scale of potential impacts on the bulk power system from a cyberattack on the grid's distribution systems is not well understood.[98]

As the deployment of DERs on the grid increases, so does the potential for these devices to face cyber threats. DER devices, owned and controlled by consumers and third parties, are equipped with digital communications and control interfaces to communicate, and interconnect with the grid.[99] These DER communication interfaces enable utility features such as remote access and control, but also provide a possible entry point for a cyberattack. The National Renewable Energy Laboratory (NREL) notes that utilities that interconnect with third-party DERs should consider cybersecurity measures at the business process and network layers of the grid's devices, communication channels, and higher-level applications.[100]

3.5. Grid Resilience

3.5.1. Overview

Resilience is a relatively new concept in utility resource planning and currently, no formal grid resilience definitions, metrics, or analysis methods have been universally accepted. The staff of the Hawaiian Public Utilities Commission defined resilience, in the context of the electric distribution system, as the ability of the system or its components to anticipate, absorb, adapt to, and rapidly recover from disruptions or a catastrophic event.[101] NREL defines the magnitude of resilience provided by renewable energy hybrid systems (e.g., microgrids) as the amount of time that the critical load is served during a grid outage and the value of the resilience as the economic value of serving the critical load.[102] All relevant costs must be captured, including the costs that utilities might incur to mitigate (and recover from) severe outages, as well as the cost of the outage to customers and the community.[103] It might

[97] Pagliery, Jose. 2015.

[98] U.S. GAO. 2021. p. 22.

[99] Horowitz, Kelsey, Zac Peterson, Michael Coddington, Fei Ding, Ben Sigrin, Danish Saleem, Sara E. Baldwin, et al. 2019. *An Overview of Distributed Energy Resource (DER) Interconnection: Current Practices and Emerging Solutions.* NREL, p. 47. Available at: https://www.nrel.gov/docs/fy19osti/72102.pdf.

[100] Ibid.

[101] Hawaiian Public Service Commission (HI PSC). 2020. *Resilience Working Group Report for Integrated Grid Planning, Hawaiian Electric Company, Maui Electric Company, and Hawai'i Electric Light Company.* p. 6. Available at: https://www.hawaiianelectric.com/documents/clean_energy_hawaii/integrated_grid_planning/stakeholder_engagement/working_groups/resilience/20200429_rwg_report.pdf.

[102] Kate Anderson, Nicholas D. Laws, Spencer Marr, Lars Lisell, Tony Jimenez, Tria Case, Xiangkun Li, Dag Lohmann and Dylan Cutler*.* 2018*. Quantifying and Monetizing Renewable Energy Resiliency.* National Renewable Energy Lab and City University of New York. p. 2. Available at: https://www.mdpi.com/2071-1050/10/4/933.

[103] HI PSC, Resilience Working Group Report for Integrated Grid Planning. p. 11.

also include costs that customers incur to mitigate the impact of severe outages, especially if those measures might be more cost effective than those incurred by the utility.[104] However, metrics to measure the resilience of electrical distribution systems are not strictly limited to costs. For example, to evaluate community resilience in response to electricity service disruptions in Puerto Rico, Sandia National Labs employed a resilience metric, which measures the burden on members of the community to satisfy their basic needs. Burden is a function of the effort required to satisfy each need, as well as each individual's ability to acquire each infrastructure service.[105] The idea is that a more resilient community will better prepare for, withstand, respond to, and recover from extreme shocks, thereby decreasing the burden imposed on its citizens following a disruption.[106]

Some resilience objectives include:

- Reducing the likelihood of power outages during a severe event;
- Reducing the severity and duration of any outages that do occur during and after a severe event;
- Reducing restoration and recovery times following a severe event;
- Returning critical infrastructure customers’ power rapidly to enable mutual support and recovery during an emergency;
- Returning all customers’ power within appropriate times; and
- Limiting the environmental impacts of a severe event.[107]

3.5.2. Grid Resilience in the Face of Threats

It is also important to consider the categories of threats, such as extreme weather events and physical and cyber-attacks, and how the electric utility would prepare for and respond to these threat scenarios to help ensure a resilient grid.

Table 7 highlights some measures that a utility could take to help reduce distribution system vulnerabilities and enhance grid resiliency.

[104] Ibid.

[105] Robert F. Jeffers, Michael J. Baca, Amanda M. Wachtel, Sean DeRosa, Andrea Staid, William Fogleman, Alexander Outkin, Frank Currie, 2018. “Analysis of Microgrid Locations Benefitting Community Resilience for Puerto Rico.” Sandia National Labs. p. 6. Available at: https://doi.org/10.2172/1481633.

[106] Ibid.

[107] HI PSC*, Resilience Working Group Report for Integrated Grid Planning*. p. 11.

Table 7: Options for Enhancing Grid Resiliency

Threat Scenario	Resiliency Measures
Cyber-attack	• Elimination of non-essential pathways to external systems • Improved cybersecurity for sensors, communication, and control systems • Systems to monitor for, and help avoid, operator error
Physical Attack	• Hardening of key substations and control centers • Substation fencing • Increased surveillance • Stockpiling of spare and mobile transformers
Extreme Weather Event	• Vegetation management • Hardening of overhead poles and crossarms (e.g., fiberglass) • Undergrounding cables • Fault Location, Isolation, and Service Restoration (FLISR)

Source: National Research Council 2012. Terrorism and the Electric Power Delivery System, p.3. https://doi.org/10.17226/12050.

Xcel's Grid Resilience Efforts

Xcel takes several measures to enhance the resilience of its distribution system. For example, Xcel's cyber security program has five categories (identify, protect, detect, respond, recover) of controls to protect and detect cyber threats to its network.[108] These controls include user access controls, encryption, use of digital certificates for user authentication, scanning equipment for known security vulnerabilities, monitoring and detecting potentially anomalous activity, data validation, communications firewalls, and periodic software updates to improve system performance and address security vulnerabilities.[109] Among other things, to enhance the physical security of its system, Xcel encloses all of its substations primarily with fencing and in some cases walls, uses motion security lighting and conducts remote surveillance of critical assets, and undergrounds some of its power lines.[110] Xcel also has spare and mobile transformers which it can deploy as needed. To make the grid more resilient to extreme weather events, Xcel has a vegetation management program, hardens its overhead poles and crossarms, and a subset of its feeders have an automated IntelliTeam scheme, which can automatically isolate and restore service to most customers when a fault occurs through switching from adjacent feeders.[111] However, most switching is done manually. When there is a power disruption, Xcel can typically address a routine outage in under two hours, a more severe outage in 4-6

[108] Xcel Energy. *2019 Integrated Distribution Plan.* Docket No. E002/M-19-666. Attachment M1, p. 240. Available at: https://www.xcelenergy.com/staticfiles/xe-responsive/Company/Rates%20&%20Regulations/IntegratedDistributionPlan.pdf.

[109] Ibid.

[110] Conversation about system resiliency with Xcel distribution planning team, April 23, 2021.

[111] Ibid.

hours through switching and/or substation transformer restoration, and in approximately 24 hours if a mobile transformer must be deployed to replace a damaged transformer.[112]

Xcel is also enhancing the resiliency of the grid through grid modernization programs and related efforts. For example, Xcel's Advanced Grid Intelligence and Security (AGIS) Initiative consists of multiple elements that work together to create a more modern and advanced distribution grid. These elements include:

1) Advanced Distribution Management System (ADMS): Consists of a real-time operating system that enables enhanced visibility into the distribution power grid and controls advanced field devices; and

2) Advanced Metering Infrastructure (AMI): Consists of an integrated system of advanced meters, communication networks, and data management systems that enable secure two-way communication between Xcel's data systems and customer meters.[113]

Protective cyber security and information technology (IT) support underlie these components.[114]

Lastly, Xcel is investigating programs like its Community Resiliency and Resiliency as a Service Program to make its distribution system more resilient through the use of distributed generation and microgrids. The Community Resiliency program involves working with communities to identify strategic locations, such as a community center or facility that provides essential services, where Xcel would provide additional back-up power with a microgrid during an extended or widespread outage.[115] Xcel plans to install the equipment necessary to provide back-up power at one strategic location in 2022.[116] In the Resiliency as a Service Program, Xcel is seeking qualified vendors to interconnect DERs and microgrids to commercial and industrial customers that have a need for higher than standard service reliability.[117]

3.6. Balancing grid security with the public benefits of HCA map data

3.6.1. Overview

In recent years, there has been a growing trend towards access of large amounts of data as it has become increasingly important for innovation, smart decision-making, economic growth, and the public good. Data access can support disaster response, agricultural and food security, mitigating climate change, and improving healthcare. For example, public access to sensitive health records sped up the

[112] Ibid.

[113] Xcel Energy. 2019. *2019 Integrated Distribution Plan.* p. 147.

[114] Ibid.

[115] Id., p. 114.

[116] Ibid.

[117] Xcel Energy. "Resiliency as a Service: Request for Qualifications." Available at: https://www.xcelenergy.com/working_with_us/renewable_developer_resource_center/resiliency_as_a_service_request_for_qualifications.

development of lifesaving medical treatments like the coronavirus vaccines produced by Moderna and Pfizer. And the federal government has created a website (data.gov) that hosts and assembles hundreds of thousands of data sets for public use, democratizing knowledge for the digital age. Economics tells us that society needs more data sharing rather than less, because the benefits of publicly available data often outweigh the costs.[118]

Access to distribution grid data for energy developers and other third parties is in the public's interest because it can increase the transparency of the utility's provision of electrical services, assist in the identification of potential DER interconnection sites, and help enable developers to accelerate progress towards decarbonizing Minnesota's grid through the efficient deployment of DERs.

However, there is also a growing recognition that vulnerabilities exist in the energy sector, including in the distribution system, and can potentially be exploited by domestic and foreign bad actors. Therefore, there must be a balance between increasing the availability of grid data for the public good while also appropriately protecting it from foreign and domestic threats.

The Commission has provided an opportunity to reconcile these competing objectives. On October 30, 2020, the Commission requested comments on "Grid and Customer Security Issues Related to Public Display or Access to Electric Distribution Grid Data" to help address the question of how we can increase the availability of grid data for the public good, while also protecting it from threats which could potentially lead to an attack on the grid.[119]

The following sections outline how energy developers benefit from increasing access to distribution grid data, how utilities in Minnesota and California currently address grid and customer security risks posed by revealing sensitive grid data on their hosting capacity maps, the types of hosting capacity information that utilities leading in this space reveal, the severity of the types of risks posed by making this grid data available, and recommendations on how to potentially move forward with addressing the competing demands of making the grid data public.

3.6.2. Public Benefits of Access to Hosting Capacity Grid Data

<u>Overview</u>

Fundamentally, hosting capacity maps provide information on the distribution system that can be used by third parties such as energy customers and developers, entrepreneurs, researchers, policy makers, clean energy advocates, and others, to deploy DERs more efficiently and effectively on the grid. This helps make the grid more reliable and resilient to threats (e.g., natural disasters) while simultaneously

[118] Deming, David. February 19, 2021. "Balancing Privacy with Data Sharing for the Public Good." *New York Times*. Available at: https://www.nytimes.com/2021/02/19/business/privacy-open-data-public.html.

[119] Docket No. E002/M-19-685, *In the Matter of Xcel Energy's 2019 Hosting Capacity Analysis Report, Notice of Comment Period*, October 30, 2020; Docket No. E999/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, Notice of Comment Period*, October 30, 2020.

advancing clean energy policy goals. Access to this information also increases transparency, which reduces the effects of utility monopoly control that result from the information asymmetry that naturally exists between electric utilities, and DER developers trying to supply customers' energy needs. Leveling the information playing field boosts public participation and results in more informed competition, thereby strengthening the local economy.

Benefits of Hosting Capacity Map Information for Policymakers

Hosting capacity map data can help inform public policymakers' efforts to decarbonize and modernize the electric grid, meet renewable portfolio standard (RPS) targets, and mitigate the effects of climate change. The transition to a low-carbon economy requires the electrification of vehicles and buildings, and the public infrastructure necessary to do so. The data in hosting capacity maps could help inform city planning programs to build public infrastructure in support of beneficial electrification. For example, the City of Minneapolis noted that publishing distribution grid data on hosting capacity maps would be helpful in its efforts to expand electric vehicle charging.[120]

Benefits of Hosting Capacity Map Information for Entrepreneurs and Companies

As we transition to an increasingly digital economy, data-driven innovation is at the heart of its success. Data made available on hosting capacity maps could be used by innovative entrepreneurs and companies to create new systems, processes, or products to solve a societal problem or meet a measurable need. One innovative U.S. startup layers hosting capacity map information on top of its data analytics platform, which enables DER developers to quickly screen sites across multiple locations based on hosting capacity, topography, and environmental characteristics (e.g., wetlands). Facebook applies custom algorithms to various public datasets to predict the locations of existing medium-voltage electrical distribution infrastructure (e.g., distribution lines) to help governments, non-governmental organizations (NGOs), and businesses plan future infrastructure and community development projects.[121] These are just a few examples of the innovation resulting from public access to grid data.

Benefits of Hosting Capacity Map Information for DER Developers

Hosting capacity maps are an integral tool for energy developers to identify prime locations for siting DERs on the distribution grid. Solar and storage developers rely on these maps to inform their prospects for locating projects, and ultimately to interconnect DERs to the grid. This not only benefits DER project developers, but also utilities that are looking to defer or avoid more costly traditional grid infrastructure. It may also help streamline the interconnection process since developers will have the necessary distribution system information to conduct their own preliminary project screens before formally applying for interconnection. The value of different types of hosting capacity information to developers for optimally siting DERs is shown in Table 8.

[120] *Hosting Capacity Analysis and Distribution Grid Data Security Workshop.* Docket No. E999/CI-20-800. (March 17, 2021).

[121] Facebook, Inc. "Data for Good. Electrical Distribution Grid Maps." Available at: https://dataforgood.fb.com/tools/electrical-distribution-grid-maps/.

Table 8: Benefits of Hosting Capacity Information to Developers

Hosting Capacity (HCA) Map Elements	Benefits to DER Developer
Substation location and HCA data	• Determine substation level constraints (e.g., size and voltage of transformer) • Identify equipment that may impact hosting capacity (e.g., load tap changer or regulator) • Determine approximate distance from circuit to substation
Feeder location and HCA data	• Determine feeder HCA constraints for DER load and generation • Assess if costly system upgrades are likely at a location given constraints • Identify equipment that may impact HCA (e.g., voltage supervisory reclosing)
HCA criteria violations	• Determine which violation criteria (e.g., thermal, voltage) is causing the limit, identify appropriate technical solutions to overcome constraint(s), and estimate associated costs (e.g., for system upgrade)
Substation/feeder load profiles	• Screening tool for locating DER load interconnections (e.g., storage, EV chargers) • Assess if costly system upgrades are likely at a location given constraints
DER connected and in queue	• Determine if hosting capacity is likely available to new projects

In an April 2021 HCA map survey (Appendix B) of developers in Xcel's service territory, substation data was identified as particularly important for inclusion in the HCA map given its value in evaluating substation constraints for hosting additional DERs. 70 percent of those surveyed said the substation transformer's rating (e.g., size) and available generation capacity were essential information to have. 60 percent said substation load profile and forecasted feeder peak load were of significant benefit. Other information identified as very important was local voltage, secondary conductor size, and hosting capacity criteria violations for designing projects to avoid certain system constraints. 60 percent of survey respondents indicated that sub-feeder and secondary level data were both essential for making informed decisions about siting DER. All of the survey respondents noted that Xcel's HCA map needed more infromation to be useful, and 70 percent stated that it is currently not helpful as a tool for informing their decision to complete a DER interconnection request. Specific suggestions for improving the HCA map's utility as an indicator for optimally siting DER projects included updating the map more frequently, ensuring the accuracy of its information, and revealing the feeder lines so that developers can trace the power lines from an address to a specific node where HCA data is provided.

3.6.3. Grid and Customer Security: California

Background

California had robust stakeholder discussions on balancing the benefits of making sensitive distribution grid data public, via online maps, with the grid and customer security concerns associated with doing so.

In 2010, the CPUC established the Renewable Auction Mechanism (RAM) program through Decision (D.) 10-12-048 to provide a streamlined process for California's three big IOUs[122] to procure RPS-eligible generation.[123] To provide stakeholders with greater access to information about the distribution grid in support of this program, the CPUC ordered the IOUs to publish grid data, at the substation and circuit-levels, in an online map.[124] In response, the IOUs created public PV RAM maps to make it easier for developers to identify prime locations on the grid to interconnect DERs. Figure 11 is an example of a PV RAM map and the type of grid data it provides. These maps were the precursor to California's ICA maps (e.g., hosting capacity maps). [125]

In 2018, during the process of working with the CPUC and several stakeholders to define what distribution grid data should continue being publicly shared, the California IOUs unilaterally removed the PV RAM maps from their websites. (Note: The maps were publicly accessible except for a two-month period between September and November 2018).[126] The California IOUs argued that no location-specific, distributed grid information (e.g., substations, feeders, circuits, and all related safety-and-security-sensitive data) should be made publicly available on their maps due to physical and cybersecurity concerns. Utility security officials elaborated that the information on the PV RAM maps: (1) provided a full connectivity layout of the distribution system, which would otherwise be very difficult to piece together and (2) could be used by a bad actor to commit a physical or cyber-attack on the grid.[127] They stated that malicious intent existed and that there was evidence of suspicious and unknown actors accessing the maps.[128] They also claimed that the maps were protected from public disclosure under the Critical Infrastructure Information Act of 2002[129] and that the release of the maps to the public should be done under an NDA, only giving access to third parties who demonstrated both a legitimate, specified need, and sufficient controls to protect the data from disclosure to the public.[130]

[122] PG&E, San Diego Gas & Electric (SDG&E), and Southern California Edison (SCE).

[123] PG&E. "PG&E Renewable Auction Mechanism." Available at: https://www.pge.com/en/b2b/energysupply/wholesaleelectricsuppliersolicitation/RAM2011/index.page.

[124] R.08-08-009, Renewable Portfolio Standard Program, D.10-12-048, Decision Adopting the Renewable Auction Mechanism, December 16,2010, pp. 70-72.

[125] Integration Capacity Analysis (ICA) is interchangeable with hosting capacity analysis (HCA).

[126] IREC. *Comments of The Interstate Renewable Energy Council, Inc. on Xcel Energy's 2019 Hosting Capacity Analysis*. Docket No. E002/M-19-685. (December 30, 2019) Appendix B, p. 4.

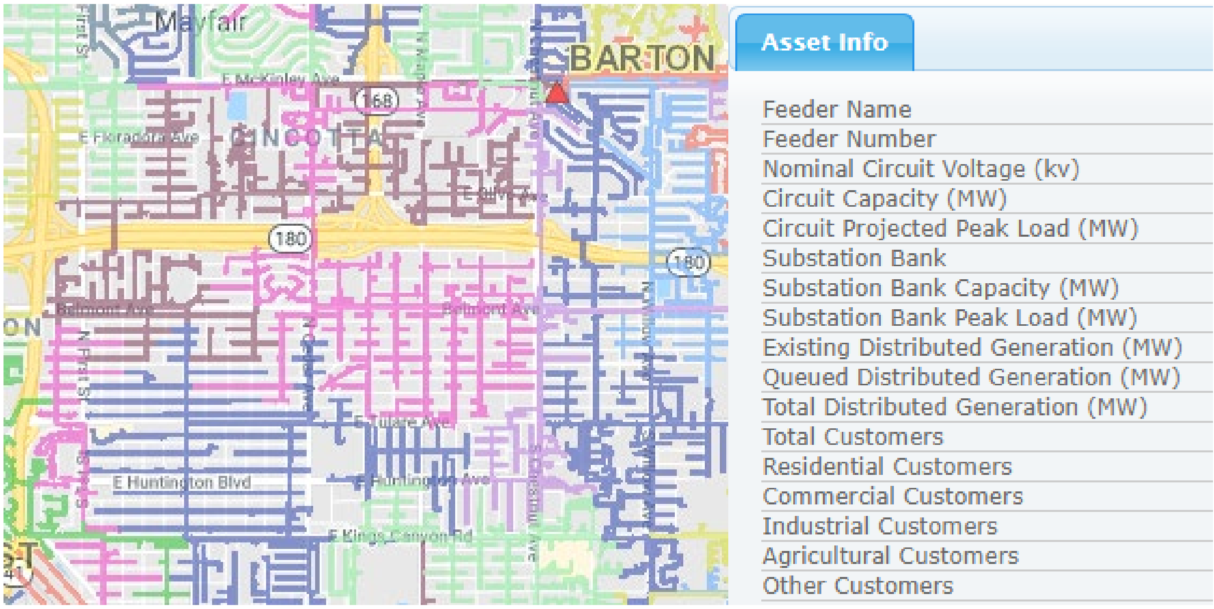
[127] Id., pp. 9-10.

[128] Id., pp. 9, 12.

[129] Id., p. 3.

[130] Id., p. 7.

Figure 11: Example California PV RAM Map and Data Fields



Asset Info

Feeder Name
Feeder Number
Nominal Circuit Voltage (kv)
Circuit Capacity (MW)
Circuit Projected Peak Load (MW)
Substation Bank
Substation Bank Capacity (MW)
Substation Bank Peak Load (MW)
Existing Distributed Generation (MW)
Queued Distributed Generation (MW)
Total Distributed Generation (MW)
Total Customers
Residential Customers
Commercial Customers
Industrial Customers
Agricultural Customers
Other Customers

Source: https://www.pge.com/en_US/for-our-business-partners/distribution-resource-planning/distribution-resource-planning-data-portal.page?ctx=large-business.

In 2018, an Administrative Law Judge ruled that the CA IOUs had to make all of their distribution system maps, as well as related analyses, publicly available through a web portal; and allow third parties to access these maps through a user registration process without having to execute an NDA. [131] He also ruled that all information that is not confidential customer data under the 15/15 aggregation standard be published, unless the utilities are able to prove that the information they wish to redact or make subject to an NDA, meets the definition of CEII that should be protected from public disclosure on confidentiality grounds.[132]

Customer Confidentiality

The CPUC adopted the 15/15 standard to require the redaction of data "in order to ensure that the released data is sufficiently aggregated to prevent the identification of [CEUD] on individuals."[133] California ruling 14-08-013 described how customer privacy should be protected on hosting capacity maps:

> Data that includes distribution load, energy usage, or demand data at a local geo-spatial level shall be anonymized and aggregated to meet

[131] CPUC*. Order, Instituting Rulemaking Regarding Policies, Procedures and Rules for Development of Distribution Resources Plans Pursuant to Public Utilities Code Section 769*. Rulemaking 14-08-013. (July 24, 2018.) p. 15.

[132] Ibid.

[133] *Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data While Protecting Privacy Of Personal Data.* (D.) 14-05-016. (May 1, 2014). p. 26-27.

> customer privacy requirements. The IOUs shall use the 15/15 Rule that the Commission established in D.97-10-031 and D.14-05-016 for data in the ICA...With respect to ICA, if the circuit level passes the 15/15 Rule but the line section does not, the IOUs shall aggregate the ICA results to the circuit level for display in the online maps and datasets. Stakeholders shall use the basic registration and log-in process to review the public DRP data with the customer privacy information redacted.[134]

As a result, California IOUs redact feeder load profile information, not the feeder itself, if it does not meet the 15/15 aggregation threshold.

Critical Infrastructure Protection and Customer Security

Initially, each IOU had a different approach to identifying and handling CEII. However, Rulemaking 14-08-013 established uniform criteria, informed by FERC and DHS definitions, for identifying data that should be classified as CEII for redaction purposes.[135] The rule also made it incumbent on the IOUs to show that the data met the redaction criteria. Each IOU that wants to redact CEII from the public-facing hosting capacity map must demonstrate that the redacted information fits within one or more of the following examples:

1. Distribution Facility necessary for crank path, black start, or capability essential to the restoration of regional electricity service that are not subject to the California Independent System Operator's operational control and/or subject to North American Electric Reliability Corporation Reliability Standard CIP-014-2 or its successors;
2. Distribution Facility that is the primary source of electrical service to a military installation essential to national security and/or emergency response services (may include certain airfields, command centers, weapons stations, emergency supply depots);
3. Distribution Facility that serves installations necessary for the provision of regional drinking water supplies and wastewater services (may include certain aqueducts, well fields, groundwater pumps, and treatment plants);
4. Distribution Facility that serves a regional public safety establishment (may include County Emergency Operations Centers; county sheriff's department and major city police department headquarters; major state and county fire service headquarters; county jails and state and federal prisons; and 911 dispatch centers);
5. Distribution Facility that serves a major transportation facility (may include International Airport, Mega Seaport, other air traffic control center, and international border crossing);

[134] CPUC. *Order, Instituting Rulemaking Regarding Policies, Procedures and Rules for Development of Distribution Resources Plans Pursuant to Public Utilities Code Section 769*. Rulemaking 14-08-013. (July 24, 2018.) pp. 11-12.

[135] Id., p. 20.

6. Distribution Facility that serves as a Level 1 Trauma Center as designated by the Office of Statewide Health Planning and Development; and
7. Distribution Facility that serves over 60,000 meters.[136]

To date, none of the California IOUs have taken these steps. Following FERC's approach, the ruling also adopted a protocol for interested stakeholders to get access to desired CEII by entering an NDA with the utility.[137] More specifically, stakeholders seeking to gain access to CEII must file a motion that explains what information they need, how they plan on using it, and why it is not available from a different source. If they are approved, they may then sign an NDA with the utility to access the requested information.

3.6.4. Grid and Customer Security: Minnesota

Background

The Commission's July 31, 2020 Order in Docket No. E002/M-19-685 (the 2020 Order)[138] required Xcel to further discuss grid and customer security issues related to the public display or access to grid data, including distribution grid mapping, aggregated load data, and critical infrastructure in a proceeding[139] that includes additional parties, experts, and utilities.[140] It also required Xcel to separately evaluate and justify each privacy and security concern and to provide a full description and specific basis for withholding any information in its 2020 HCA.[141]

Public Display of Distribution Lines on HCA Map

In Pt. 12 of the 2020 Order, the Commission directed Xcel, to the extent practicable, to show the actual locations of distribution system lines instead of broad blocks of color on the HCA map. Figure 12 provides an example of Xcel's HCA map with blurred grid lines providing a "heat map" presentation.

[136] Id., pp. 20-21.

[137] Id., p. 21.

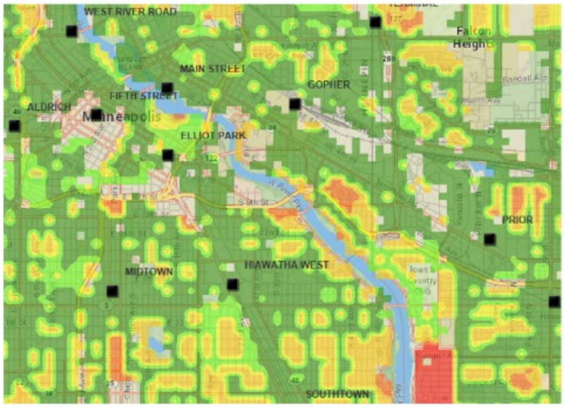
[138] *Order Accepting Report and Setting Further Requirements*. Docket No. E002/M-19-685. (July 31, 2020).

[139] The Commission initiated the proceeding on October 30, 2020, issuing a Notice of Comment Period in Docket Nos. E002/M-19-685 (Xcel's 2019 HCA proceeding) and E999/CI-20-800.

[140] Xcel Energy. *Distribution System–Hosting Capacity Analysis Report (HCA Report)*. Docket No. E002/M-20. (November 2, 2020). Attachment E, p. 1.

[141] Ibid.

Figure 12: Example of Xcel Energy HCA Map Results



Source: 2020 HCA Report, p.9.

While Xcel provides sub-feeder (e.g., line segment) level hosting capacity results, which vary at different points along the feeder, the map cannot be used to specifically identify the locations of the feeder line-segments for which those results are provided. Local energy developers frequently request that Xcel show the exact feeder lines on its map to help them more easily identify suitable DER interconnection locations. However, Xcel continues to state that doing so would risk grid security and customer confidentiality.[142] Xcel argues that an unblurred map would clearly lay out the electrical connectivity configuration of its distribution network, providing a bad actor with the information needed to plan an attack for maximum impact. Xcel further explains that revealing this information would allow a bad actor to identify which lines extend to specific substations and/or critical customer facilities and to determine the location of the system's major loads, rendering the distribution grid unnecessarily vulnerable. Xcel states that it does not intend to make it "easy" for a bad actor to obtain this type of information and claims that not publicly providing the detailed connectivity of its distribution system mitigates the increased threat of cyber and physical attacks.[143]

Customer Confidentiality

Xcel applies the 15/15 aggregation standard to determine if CEUD is sufficiently aggregated to be released. Xcel marks information that falls under the 15/15 threshold as protected data (e.g., Trade Secret information) and does not make it public.[144] Xcel excluded the feeders that did not meet its 15/15 aggregation threshold from its HCA map but included them in the HCA tabular spreadsheet with the rationale that publicly disclosing these feeders on the map would make it easier to identify actual customer connections and could compromise customer confidentiality.[145]

[142] Xcel Energy. 2020. HCA Report. Attachment A, p. 19.

[143] Id., Attachment E, p. 6.

[144] Id., p. 4.

[145] Id., p. 5.

Peak Substation Transformer and Feeder Load Data

The Commission's 2018 HCA Order required Xcel to "provide hosting capacity data by substation and feeder," including "peak load," in its public-facing hosting capacity map, "except to the extent that publicly disclosing this data would violate specific data privacy requirements or pose a significant security risk to Xcel's system or its customers."[146]

Xcel does not publicly provide the peak substation transformer load or peak feeder load data in its HCA map or table. Xcel states that load information is security information and contends that publishing peak load or maximum capacity information for its distribution system facilities could aid bad actors in planning an attack for maximum impact and disruption.[147] Xcel elaborates that such information can help adversaries plan and execute load manipulation attacks in ways that could lead to equipment damage and other disruptive effects.[148] Xcel adds that the data could also compromise the privacy or confidentiality interests of large or critical infrastructure customers.[149] Xcel legally justifies withholding this information noting that it is classified as "security " and "Trade Secret" information.[150]

Critical Infrastructure Protection and Customer Security

To align with protecting critical infrastructure sectors, as identified by DHS, Xcel identified customers and their associated feeder(s) that, in its judgement, would warrant protection based on the criticality of the loads they serve. These critical customers fell into the following categories:

- Critical Energy Infrastructure (similar to DHS Energy sector);
- Critical Hospitals - Level 1 or 2 Trauma Centers (similar to DHS Healthcare and Public Health sector);
- Critical Data Centers (similar to DHS Communications and Information Technology sectors); and
- Critical Public Gathering Center (similar to DHS Commercial Facilities sector).[151]

Xcel excluded a feeder from its HCA map when it was connected to critical infrastructure or did not meet its 15/15 aggregation threshold. Xcel excluded 115 out of a total of 1,050 feeders from its map.[152] However, Xcel provided data for all feeders in the HCA tabular spreadsheet. Xcel notes that the spreadsheet does not identify which feeders fall under the critical infrastructure sectors categories or

[146] *Order Accepting Study and Setting Further Requirements.* Dkt. E-002/M-18-684 (Aug. 15, 2019). Paragraphs 2.B, 2.C.

[147] Xcel Energy. 2020. HCA Report. Attachment E, p. 5.

[148] Xcel Energy. *Comments–Response to Notice Distribution Grid and Customer Security Docket Nos.E002/M-19-685 and E999/Ci-20-800* , Docket Nos. E002/M-19-685 and E999/CI-20-800, (January 21, 2021). Attachment B, p 3.

[149] Ibid.

[150] Xcel Energy. 2020. HCA Report. Attachment E, p. 5.

[151] Id., p. 4.

[152] Id., p. 3.

which are subject to privacy concerns, to not make it apparent for a bad actor to target sensitive feeders.[153]

3.6.5. *Discussion of Grid and Customer Security Concerns and Public Benefits*

Overview

Xcel states that there is growing recognition that the vulnerabilities of the energy sector are of particular concern to national security and that the electric grid is both highly vulnerable to attack and attractive to potential adversaries due to the dependence of all other critical infrastructure on it.[154] During the first HCA and Distribution Grid Data Security workshop, Xcel mentioned that it is constantly assessing threats and upgrading its defensive capabilities to secure the grid but noted that attackers only have to be successful once, while the utility has to be successful every time. Xcel further states that there are risks associated with access to certain distribution grid data whether it is provided publicly or with protections.[155]

While the likelihood and the scale of potential threats to the distribution systems are unclear, and the risk of disclosure of specific grid data may be unknown, it is not enough to state that risk exists. There is no disagreement that there is always some level of risk involved with sharing sensitive information, but attempting to quantify the level of risk and weigh it against the benefits of making certain grid data available to the public is essential. Xcel is generally aligned with this idea, and proposed a tiered-access approach to the provision of distribution grid data, which would enable appropriate access to relevant information while taking steps to reasonably maintain the security of the grid.[156] The following sections discuss some of the grid and customer security concerns associated with information that is currently withheld from Xcel's hosting capacity map as well as the potential benefits that this information could provide to the public.

Distribution Lines Should be Publicly Displayed on HCA Map

Xcel claims that an unblurred map would clearly lay out the electrical connectivity configuration of its distribution network, providing a bad actor with the information needed to plan an attack for maximum impact. Xcel maintains that revealing this information would also jeopardize customer security and confidentiality, by enabling bad actors to identify which lines extend to critical customer facilities, and to determine the locations of the system's major loads. Xcel also states that it does not want to make it "easy" for a bad actor to obtain this type of information, and claims that not publicly providing the

[153] Ibid.

[154] Xcel Energy. 2020. HCA Report. Attachment E, p. 1.

[155] Xcel Energy Comments, January 2021. p. 13.

[156] Id., p. 4.

detailed connectivity of its distribution system mitigates the increased threat of cyber and physical attacks.[157]

While it may be more difficult for a bad actor to piece together a map of the electrical connectivity of the distribution system than if Xcel provided it, that does not make it impossible to do so. There are publicly available resources, like Google Earth and Maps, which can assist in this task. Moreover, obscurity is not security. A less well-known target may appear more secure than it is. This is evident from the growing list of recent cybersecurity data breaches of U.S. companies. In fact, believing that concealed data is inherently more secure may provide a false sense of security and reduce a company's sense of urgency for bolstering its cybersecurity defenses. Furthermore, providing distribution system connectivity information does not necessarily lead to, or mitigate, physical or cyber threats from a bad actor, but strengthening the grid's physical and cybersecurity defenses, and enhancing the grid's reliability and resiliency does.

The following sections further elaborate on these comments.

Various Tools Available to Map Distribution System Infrastructure

There are a variety of tools available to help map the locations of distribution system facilities and an attacker could use a combination of these tools to launch an attack. For example, an attacker could easily identify substation locations in Minnesota using the publicly available geospatial substation data on the DHS Homeland Infrastructure Foundation-Level Data website[158] and use it with satellite imagery from Google Earth to trace the path of distribution lines to a substation. Google Maps can also be used to identify the physical locations of substations. There are also private companies such as Kevala Analytics, which uses its Grid Assessor[159] software to identify distribution system infrastructure, including substations and feeders, across the United States to help developers quickly find ideal project locations for DERs. Facebook created a predictive model using publicly available datasets, including NASA satellite imagery, to predict the locations of distribution lines.[160] Facebook also provides information on how to use the model and the code is open source. However, it is not necessary for a bad actor to use an online geospatial tool or analytical model. S/he could simply locate a substation and/or a critical customer facility, like a hospital, and visually trace the power lines emanating in either direction to plan an attack. The National Research Council (NRC) further highlights the fact that sensitive grid information is already in the public domain, stating:

> High-value choke points, those facilities which, if destroyed, will significantly degrade power systems capabilities, are easily located either on the ground or

[157] Xcel Energy. 2020. HCA Report. Attachment E, p. 6.

[158] Department of Homeland Security (DHS). "Homeland Infrastructure Foundation-Level Data." Available at: https://hifld-geoplatform.opendata.arcgis.com/.

[159] Kevala Analytics. "Grid Assessor." Available at: https://kevalaanalytics.com/grid-assessor/.

[160] Facebook, Inc. "Data for Good, Electrical Distribution Grid Maps." Available at: https://dataforgood.fb.com/tools/electrical-distribution-grid-maps/.

> from system maps. Detailed maps of the U.S. power system were once readily available in the public domain and on the Internet. Despite attempts to control access to such maps, they can still be easily obtained. Commercially available satellite data, as well as direct observation on the ground, can also be used to readily update and confirm system map information for potential attackers.[161]

Thus, rather than focusing on not providing access to information about the locations of feeders and substations, which is likely already in the public domain or can be constructed, the utility should focus on bolstering its physical and cybersecurity defenses in case of an attack, and on enhancing the reliability and resiliency of the grid in general. Some ways to accomplish this are to harden distribution infrastructure (e.g., feeders and substations), underground feeder lines, improve surveillance equipment, and improve planning on how to repair and restore facilities in case of an attack.[162] In a report for the Department of Defense, the RAND Corporation, a research organization that helps develop public policy solutions to address security risks, highlighted the importance of improving the reliability and resiliency of the grid to deter would-be adversaries from attacking or "deterrence by denial."[163] RAND states that knowledge of such investments to strengthen the grid might have a deterring effect by reducing or removing the perceived benefits that an adversary associates with an attack.[164] RAND further notes, that "in addition to providing value through deterrence of adversary attacks (cyber-related or otherwise), investments in measures aimed at limiting or denying adversary success serve a broader purpose of improving mission resilience to power disruptions resulting from natural disasters, operator error, or equipment failures."[165]

<u>Hosting Capacity Maps Generally Show Feeder Lines</u>

Typically, publicly available hosting capacity maps of U.S. electric utilities leading in this space show the distribution system feeder lines to assist developers in locating optimal sites for DER deployment. HCA maps should be sufficiently detailed to be useful to stakeholders. Xcel provides HCA results at the sub-feeder level. Other U.S. electric utilities leading in the development of HCA maps are also providing HCA results at the sub-feeder level. This is a granular level of distribution system detail, which is useful for DER developers who want to determine the part (e.g., line segment) of a feeder with the most hosting capacity. In Xcel's HCA map, this granularity is lost because the actual feeders are blurred.

High voltage transmission lines are generally less resilient to attack than distribution lines due to distribution circuit redundancy (e.g., "auto-loop" radial grids or network grids) which helps to quickly

[161] National Research Council. 2012. *Terrorism and the Electric Power Delivery System.* pp. 32-33.

[162] Id., pp. 34-36.

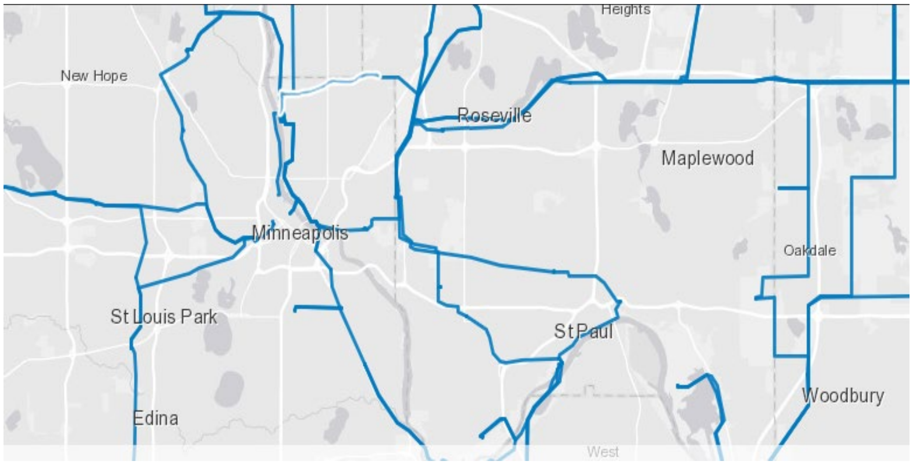
[163] Narayanan, Anu, Jonathan William Welburn, Benjamin M. Miller, Sheng Tao Li, and Aaron Clark-Ginsberg. 2020. *Deterring Attacks Against the Power Grid: Two Approaches for the U.S. Department of Defense.* RAND Corporation. p. x. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3187/RAND_RR3187.pdf.

[164] Ibid.

[165] Ibid.

isolate a fault or provide redundant sources of backup power in the case of failures on the grid. Yet, despite the inherent, and generally higher, vulnerabilities in transmission lines and their potential to cause widespread outages when down, the DHS provides public, searchable, geospatial maps showing the locations and voltages of transmission lines across the United States in support of community preparedness, resiliency, and research.[166] Figure 13 provides an example of the DHS transmission line map. If the DHS, which has identified energy as a critical infrastructure sector whose assets and networks are vital to U.S. national security, publicly displays the entire country's electric power lines, it also seems reasonable that a local electric utility should show the distribution lines on its HCA map for the public good.

Figure 13: DHS, Homeland Infrastructure Foundation-Level Data Transmission Lines



Source: DHS, Homeland Infrastructure Foundation-Level Data. https://hifld-geoplatform.opendata.arcgis.com/

Distribution Systems Are Lower Value Targets than Transmission Systems

While the likelihood and the scale of potential threats to distribution systems are unclear, to date there have been no reported terrorist attacks on distribution system infrastructure in the United States. This could be due, in part, to the fact that distribution systems are lower value targets relative to the transmission (e.g., bulk power) system. A 2018 CPUC staff report noted that distribution assets are not attractive, high-value targets and that the vast majority of "physical security" incidents on the distribution system consist of minor property crimes including vandalism, copper theft, and trespassing.[167] Moreover, distribution system resiliency and redundancy to ensure reliability make it a lower value target. The CPUC report noted that distribution systems that incorporate automation can often isolate a problem and restore service for affected customers in a matter of seconds or minutes.[168]

[166] DHS. "Homeland Infrastructure Foundation-Level Data." Available at: https://hifld-geoplatform.opendata.arcgis.com/.

[167] CPUC. 2018. *Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699.* pp. 38-39.

[168] Ibid.

It further explains that if a distribution substation transformer were targeted by a physical attack, operators typically could respond by remote-grid-switching to bypass the affected substation, and reliability response teams could dispatch replacement parts such as distribution transformers, often within 24 hours.[169]

In contrast, there is general agreement among security planners that key high-voltage substations are the most worrisome terrorist targets within the power transmission system.[170] They are difficult to protect and replace. Additionally, transmission lines can temporarily be disabled by fairly simple means such as shooting insulators on a tower.[171] On some transmission lines, taking out a tower can cause a domino effect, resulting in a cascade collapse of several adjacent towers, and taking out a tower where two lines cross, can disable both circuits simultaneously.[172]

Significant Benefit to Developers of Knowing Locations of Distribution Lines

There is a considerable benefit to developers knowing the locations of distribution lines on Xcel's HCA map to identify potentially suitable sites for deploying DERs. During the second HCA and Distribution Grid Data Security workshop, Xcel remarked that it frequently gets requests from DER developers to reveal the locations of its feeder lines. This is a clear indication of the value to, and need for, DER developers to have this information. Xcel suggests striking a balance between the need to share sensitive information with the need to protect it[173] and supports "a tiered-access approach to the provision of distribution grid data, based on its necessity and value to achieving a defined and specific public purpose."[174] While this sounds reasonable at the surface, it is important to dig deeper into what Xcel means by this statement. Greater clarity is provided in Xcel's discussion of integrating its Pre-Application Report with the HCA. Xcel states: "the Pre-Application Data Report requires the requestor to sign a Non-Disclosure Agreement, which is necessary because the Company maintains some of the data provided as non-public. This would not change with an integrated process/tool."[175]

A tiered-access approach that requires an NDA to view the distribution lines on the HCA map is unduly burdensome. This would essentially make the entire HCA map confidential instead of specific pieces of grid data (e.g., feeder peak load). In general, HCA maps are created to provide stakeholders with greater access to information about the distribution grid with the goals of promoting competition, decreasing the costs of achieving RPS policy objectives, and increasing transparency so that DER developers, and not just the electric utility, can make informed decisions about how best to site DERs on the grid.

[169] Ibid.

[170] National Research Council. 2012. *Terrorism and the Electric Power Delivery System.* p. 33.

[171] Ibid.

[172] Ibid.

[173] Xcel Energy Comments, January 2021, p. 12.

[174] Id., p. 4.

[175] Xcel Energy. 2020. HCA Report. Attachment F, p. 16.

Knowing the locations of feeder lines is a fundamental component of a useful HCA map. Over-classifying essential HCA map information, like the locations of feeder lines, creates a significant barrier to developers for obtaining the requisite information needed to conduct quick, initial screens for locating preferred interconnection points. These barriers to information about the distribution grid would increase costs for developers and customers and decrease the efficiency of the interconnection process.[176] Borrego Solar, a leading U.S. commercial-scale solar and storage project developer, amplified this point. It noted that the Borrego Solar development team frequently uses HCA maps during the early stages of project development to identify optimal grid locations for siting its systems.[177] The company explained that requiring an NDA to access this information would "hamstring" the development process by adding layers of bureaucracy which would "significantly slow down" its efforts to develop large-scale solar and storage projects.[178] It elaborated that an NDA would require multiple parties within the company to sign it to utilize the information, and by extension, its customers, who would have to sign as well for the company to be able to communicate information in the map applicable to the customer's project.[179] The NDA would also create liability for disclosure or misuse of the data, and an inadvertent disclosure by a small solar company to a customer over the course of its interactions while developing a project could be legally and financially devastating.

Customer Confidentiality

Xcel applies the 15/15 aggregation standard to determine if CEUD is sufficiently aggregated to be released and uses this aggregation threshold to exclude feeders from its HCA map. Other states like Colorado and California also use the 15/15 standard to protect CEUD.[180] However, the issue is not using the 15/15 standard to protect CEUD but rather its application to Xcel's HCA map, where it is used to remove the feeder, and all corresponding HCA data, even if it is unrelated to a customer's energy use. Xcel justifies redacting the feeder when it violates the 15/15 threshold stating that "showing this information on the heat map would make it easier to identify actual customer connections and risk erosion of customer confidentiality protection."[181] Xcel explains that low density feeders serving fewer than 15 premises, which is the same threshold it applies to requests for aggregated CEUD feeders, may provide insights into those customer locations that could compromise customer confidentiality and/or customer energy security.[182] The Interstate Renewable Energy Council (IREC), a non-profit organization

[176] *Response of the Joint Parties to Joint Petition of PG&E, SDG&E and SCE for Modification of D.10-12-048 and Resolution E.4414 to Protect the Physical Security and Cybersecurity of Electric Distribution and Transmission Facilities,* Rulemaking 08-08-009. (January 9, 2019). p. 16.

[177] Declaration of Rachel Bird on behalf of Borrego Solar Systems, Inc., Rulemaking 08-08-009, D.10-12-048 and Resolution E.4414. Appendix B.

[178] Ibid.

[179] Ibid.

[180] *Comments of the Interstate Renewable Energy Council, Inc. (IREC) on Xcel's 2020 Hosting Capacity Analysis.* Docket No. E002/M-20-812. (April 7, 2021). p. 21.

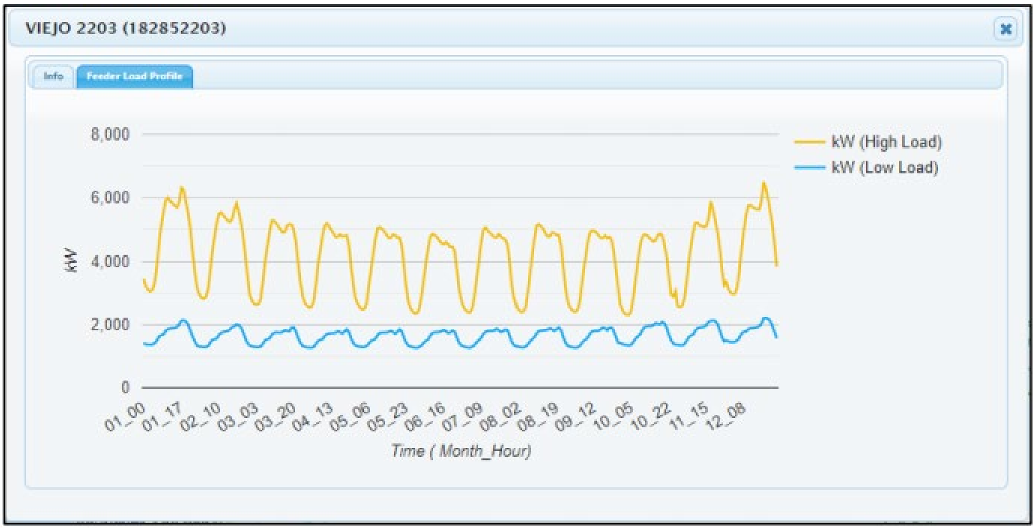
[181] Xcel Energy. 2020. HCA Report. Attachment E, p. 5.

[182] Ibid.

working to expand consumer access to clean energy, stated that "using the 15/15 standard to redact data that is not in any way related to a customer's energy use is an incorrect application of the standard" and noted that "protecting customer privacy is not a valid rationale for withholding data that has nothing to do with customer energy use."[183] IREC stated that the purpose of protecting CEUD is to prevent third parties from accessing the energy use patterns of a specific customer and not to prevent the identification of the feeder that the customer connects to.[184] IREC explained that knowing that a feeder has fewer than 15 customers or one customer with more than 15 percent of the load does not reveal the customer's data.[185] Participants in Xcel's September 2020 HCA stakeholder workshop also requested that the HCA map include all the basic distribution system data, as long as it does not violate the 15/15 rule regarding customer data privacy.[186]

California utilities also apply the 15/15 standard to protect customer load information in their HCA maps; when a feeder or substation violates this standard, the load profile data, which includes minimum and peak load, is redacted. However, the exact location of the feeder lines are published on the map and all non-load (e.g., non-CEUD) data is published. Figure 14 provides an example of how one California IOU displays a feeder's load profile in its HCA map.

Figure 14: PG&E Feeder Load Profile



Source: PG&E ICA Map User Guide, p. 9, https://www.pge.com/b2b/distribution-resource-planning/downloads/integration-capacity/PGE_ICA_Map_User_Guide.pdf

[183] IREC Comments on Xcel's 2020 Hosting Capacity Analysis. p. 22.

[184] IREC Comments on Xcel's 2019 Hosting Capacity Analysis. p. 21.

[185] Ibid.

[186] Xcel Energy. 2020. HCA Report. Attachment E, p. 2.

It is important not to conflate the issues of customer confidentiality and grid security. If a feeder violates the 15/15 standard, the appropriate measure to protect a customer's privacy is to remove CEUD. Customer load data directly relates to CEUD. Thus, it would be appropriate to redact different types of load information like peak load and absolute minimum load from the feeder. However, the feeder itself should not be redacted based on a violation of the 15/15 standard unless it is dedicated to a single, large energy consuming customer (e.g., skyscraper), which could then reveal its energy use patterns. Generally, this would represent a spot network, which is a small network grid that is implemented for a single, large energy user. However, Xcel's HCA excludes network feeders so this should not be an issue.[187] Furthermore, if the feeder is connected to a critical customer or infrastructure, as defined by Xcel's critical infrastructure categories, then that feeder should be redacted. One northeast IOU[188] follows a similar approach, only redacting feeders from its HCA map which are connected to critical customers or that serve a dedicated customer. The utility noted that it does not redact information that could easily be identified by simple visual surveillance (e.g., walking around the block and examining distribution lines). Finally, HCA maps which reveal feeder lines do not show locations of any individual customer or service connections (e.g., how they are electrically fed from equipment). For example, to protect customer privacy on its hosting capacity map, Pepco notes that distribution circuits are represented as a colored line without any equipment shown. These colored lines extend to premises which are just depicted as gray blocks.[189]

In summary, given stakeholders' desire to have HCA results and non-CEUD information made available on the HCA map when a feeder does not meet the 15/15 standard, how other utilities appropriately balance providing HCA results and feeder locations while not revealing customer privacy (e.g., CEUD) on their maps when similarly applying the 15/15 standard, and Xcel's prerogative to redact feeders from its map that violate CEII and critical customer group screens, the Commission should allow Xcel to only redact load data, and require it to publish all other HCA data on its map when the application of the 15/15 standard calls for the redaction of CEUD to protect customer privacy.

Peak Substation Transformer and Feeder Load Data

Xcel does not publicly provide the peak substation transformer load or peak feeder load data in its HCA map or table. It claims that publicly publishing peak load or maximum capacity information for its distribution system facilities could aid bad actors in planning an attack for maximum impact and disruption.[190] Xcel noted that the data could also compromise the privacy or confidentiality interests of large or critical infrastructure customers, and noted that while it can mitigate customer privacy and

[187] Id., p. 3.

[188] Synapse communication, April 7, 2021.

[189] Steffel, Steve. 2020. *Hosting Capacity - Lessons Learned*. Pepco Holdings. p. 24. Available at: https://www.oregon.gov/puc/utilities/Documents/DSP-Hosting-Capacity-SSteffel.pdf.

[190] Xcel Energy. 2020. HCA Report. Attachment E, p. 3.

confidentiality concerns by applying the 15/15 standard, customer and grid security concerns remain.[191] Xcel also noted that developers who attended its 2019 Workshop, or participated in the post-workshop survey, did not state that peak load was a necessary or useful piece of information, even when prompted.[192] IREC countered that Xcel did not survey a diverse enough group of developers to make that assertion and argued that customers and developers need peak load data to strategically locate DERs that are load sources, such as electric vehicles and energy storage.[193] IREC added that a load profile could be used by customers with DERs (e.g., energy storage) looking to provide the valuable service of peak load shaving (e.g., reducing peak load hours).[194]

Given competing claims about the value of this information to DER developers, and the risks associated with publicly providing it, a Risk-Benefit Framework, as proposed in Section 4.2, should be applied to help determine whether substation and feeder peak loads should be publicly provided as requested by the Commission. This framework will help to weigh the need for this information by a diverse group of DER developers (e.g., storage, electric vehicle, and solar) against the customer and grid security risks of publishing it.

Critical Infrastructure Protection and Customer Security

Xcel excluded a feeder from its HCA map when it was connected to critical infrastructure as defined according to its five critical infrastructure categories.[195] Given the importance of protecting critical infrastructure and customer groups, this approach seems reasonable. However, to increase transparency with the public, Xcel should specify in greater detail the types of customers that may fall into any other categories of critical, grid-dependent customers. During the second HCA and Distribution Grid Data Security workshop, Xcel noted that other types of critical customers could include airports, for example. However, Xcel should make this list explicit. It is clear what Xcel means by Critical Hospitals (Level 1 or 2 Trauma Centers), Critical Data Centers, and Critical Public Gathering Centers (e.g., stadiums); and while slightly less clear, in the case of the Critical Energy Infrastructure category, it is still understandable.

Like California, Xcel should also create a transparent process for how third parties can access CEII, on a “need-to-know” basis, with appropriate protections (e.g., NDA) in place.

3.7. HCA Map Integration with Pre-Application Data Report

[191] Ibid.

[192] Ibid.

[193] IREC Comments on Xcel’s 2019 Hosting Capacity Analysis. p. 23.

[194] Ibid.

[195] Xcel Energy. 2020. HCA Report. Attachment E, p. 4.

3.7.1. Background on Pre-Application Report Integration

Xcel stated that one of the most common stakeholder requests was integration of the information contained in the pre-application data report with the HCA map for potential interconnection customers. Together, these two items provide a baseline determination of whether DER interconnection in a particular location is viable. According to Xcel, although there would be clear benefits to integrating pre-application data with the HCA map, there would also be significant costs and technical barriers. For example, additional querying functionality would need to be added to the map, and some information would need to be excluded for security and privacy reasons.[196] In the 2020 HCA report, Xcel estimated that fully integrating the Pre-Application Report with the HCA would take one year and cost between $600,000 and $1.2 million.[197] The Commission directed Xcel to continue working with stakeholders to identify opportunities to integrate the HCA and the Minnesota DER Interconnection Process (MN DIP) Pre-Application Report in future iterations of the HCA.

3.7.2. Pre-Application Report Confidentiality

Xcel Energy, Minnesota Power, and Otter Tail Power require that interested parties sign a confidentiality agreement prior to receiving a Pre-Application Report. The Minnesota Power and Otter Tail Power's Pre-Application Request Forms include the following text:

> I understand that the confidentiality provisions of MN DIP Section 5.9 apply to the contents of the Pre-Application Report...Each Party shall hold in confidence and shall not disclose Confidential Information, to any person (except employees, officers, representatives and agents, who agree to be bound by this section). Confidential Information shall be clearly marked as such on each page or otherwise affirmatively identified. … Each Party shall employ at least the same standard of care to protect Confidential Information obtained from the other Party as it employs to protect its own Confidential Information. … Each Party is entitled to equitable relief, by injunction or otherwise, to enforce its rights under this provision to prevent the release of Confidential Information without bond or proof of damages, and may seek other remedies available at law or in equity for breach of this provision.

Xcel has the same MIN DIP confidentiality provisions embedded in its tariff[198] and on its Pre-Application Request Form it states: "Xcel Energy will require that you sign an NDA prior to receiving Pre-Application Data Report - you will receive the NDA after we receive this form and associated fees. Note that a

[196] *In the Matter of Xcel's 2019 HCA Report. Order Accepting Report and Setting Further Requirement*. Docket No. E-002/M-19-685. (July 31, 2020).

[197] Xcel Energy. 2020. HCA Report. Attachment F, p. 16.

[198] Northern States Power Company. *Minnesota Electric Rate Book – MPUC No. 2. Distributed Resources.* Section No. 10-212. Available at: https://www.xcelenergy.com/staticfiles/xe-responsive/Working%20With%20Us/Renewable%20Developers/Me_Section_10.pdf.

separate NDA will be required for each location screened." [199] Xcel also states that the data listed below are:

> Confidential Information, are non-public, and are subject to the Confidentiality provisions in MN DIP section 5.9, as well as the confidentiality provision contained in the signed Pre-Application Report Request Form:
>
> - Transformer Rating (MVA)
> - Transformer Peak Loading (MVA)
> - Available Transformer Generation Capacity
> - Feeder Rating at head end (MVA)
> - Feeder Peak Loading at head end (MVA)
> - Available Feeder Generation Capacity at the head end
> - Protective devices and regulators between site and substation
> - Conductor(s) between sites and substation
> - Other existing or known constraints, including, but not limited to, short circuit interrupting capacity issues, power quality or stability issues, capacity constraints.

Dakota Electric Association currently does not have any confidentiality requirements that Pre-Application Report requestors must sign but indicated that it may do so in the future. [200]

To date, Dakota Electric, Minnesota Power, and Otter Tail Power have received few Pre-Application Request Forms. Dakota Electric received three Pre-Application Request Forms since it began offering them.[201] Minnesota Power processed two Pre-Application Reports in 2020 and eight so far as of April 2021.[202] Otter Tail Power has not had to process a Pre-Application Report.[203] However, Xcel received and processed 368 Pre-Application Report requests in 2020.[204]

3.7.3. Value to Stakeholders of Integrating Pre-application Report with HCA

On September 10, 2020, Xcel held a stakeholder workshop exploring how the HCA could be integrated with the Pre-Application Report. Participants stated that they use the Pre-Application Report to find suitable project sites, to identity potential landowners, and to obtain more detailed information about relevant feeders and substations of interest, among other applications. Participants also noted that the

[199] Xcel Energy. "Pre-Application Data Request." Available at: https://www.xcelenergy.com/staticfiles/xe-responsive/Working%20With%20Us/Renewable%20Developers/Pre-Application-Data-Request.xlsx.

[200] Synapse email correspondence with Dakota Electric Association on April 12, 2021.

[201] Synapse email correspondence with Dakota Electric Association on April 13, 2021.

[202] Synapse email correspondence with Minnesota Power on April 13, 2021.

[203] Synapse email correspondence with Otter Tail Power on April 12, 2021.

[204] *Xcel Energy Compliance Filing – 2020 Interconnection – Corrected Generic Standards for Interconnection and Operation of Distributed Generation Facilities*, Docket Nos. E999/CI-01-1023 and E999/CI-16-521, (March 17, 2021), p. 7.

accuracy of the Pre-Application Report was the top priority, followed by a fast turnaround time.[205] One participant stated that the Pre-Application Report should be available quickly and that the current turnaround time of 15 business days is too long.[206] Participants also noted that the HCA map should provide the total queued and connected generation, at both the substation and feeder levels, to help developers better understand how an application may potentially be impacted by substation or feeder queue backlogs or substation capacity constraints.[207]

3.7.4. Comparison of Pre-Application Report Information with HCA

Section 1.4.2 of the MN DIP requires the Minnesota electric utilities to "identify the substation/area bus, bank or circuit likely to serve the proposed Point of Common Coupling" in their Pre-Application Reports.[208] Xcel provides most of the information listed in its Pre-Application Report in its HCA in either map and/or tabular format. Table 9 lists all the data elements in Xcel's Pre-Application Report which are not included in the HCA in either map and/or tabular format, and Xcel's rationale for not doing so.[209] Table A-1 provides a complete list of Xcel's pre-application data elements and whether they are included in the HCA.

The Pre-Application Report information that is not included in the HCA is currently excluded for either privacy and security reasons, technical barriers, or both.

Table 9: Comparison of Pre-Application Report data elements with HCA

Pre-application Data Element	Information Available on Map	Information Available in Tabular Format	Notes
Transformer Rating	No	No	Privacy/Security Concerns.
Transformer Peak	No	No	Privacy/Security Concerns.
Transformer Gen Capacity	No	No	Security concerns and significant technology requirement. Equation would need to be implemented within the map or prior to map creation.

[205] Xcel Energy. 2020. HCA Report. Attachment D2, p. 12.

[206] Id., 13.

[207] Id., 4.

[208] MPUC. *Minnesota Distributed Energy Resource Interconnection Process (MN DIP) Version 2.3.* p.5. Available at: https://mn.gov/puc/assets/MN%20DIP_tcm14-431769.pdf.

[209] *Comments of the Interstate Renewable Energy Council, Inc. on Xcel Energy's 2019 Hosting Capacity Analysis.* Docket No. E002/M-20-812. (December 30, 2019). Attachment A: Xcel Energy's Response to IREC Information Requests Nos. 1-6. Dec. 17, 2019.

Pre-application Data Element	Information Available on Map	Information Available in Tabular Format	Notes
Distance from site (PCC) to substation	No	No	Significant technology requirement. Query function would need to be built into Hosting Capacity Map.
Feeder Rating	No	No	Privacy/Security Concerns.
Feeder Peak	No	No	Privacy/Security Concerns.
Feeder Gen Capacity	No	No	Security concerns and significant technology requirement. Equation would need to be implemented within the map or prior to map creation.
Distance to 3 phase circuit	No	No	Significant technology requirement. Query function would need to be built into Hosting Capacity Map.
Protective devices and regulators between site and substation	No	No	Security concerns and significant technology requirement. Query function would need to be built into Hosting Capacity Map.
Conductor between site and substation	No	No	Security concerns and significant technology requirement. Query function would need to be built into Hosting Capacity Map.

Source: Xcel Energy's Response to IREC Information Requests Nos. 1-6. Dec. 17, 2019.

3.7.5. Recommendation on Integrating Pre-Application Report with HCA

During Xcel's workshop on integrating the HCA with the interconnection process, participants commented that the current interconnection process (MN DIP) was not working due to feeders and substation transformers that had capacity constraints, and long DER project queues (e.g., many projects "On Hold").[210] Xcel acknowledged that there have been problems with the MN DIP process; it stated that it is committed to making sure the process works better and is implementing process improvements.[211] One way for Xcel to help streamline the MN DIP process and address some of these issues is to integrate specific data fields from the Pre-Application Report into the HCA.

[210] Xcel Energy. 2020. HCA Report. Attachment D2, p. 3.

[211] Ibid.

Filing a Pre-Application Report adds time and expense to an initial DER project screen. There is currently not a central data repository at Xcel for all the information needed to complete a Pre-Application Report, which adds to the complexity and time required to fulfill these requests.[212] Furthermore, Xcel's Pre-Application Report states that data provided may become outdated and not useful at the time of submission of the complete Interconnection Request. To acquire additional information on various substations and circuits across multiple locations in the service territory using a Pre-Application Report would cost $300 per interconnection address. Therefore, if the HCA map were to include the Pre-Application Report data, especially the substation and feeder level generation capacity, this would make it quicker for developers to screen for beneficial DER sites and less expensive for them to apply for interconnection. It would also help to increase the overall efficiency of the interconnection process. This assumes that the information provided by the HCA map is current (e.g., refreshed monthly) [213] and accurate (e.g., data validation).

There is value to developers of integrating information which is currently listed in the Pre-Application Report into the HCA map. Xcel notes that the information in the Pre-Application Report, which is not provided in the HCA map, is not included for two main reasons. Capacity and loading data are not revealed for security reasons, while location-specific information, such as distance and equipment types, are impeded by technical limitations and the need for a query to be implemented within the map.[214] Where the information in the Pre-Application Report is not made public due to security concerns, the benefits to developers of having this information should be weighed against the risk of publicly revealing it.

While a Risk-Benefit Framework (Section 4.2) could be helpful in assessing whether to make some of the confidential information public based on the level of risk involved in doing so, special examination is needed to understand why the available generation capacity at the substation transformer and feeder levels is not already being made public. The security rationale for not providing the available generation capacity at the substation and feeder levels in the HCA is unclear, yet the benefit to DER developers of having access to this information is substantial. More specifically, it enables them to determine how to appropriately size their systems to mitigate constraints or informs their decision of whether to avoid certain constrained feeders altogether. Xcel states in its January 2021 Distribution Grid and Customer Security Comments that, at the substation and feeder levels, "aggregate levels of connected or in-queue distributed generation do not represent grid security risk" and could be made public.[215] HCA maps in New York and California provide connected/existing and in-queue distributed generation at the circuit level. California and New York IOUs provide substation capacity while California IOUs also provide feeder

[212] EPRI. 2020. *Defining a Roadmap for Integrating Hosting Capacity in the Interconnection Process*. p. 12.

[213] Xcel estimates that monthly HCA updates will take 3-4 years to complete, will have a project cost of $1.4M -$2.8M, and an annual incremental labor cost of $375,000 - $500,000.

[214] Xcel Energy. 2020. HCA Report. Attachment F, p. 16.

[215] Xcel Energy. *Comments – Response to Notice Distribution Grid and Customer Security.* Docket Nos.E002/M-19-685 and E999/CI-20-800 Nos. E002/M-19-685 and E999/CI-20-800. (January 21, 2021). Attachment B, pp. 4, 6.

capacity in their HCA maps. Given that Xcel does not classify installed, queued, or total distributed generation as confidential information, by extension, available capacity at the substation and feeder levels could also be made public. In a sense, Xcel is possibly providing feeder capacity by publishing maximum HCA results for a feeder. Hosting capacity at the head end of a feeder could possibly be the same as the "feeder rating" at the head. The former is based on the results of load flows, which account for impacts beyond just thermal limits, while the latter is only looking at the thermal (ampacity) of the equipment at the head end of the feeder. However, while the values may be different, they may also be the same. Thus, it seems reasonable that Xcel could publish the "feeder rating at the head end" on its HCA map. Or at minimum, Xcel could provide appropriate ranges for substation capacity (e.g., 10 MVA-20 MVA).

Where there are technology requirements rather than security concerns limiting integration of the Pre-Application Report data with the HCA, such as in the case of the distance from the site to the substation, Xcel should estimate the level of effort and cost to incorporate these data elements into the HCA. For example, Xcel estimated the cost of hiring a Geographic Information System (GIS) specialist to assist with updating and maintaining its HCA map.[216] Thus, Xcel could estimate the cost required to implement the equation(s) necessary to include the transformer and feeder generation capacity values in the map, as well as the cost for incorporating querying and search functionality. The latter improvement would enable users of the HCA map to determine the distance from the site to the substation or the distance to a 3-phase circuit, for example. DER developers in other states have noted the importance of querying functionality in hosting capacity maps for identifying suitable locations to interconnect DERs. However, an HCA map must first display the distribution lines before the querying/search functionality is incorporated. In the case of Xcel's HCA map, this feature would only be useful once the distribution lines are unblurred and so this should be the priority. Once this is achieved, Xcel could survey developers and other interested parties to determine the value of integrating the remaining Pre-Application Report data elements (such as the circuit distance from the point of coupling (PCC) to the substation, where a visual representation would be helpful) into the HCA map. The incremental benefits of integrating this additional information in the HCA could be balanced against the costs using a Cost-Benefit Framework as described in Section 4.3.

In summary, to really capture the value from integrating the Pre-Application Report with the HCA map, the priority should be for Xcel to unblur the map to reveal the feeder lines so that spatial information like the distance from the feeder to the substation can easily be visualized. Xcel should also prioritize increasing the refresh rate of its HCA map and validating its data so that it is accurate and current. This will enable customers to quickly screen for promising sites to inform their decision to interconnect DERs to the grid. Once Xcel accomplishes those tasks, integrating the remaining Pre-Application Report data into the HCA will be more useful to developers. However, in the interim, Xcel should clearly justify the security concerns it has regarding revealing substation and feeder thermal capacities given the tangible benefits to DER developers of having that information, and the fact that the feeder rating (thermal

[216] Xcel Energy. 2020. HCA Report. Attachment F, p. 14.

ampacity) at the head might already be public by using a feeder’s max hosting capacity results as a proxy. A Risk-Benefit Framework could also assist in balancing the risks of publishing substation and feeder capacities and peak loads against the public benefits.

4. Frameworks for Assessing Inclusion of Grid Data in HCA Maps

4.1. Overview

Minnesota DER developers and other renewable energy stakeholders want to increase the availability of specific types of grid data on Xcel’s HCA map to identify ideal locations for DERs and to promote beneficial electrification. Xcel also supports increasing DER penetration in its service territory and sharing grid data with developers but expresses concern that this needs to be done in a secure manner. There is always some level of risk or the possibility of an attack on the grid, but an appropriate framework can help to estimate and/or bound the risk and inform the Commission’s decision on whether, and how, sensitive grid distribution data should be shared. Application of a relatively simple and transparent framework could help to balance the grid security risks of revealing sensitive data with the public benefits. The results of such a framework could then provide a basis to develop risk mitigation plans and data-sharing policies to satisfy competing stakeholder objectives.

The Risk-Benefit Framework (Section 4.2) and the Cost-Benefit Framework (Section 4.3) are two possible frameworks that could be applied to help strike a balance between the need to block adversary access to sensitive grid information and providing information to developers who could use it to deploy DERs more effectively.

The Risk-Benefit Framework is used to semi-quantitatively determine the risk to a critical asset (such as a substation) due to revealing sensitive information about it (e.g., on an HCA map) over a one-year period. The framework does this by estimating the probability of an attack and the resulting consequence if the attack were successful. Based on the expected value of the risk, it can be categorized as a low, moderate, or significant risk. The risk level for each critical asset evaluated would then be compared to the value of revealing information about the same asset to the public.

The Cost-Benefit Framework could be used to compare the costs and benefits to the public/ratepayer of publicly revealing specific grid information. The benefits would include the incremental customer and societal benefits of making the information public and the costs would include the costs to the utility of providing this information and of defending against a better-informed attack. A net public benefit would inform whether the specific grid information should be made public.

In general, the Risk-Benefit Framework should be applied first to determine the overall level of risk to an asset from revealing information about it. The Cost-Benefit Framework can supplement it, adding more details about the actual cost of providing the information when there is an incremental labor cost to doing so (e.g., HCA map enhancements such as formulas and search functionality). If there is no risk involved with providing specific information, then the Cost-Benefit Framework should be used instead since it focuses primarily on weighing the economic costs versus the benefits.

Every framework or model has its limitations, and it is important to acknowledge them. There are several limitations to the risk formula in the Risk-Benefit Framework, including trying to directly assess probabilities for the actions of bad actors instead of modeling their ability to intelligently adapt; its failure to adjust for correlations among its components; and the intrinsic subjectivity and ambiguity of the threat, vulnerability, and consequence numbers.[217] Despite the framework's limitations, it still has some value given its relative simplicity, and for using it as a starting point for transparent discussions between stakeholders regarding the level of risk to the grid from revealing sensitive information. It is unacceptable to state that there are myriad undefined threats or attack vectors that exist, and consequently, no sensitive grid information should be revealed on a hosting capacity map. Using a risk-based framework helps stakeholders gain a shared understanding of the information under consideration so they can discuss risk more tangibly. These discussions will likely need to take place in a secure setting. Additionally, while the Cost-Benefit Framework is useful in weighing the costs and benefits of competing demands, it is not an exact science and has limitations. However, it can be useful as another data point when evaluating the net societal benefits of publicly releasing sensitive grid data.

Regardless of the framework selected, stakeholder discussions of the framework(s) need to be transparent and inclusive. A diverse stakeholder group including but not limited to DER developers, clean energy entrepreneurs, electric utilities, consumer advocates, local government and non-governmental organizations, and grid security experts should actively engage in these discussions to enable a broad range of contributions. This will ensure a more transparent and fair process for balancing the grid security risks with the public benefits of sharing sensitive information. Input from developers and other grid stakeholders will be essential to help determine the value of specific types of information for DER projects and other related renewable energy development efforts. It is important to recognize that there will be asymmetric access to the information needed to analyze the frameworks between the utilities and the public (e.g., DER developers, energy organizations), and that only the utilities may have sufficient resources (e.g., time and staff) to fully engage. These are inherent limitations of the stakeholder working group process.

4.2. Risk-Benefit Framework

4.2.1. Overview

Terrorist attacks such as 9/11 and natural disasters have heightened the nation's awareness of the risks to critical infrastructures. DHS released a risk-based performance standard, which is widely used by government agencies and industry, to estimate risk using the formula:

[217] Cox, Louis. 2008. *Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks.* The Society for Risk Analysis. 28. 1749-61.

Risk = Threat x Vulnerability x Consequence [Equation 1].

Where:

Risk = The potential for loss or harm due to the likelihood of an unwanted event and its adverse consequences.

Threat = The probability that an adverse event will occur within a specified period, usually one year. The event could be any with the potential to cause the loss of or damage to an asset or population.

Vulnerability = The probability that the estimated consequences of the adverse event will ensue. For example, if the adverse event is a terrorist attack, the "threat" is the probability of the attack occurring and the "vulnerability" is the probability of the attack succeeding.

Consequence = The outcomes of an event occurrence, including immediate, short- and long-term, and direct and indirect losses and effects. Loss may include human fatalities and injuries, economic damages, and environmental impacts, which can generally be estimated in quantitative terms, and non-quantifiable effects, including reductions in operational effectiveness or readiness, etc.[218]

Another closely related concept, *resilience*, is central to the purposes of risk management for critical infrastructures. It is defined as the ability of an asset, system, or facility to withstand an adverse event while continuing to function at acceptable levels or, if functioning is diminished, the speed by which an asset can return to the acceptable level of function (or a substitute function or service provided) after the event.[219] Resilience can be incorporated into Equation 1 as follows:

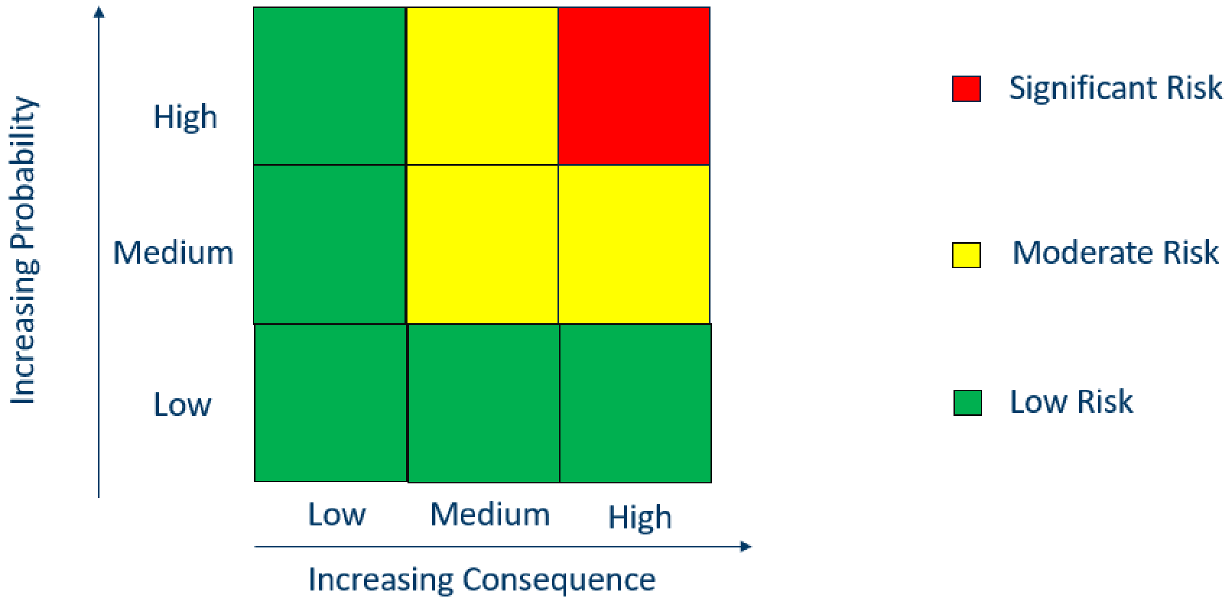
Risk = Threat x Vulnerability x Resilience x Consequence [Equation 2].

Figure 15 provides a qualitative representation of the overall level of risk based on the increasing probability of the threat occurring, as shown on the vertical-axis, and the increasing consequence of a successful attack, as displayed on the horizontal-axis. The colored squares in the figure indicate whether there is a low, moderate, or significant level of risk.

[218] Brashear, Jerry & Jones, James. 2010. *Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus)*, p. 3. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470087923.hhs003.

[219] Ibid.

Figure 15: Risk Framework



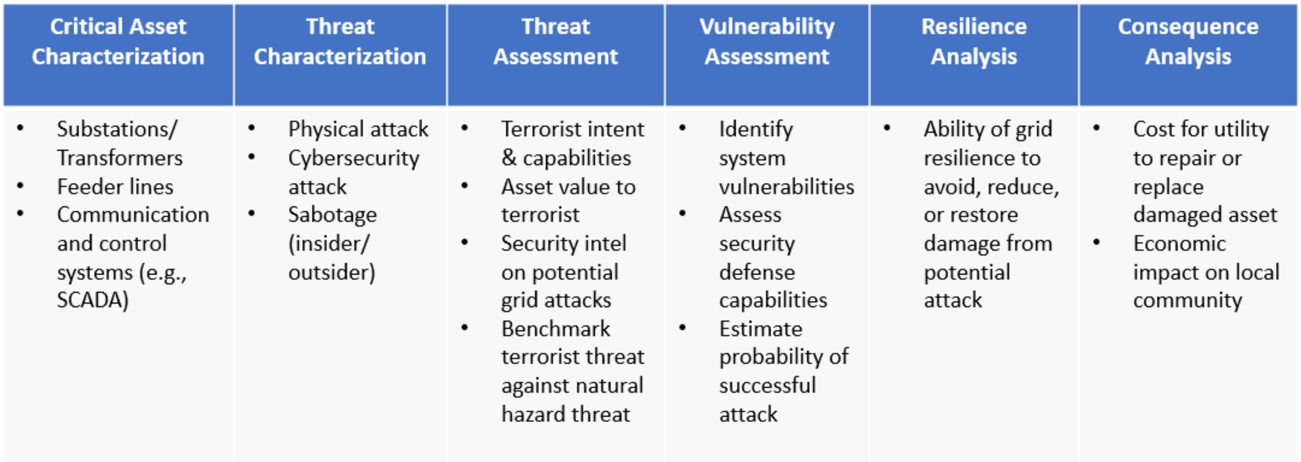
Source: https://www.stakeholdermap.com/risk/risk-assessment-matrix-simple-3x3.html

The framework could also apply to coordinated, simultaneous cyber and physical attacks against a single asset, or multiple assets at different locations on the distribution system, which could result in greater damage. Fundamentally, risk is an expectation, and expectations are additive in nature. Thus, the framework could be used to compute the expected risk for each attack type, on each critical asset. Those risks could then be added to obtain the overall risk for a coordinated, simultaneous, blended attack scenario.

The Risk Analysis and Management for Critical Asset Protection (RAMCAP^{TM}) Plus framework used by the DHS is an all-hazard risk and resilience management process for critical infrastructure.[220] A description of each step as applied for the purpose of determining the risk of a cyber or physical attack on the electric distribution system is listed below and summarized in Table 9.

[220] Id., p. 1.

Table 10: Risk Framework Analysis



Critical Asset Characterization	Threat Characterization	Threat Assessment	Vulnerability Assessment	Resilience Analysis	Consequence Analysis
• Substations/ Transformers • Feeder lines • Communication and control systems (e.g., SCADA)	• Physical attack • Cybersecurity attack • Sabotage (insider/ outsider)	• Terrorist intent & capabilities • Asset value to terrorist • Security intel on potential grid attacks • Benchmark terrorist threat against natural hazard threat	• Identify system vulnerabilities • Assess security defense capabilities • Estimate probability of successful attack	• Ability of grid resilience to avoid, reduce, or restore damage from potential attack	• Cost for utility to repair or replace damaged asset • Economic impact on local community

Source: Brashear, Jerry & Jones, James. (2010). Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus modified), p.5. 10.1002/9780470087923.hhs003

1. Critical Asset Characterization – List all the critical distribution system assets that could be attacked given public disclosure on a hosting capacity map.
   - Substations
   - Feeder lines
   - Other distribution facilities (please specify)

2. Threat Characterization – Determine the specific types of terrorist threat(s) or attack modes, in the local context, for each critical asset identified in 1.
   - Physical attack (e.g., sniper shooting a substation)
   - Cybersecurity attack (e.g., load manipulation)
   - Sabotage – physical/cyber by insider

3. Threat Assessment – Estimate the probability that a specific terrorist threat, as identified in 2, will occur in a specific city (e.g., Minneapolis) on a critical distribution system asset, in a given timeframe (typically a year). Can use information based on historical attacks of the distribution system in combination with subjective probability judgements to ascertain the probability of current and future risk. Other factors to consider include:
   - Potential terrorist motivations, intent, and capabilities
   - Attractiveness of grid facility relative to alternative targets
   - Critical asset's expected value (e.g., asset value to terrorist and consequence of asset damage/loss)
   - Intelligence from state homeland security officials and local law enforcement agencies
   - Comparisons with natural hazard risks to help deduce a terrorism threat probability

4. Vulnerability Assessment – Estimate the conditional probability that, if a given attack occurs, it will succeed. Vulnerability analysis involves an examination of existing system vulnerabilities, security capabilities, as well as countermeasures and their effectiveness. A process to assist in this determination is to:
   - Identify and rank potential distribution system critical asset vulnerabilities (e.g., physical, cyber, and personnel)

- Identify security capabilities to defend against threats given critical asset vulnerabilities (e.g., physical surveillance, asset hardening, cybersecurity, screening of personnel)
- For each specific attack vector, estimate the probability it will succeed given defense measures
  - Benchmark probability estimates of a successful threat from a natural hazard (e.g., severe weather causing a power outage) against probability estimates of a successful terrorist attack on a critical asset

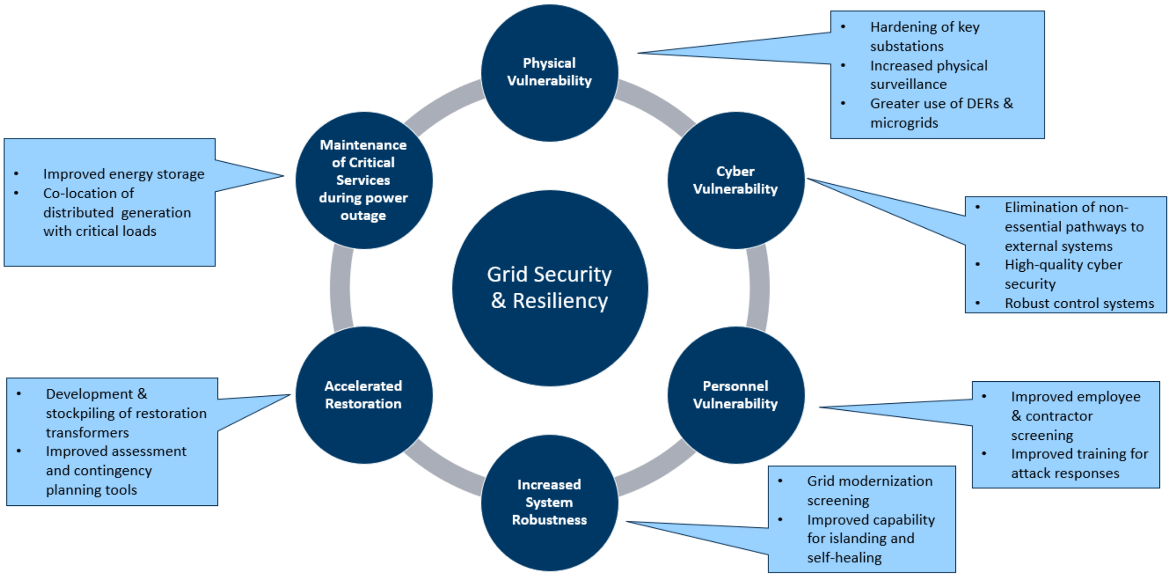
5. Resilience Analysis – Estimate the ability of the electric distribution system to avoid or withstand grid stress events without suffering operational compromise, or to adapt to and compensate for the resultant strains to minimize damage, and to rapidly recover from breakdown.[221]

6. Consequence Analysis – Identify and estimate the worst reasonable consequences generated by each specific asset/threat combination to estimate economic impacts. Economic impacts occur at two levels: (1) the financial consequences to the electric utility and (2) the economic consequences to the regional community in the electric utility's service territory. The primary concern for the public or community is the duration of the power outage and the direct and indirect economic consequences of service denial.

Figure 16 shows several grid security and resiliency factors which should be analyzed when conducting the distribution system threat and vulnerability assessments and resilience analysis. This includes a thorough assessment of the physical, cyber, and personnel vulnerabilities pertaining to grid security, and an assessment of the system's resilience. The system can be made more resilient through grid modernization, maintaining equipment stockpiles, contingency planning, and the strategic placement of DERs and microgrids to power critical services during an outage.

[221] *Hosting Capacity Analysis and Distribution Grid Data Security Workshop.* Docket No. E999/CI-20-800. (March 17, 2021). Attachment 3, p. 11.

Figure 16: Grid Security and Resiliency Factors


Physical Vulnerability
Hardening of key substations
Increased physical surveillance
Greater use of DERs & microgrids
Maintenance of Critical Services during power outage
Improved energy storage
Co-location of distributed generation with critical loads
Cyber Vulnerability
Elimination of non-essential pathways to external systems
High-quality cyber security
Robust control systems
Grid Security & Resiliency
Accelerated Restoration
Development & stockpiling of restoration transformers
Improved assessment and contingency planning tools
Personnel Vulnerability
Improved employee & contractor screening
Improved training for attack responses
Increased System Robustness
Grid modernization screening
Improved capability for islanding and self-healing

Source: National Research Council 2012. Terrorism and the Electric Power Delivery System, p.3. https://doi.org/10.17226/12050

4.2.2. Vulnerability Assessment

In conducting the vulnerability assessment in Step 4, specific points of vulnerability can be evaluated for each major component of the distribution system:

- Substation Transformers
- Feeder Circuits
- Protective Equipment/Switches
- Telecommunications
- Automation & Control Systems (e.g., supervisory control and data acquisition (SCADA), Distributed Energy Resource Management System (DERMS), Distribution Automation)
- Advanced Metering Infrastructure (AMI)

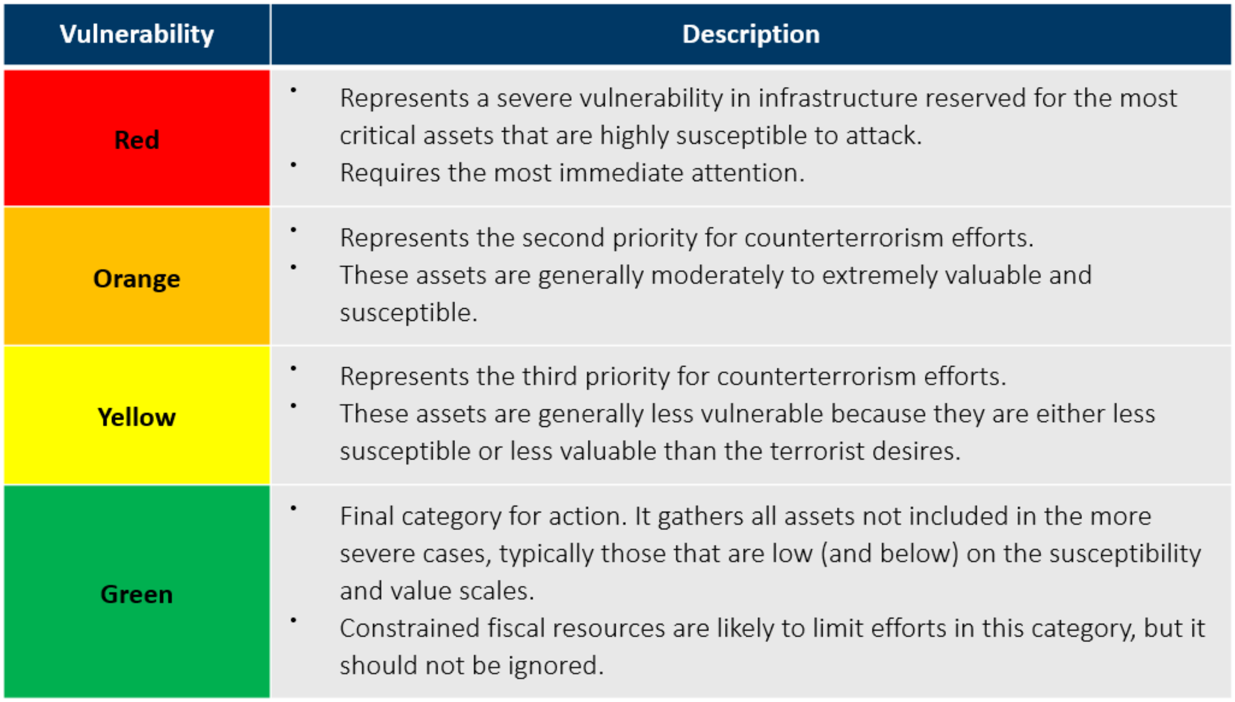
For example, when evaluating the vulnerability of a substation, security criteria to be considered include:

- Potential threat and probability of attack
- Frequency and duration of past security breaches
- Severity of damage
- Cost of breaches
- Safety hazards in the substation
- Equipment types and design
- Number and types of customers served

- Substation location
- Criticality of load
- Overall cost of facility
- Quality of service at existing substations
- Exposure to vandalism, sabotage, and terrorist attack of control houses, control equipment, and key electrical system components.[222]

Additionally, criteria can be established to categorize the different levels of critical asset vulnerability (Table 11). Critical distribution system assets which are especially vulnerable to attack fall into the red category and require immediate attention. Lower value, less vulnerable assets fall into the green category and require minimal attention but should not be ignored. Other distribution assets fall into the orange and yellow categories which represent the second and third priority for counterterrorism efforts.

Table 11: Vulnerability Characterization



Vulnerability	Description
Red	• Represents a severe vulnerability in infrastructure reserved for the most critical assets that are highly susceptible to attack. • Requires the most immediate attention.
Orange	• Represents the second priority for counterterrorism efforts. • These assets are generally moderately to extremely valuable and susceptible.
Yellow	• Represents the third priority for counterterrorism efforts. • These assets are generally less vulnerable because they are either less susceptible or less valuable than the terrorist desires.
Green	• Final category for action. It gathers all assets not included in the more severe cases, typically those that are low (and below) on the susceptibility and value scales. • Constrained fiscal resources are likely to limit efforts in this category, but it should not be ignored.

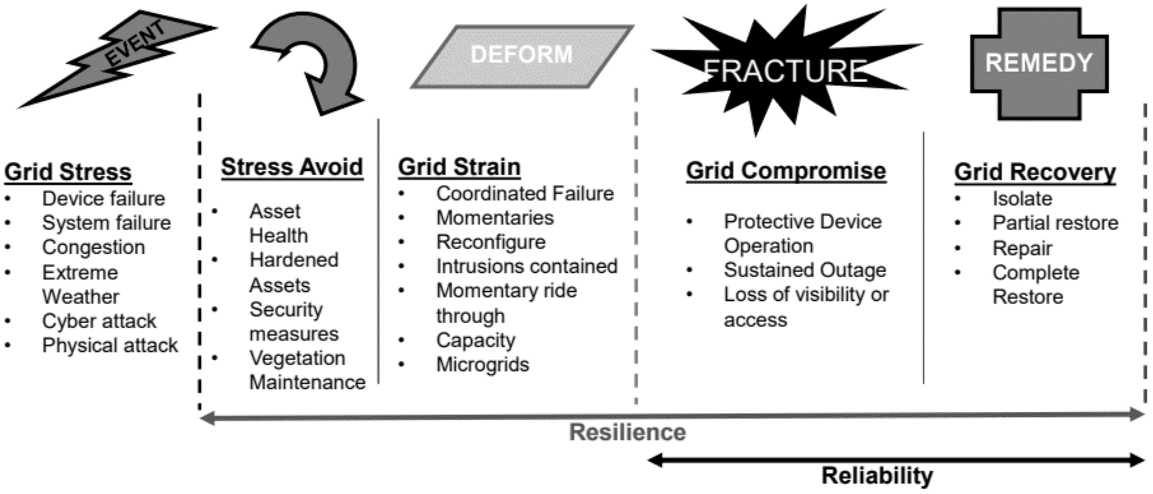
Source: Apostolakis, G. & Lemon, Douglas. (2005). A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. Risk analysis: an official publication of the Society for Risk Analysis. 25. 361-76.

[222] National Research Council 2012. *Terrorism and the Electric Power Delivery System*. p. 33.

4.2.3. Resilience Analysis

In Step 5, the utility will conduct a resilience analysis to assess its ability to recover from deliberate attacks, accidents, or naturally occurring threats or incidents.[223] While there is no industry definition of grid resilience, a perfectly resilient grid would be self-healing. This means that it could avoid, withstand, or minimize the effects of grid stress events. Figure 17 characterizes grid resilience along a spectrum ranging from grid stress to grid recovery based on the impact of the event (e.g., terrorist attack or natural hazard) given the distribution system's ability to withstand, respond to, or recover from it.

Figure 17: Characterization of Distribution System Operational Resilience



Source: Based on PNNL "Electric Grid Resiliency and Reliability for Grid Architecture" report, March 2018.

Table 12 provides an example of how the effects of resilience could be incorporated into Equation 2 using a resilience multiplier. When the distribution system has a high level of resilience (e.g., resilience level 3), and can avoid grid stress in response to a specific threat, then it would have a resilience multiplier close to zero, since it is fully able to mitigate or nullify the threat. On the other extreme, when the system has low or no level of resilience (e.g., resilience level 0) in response to a threat, then it would have a resilience multiplier closer to one, since it is unable to mitigate the impact of the threat.

[223] *Hosting Capacity Analysis and Distribution Grid Data Security Workshop.* Docket No. E999/CI-20-800. (March 17, 2021). Attachment 3, p. 6.

Table 12: Resilience Characterization

Resilience Level	Description	Resilience Multiplier
3	Resilience results in grid stress avoidance in response to threat	0.01
2	Resilience results in grid strain in response to threat	0.25
1	Resilience results in significant grid compromise in response to threat	0.75
0	No grid resilience in response to threat	1.00

4.2.4. *Consequence Analysis*

In conducting the consequence analysis in Step 6, it is important to separate the consequence of a successful physical or cybersecurity attack into two parts: (1) the consequence to the utility and (2) the consequence to the community. The consequence to the electric utility measures the economic impact of the attack on the utility. Table 13 shows how an attack's economic impact on a utility could be characterized. The consequence level indicates the severity of the damage to the electric utility and the disutility values are different weighting factors that could be applied based on the severity of the consequence. For example, if the attack would result in catastrophic grid equipment damage (e.g., on the order of more than $10 million) then it would have a disutility of one. However, if the attack would not result in any grid equipment damage, then it would have a disutility of zero.

Table 13: Consequence Characterization - Economic Impact to Utility

Consequence Level	Description	Disutility
3	Catastrophic grid equipment damage, greater than $10 million	1.00
2	Major grid equipment damage, $1 million to $10 million	0.75
1	Minor grid equipment damage, less than $1 million	0.25
0	No grid equipment damage	0.00

Similarly, Table 14 provides an example of how an attack's economic impact on a community could be characterized. The consequence level indicates the severity of the damage to the community in terms of the duration of a power outage, and the disutility values are different weighting factors that could be applied based on the severity of this consequence. For example, if the attack would result in a long duration power outage (e.g., 2-3 days), which would severely impact customers in the utility's service territory, then it would have a disutility of one. However, if the attack did not have any impact on customers, then it would have a disutility of zero. It is important to note that power outage duration is used as a proxy for community impacts more broadly and does not encapsulate all possible societal impacts to avoid making the framework overly complex. For example, an extended power outage which occurred during extreme weather conditions could result in loss of life. The power outage duration partially captures this dynamic given that a longer power outage is more likely to cause death than a shorter one.

Table 14: Consequence Characterization - Economic Impact to Community

Consequence Level	Description	Disutility
3	Severe impact to customers in utility service territory, power outage of 2-3 days	1.00
2	Major impact to customers in utility service territory, power outage lasting 24 hours	0.75
1	Minor impact to customers in utility service territory, power outage of 4-6 hours	0.25
0	No impact to customers in utility service territory	0.00

For each threat, the disutility of the consequence to the community and of the consequence to the electric utility could be appropriately weighted and combined. Assuming that both types of consequences are equally weighted, the disutility values could simply be averaged.

4.2.5. Example of Risk-Benefit Framework

Once all the threats, vulnerabilities, resiliency measures, and potential consequences have been assessed, the risk can be calculated using Equation 2. More explicitly writing out the components of Equation 2:

Risk = Threat x Vulnerability x Resilience x Consequence [Equation 2].

Where:
Threat = Probability of an attack: P(attack);
Vulnerability = Probability of a successful attack: P(success|attack);
Resilience = Resilience multiplier (e.g., a constant between 0 and 1); and
Consequence = Consequence of successful attack as represented by disutility (e.g., a constant between 0 and 1).

Table 15 displays how the risk components of Equation 2 could be summarized in a table for each critical asset (e.g., feeder, substation) and attack type (e.g., physical, cybersecurity) in a given year. The numbers in Table 15 are for illustrative purposes only.

Table 15: Risk Analysis

Critical Asset	Attack Type	Threat	Vulnerability	Resilience	Consequence	Risk per Asset
Substation	Physical	0.90	1.00	0.75	1.00	0.68
Feeder	Cyber	0.65	0.80	1.00	0.75	0.40
Feeder	Physical	0.40	0.30	1.00	0.25	0.03

Once the risk is calculated, the result can be matched according to the risk lower and upper bounds in Table 16 to determine the level of risk. The lower and upper risk bounds inTable 16 are for illustrative purposes.

Table 16: Risk Characterization

Risk Level	Risk Lower Bound	Risk Upper Bound
Significant Risk	0.66	1.00
Moderate Risk	0.36	0.65
Low Risk	0.00	0.35

The second part of the Risk-Benefit Framework involves estimating the public benefits of revealing sensitive-grid data on the hosting capacity map. Interested stakeholders should collaboratively develop survey questions that identify the main points of contention, such as whether to provide substation transformer ratings on the HCA map. The survey would be sent to members of the public including DER developers, entrepreneurs, clean energy organizations and advocates, and local energy policymakers to assess the value in making certain distribution system information available on Xcel's HCA map. An appropriate survey sample size would have to be determined at the outset to ensure a statistically significant response rate. The survey could ask for the respondent to rank the benefit of receiving substation transformer ratings, for example, on the HCA map as having "No Benefit," "Low Benefit," "Moderate Benefit," "Significant Benefit," or "Essential Benefit." The results for each question could then be analyzed using the values associated with each level of benefit shown in Table 17.

Table 17: Public Benefit Valuation

Public Benefit	Value
Essential Benefit	1.00
Significant Benefit	0.75
Moderate Benefit	0.50
Low Benefit	0.25
No Benefit	0.00

For example, if the survey question received 100 responses with the following response breakdown:

- No Benefit = 2 responses
- Low Benefit = 5 responses
- Moderate Benefit = 5 responses
- Significant Benefit = 60 responses
- Essential Benefit = 28 responses

The public benefit of having substation transformer ratings could be calculated using a value-weighted (e.g., benefit value x number of responses selecting this benefit) average as follows:

Public benefit of substation transformer ratings = [(0.00) x 2 + (0.25) x 5 + (0.50) x 5 + (0.75) x 60 + (1.00) x 28]/100 = 0.77.

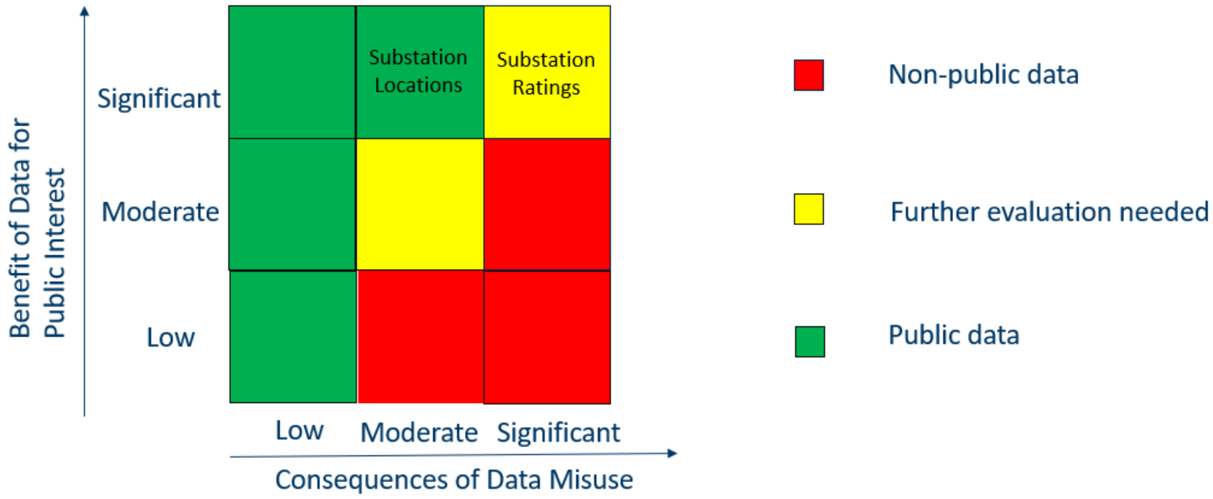
The public benefit value calculated for each question could then be matched to the public benefit category, between the appropriate lower and upper bounds, in Table 18. The lower and upper benefit bounds in Table 18 are for illustrative purposes only.

Table 18: Public Benefit Characterization

Public Benefit	Benefit Lower Bound	Benefit Upper Bound
Essential Benefit	0.85	1.00
Significant Benefit	0.75	0.84
Moderate Benefit	0.36	0.74
Low Benefit	0.00	0.35

Once the benefit has been calculated for each sensitive piece of grid information, such as substation transformer ratings or peak substation/feeder load, the benefits can then be weighed against the risks using the Risk-Benefit Framework. In this framework, grid data is categorized by the public benefit and the severity of the consequence from its misuse. Data becomes increasingly beneficial to the public up the vertical axis and the consequence of data misuse increases along the horizontal axis. The vertical axis uses the value-based classification for data: low benefit, moderate benefit, and significant benefit. The horizontal axis is categorized by the three levels of risk mentioned before: low risk, moderate risk, and significant risk. Where the data falls on the risk-benefit matrix determines whether it should be made publicly available. Figure 18 shows how the framework could be used to assess whether to make substation locations and substation transformer ratings publicly available on the hosting capacity map. Where those grid data points fall on the matrix is only for illustrative purposes. For example, grid data with significant benefit and a low level of risk regarding data misuse would clearly be made public. On the other hand, grid data with low benefit and a high level of risk for data misuse would not be made public. In scenarios where the grid data provided a significant public benefit but at a significant level of risk, further evaluation would be needed.

Figure 18: Risk-Benefit Framework



Benefit of Data for Public Interest	Low	Moderate	Significant
Significant	🟩	🟩 Substation Locations	🟨 Substation Ratings
Moderate	🟩	🟨	🟥
Low	🟩	🟥	🟥

Consequences of Data Misuse

🟥 Non-public data

🟨 Further evaluation needed

🟩 Public data

It is important that there be an open, transparent process, involving a diverse group of stakeholders, for evaluating and categorizing the benefits and risk levels associated with different types of grid data when determining whether they should be made public. The Commission should ultimately decide on the data's classification under this framework and should take stakeholder discussions into account.

4.3. Cost-Benefit Framework

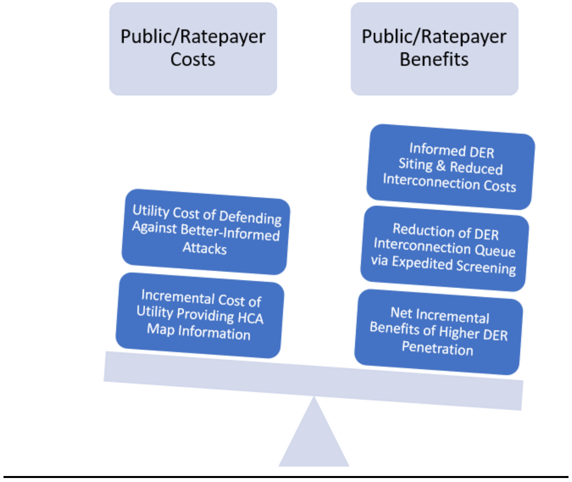
4.3.1. Overview

Cost-Benefit Analysis is a systematic approach for comparing the costs and benefits of alternative options. It is often used by electric utilities, both to optimize internal resource investment decisions and to justify these decisions to regulators and stakeholders.[224] A Cost-Benefit Framework can also be used to estimate the public/ratepayer benefits and costs of making specific distribution grid information public. The benefits would include the incremental customer and societal benefits of making the

[224] National Standard Practice Manual for Benefit-Cost Analysis of Distributed Energy Resources. 2020. p. 1-2. Available at: https://lpdd.org/wp-content/uploads/2020/08/NSPM-DERs_08-04-2020_Final.pdf.

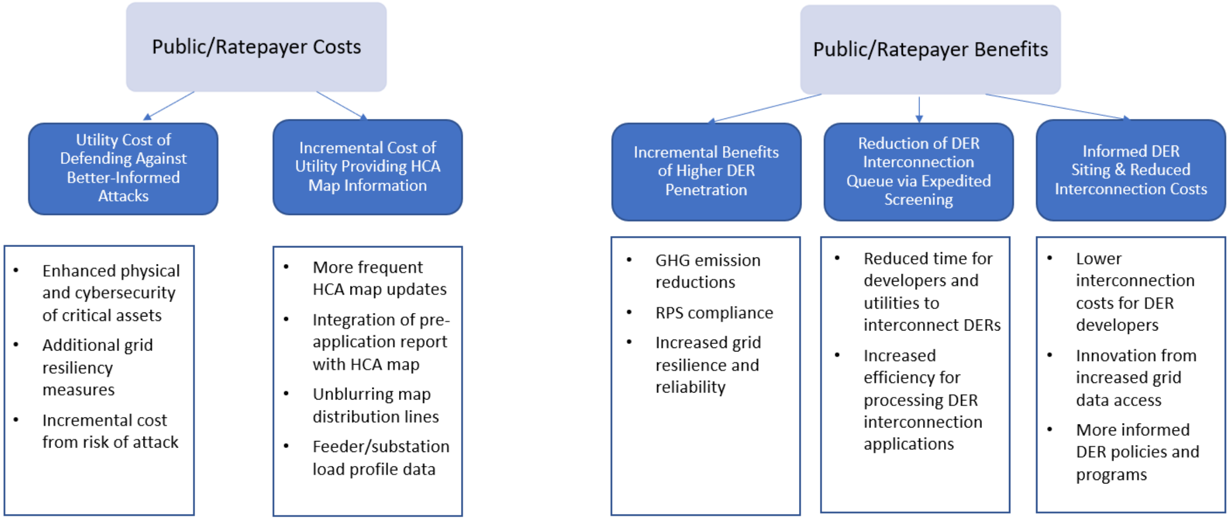
information public and the costs would include the costs to the utility of providing this information and of defending against a better-informed attack (Figure 19). A net public benefit would inform whether the specific grid information would be made public.

Figure 19: Cost-Benefit Framework


Public/Ratepayer Costs
Public/Ratepayer Benefits
Informed DER Siting & Reduced Interconnection Costs
Utility Cost of Defending Against Better-Informed Attacks
Reduction of DER Interconnection Queue via Expedited Screening
Incremental Cost of Utility Providing HCA Map Information
Net Incremental Benefits of Higher DER Penetration

When conducting this analysis, it is important to compare the incremental costs and benefits to the public or ratepayer for revealing specific types of grid data on the HCA map. For example, the calculation could weigh the incremental cost in releasing feeder location and peak loads against the incremental benefits of releasing the same data. Figure 20 further illustrates this comparison in greater detail.

Figure 20: Detailed Cost-Benefit Framework


Public/Ratepayer Costs
Utility Cost of Defending Against Better-Informed Attacks
Incremental Cost of Utility Providing HCA Map Information
Public/Ratepayer Benefits
Incremental Benefits of Higher DER Penetration
Reduction of DER Interconnection Queue via Expedited Screening
Informed DER Siting & Reduced Interconnection Costs

- Enhanced physical and cybersecurity of critical assets
- Additional grid resiliency measures
- Incremental cost from risk of attack

- More frequent HCA map updates
- Integration of pre-application report with HCA map
- Unblurring map distribution lines
- Feeder/substation load profile data

- GHG emission reductions
- RPS compliance
- Increased grid resilience and reliability

- Reduced time for developers and utilities to interconnect DERs
- Increased efficiency for processing DER interconnection applications

- Lower interconnection costs for DER developers
- Innovation from increased grid data access
- More informed DER policies and programs

4.3.2. Assessing Benefits

Beginning with the ratepayer benefits side of the equation, for each piece of grid information (e.g., peak load), the relevant stakeholders (e.g., developers, entrepreneurs, local energy policymakers, etc.) could be surveyed to better understand the incremental value of that specific information in terms of effectively siting DERs, lowering interconnection costs (e.g., screening out locations which may require costly system upgrades), informing policy, and/or other potential benefits. This same question could be repeated more specifically for DER developers in terms of how having access to that information could enable expedited screening of potential opportunities, and ultimately help to speed up the interconnection process.

Given that Xcel's HCA map has always been blurred (e.g., never displayed its feeder lines), it is difficult to estimate the incremental benefits of higher DER penetration due to providing more detailed information. However, lacking this information in Xcel's service territory, one could use as a proxy information from utilities on the coasts (e.g., New York and California) that went from less revealing hosting capacity maps (e.g., indicator maps) to detailed sub-feeder level hosting capacity maps to determine if the level of interconnections significantly increased because of that change. However, there is the possibility that other external factors, such as ramping up DER deployment to meet RPS targets, or policy changes leading to reductions in barriers to interconnection, could have also led to increases in DER interconnections. These external factors should be appropriately addressed in the framework. Alternatively, one could use the two-month period of September to November 2018 when California IOUs removed public access to their PV RAM maps, to assess the incremental impact that that change had on DER project development and interconnections. That information could then be used as a proxy to estimate how a change in hosting capacity information affected DER interconnections (e.g., percentage change) and deployment. This estimated effect could be used to approximate the corresponding societal benefits including environmental (e.g., reduced greenhouse gas emissions) and grid modernization (e.g., increased grid resiliency) benefits.

4.3.3. Assessing Costs

When assessing the incremental costs to the public/ratepayer from making certain grid data public on the hosting capacity map, one must examine the incremental costs to the utility of (1) providing the information and (2) the marginal cost of defending against a better-informed attack. With respect to the first point, Xcel has provided the costs of making several hosting capacity map improvements such as integrating its Pre-Application Report data and refreshing the map monthly. The cost (in dollars) of unblurring the distribution circuits on its map and providing substation and feeder load profiles could also be estimated. At the end of this part of the cost analysis, there would be a total dollar value associated with making these hosting capacity map improvements.

To approximate the marginal cost of defending against a better-informed attack, for each piece of grid data (e.g., revealing distribution lines), the utility would have to estimate the incremental cost of protecting its distribution infrastructure. This could include hardening additional distribution substations, and other critical infrastructure, burying more feeder lines underground, upgrading its cybersecurity defense capabilities, and other resource investments that would make the grid more resilient to an attack. The risk values determined in the Risk-Benefit Framework could inform the calculation of the incremental cost from the risk of an attack. In the Risk-Benefit Framework, the probability of an attack(s) on critical distribution system assets is estimated. Xcel could quantify the costs of potentially having to repair or replace damaged distribution infrastructure from an attack, and if it resulted in a power outage, estimate the costs to the public using metrics such as value of lost load and time to restore the system. Similar analyses are conducted to estimate the cost of a power outage due to a natural disaster. The Lawrence Berkeley National Laboratory Interruption Cost Estimate (ICE) calculator is a useful electric reliability planning tool that can be used to estimate the cost of an electric power interruption in the United States.[225]

4.3.4. Example of Cost-Benefit Framework

The following Cost-Benefit Framework example is for illustrative purposes only and an actual Cost-Benefit Analysis should be informed by data and assumptions from the utilities and stakeholder input.

The Cost-Benefit Framework could be applied for weighing the costs and benefits of integrating the Pre-Application Report grid data into the HCA map. The main benefits from Figure 20 that would be assessed are “Lower interconnection costs for DER developers,” “Increased efficiency for processing DER interconnection applications,” and “GHG emission reductions.” The other benefits included in Figure 20, while tangible, are more qualitative in nature. The primary costs from Figure 20 which would be analyzed in this example are the cost of the “Pre-Application Report Integration with HCA” and the “incremental cost from risk of an attack.” The other costs in Figure 20 including “enhanced physical and cybersecurity of critical assets” and “additional grid resiliency measures” could also be included, if Xcel provided cost information on implementing these measures as a direct result of revealing additional Pre-Application Report data in the HCA map. For simplicity, these costs were not included in the Cost-Benefit Analysis. Table 18 displays the results of this Cost-Benefit Analysis.

[225] Lawrence Berkeley National Laboratory, Nexant Inc., and U.S. Department of Energy. “Interruption Cost Estimate (ICE) Calculator.” Available at: https://www.icecalculator.com/home.

Table 19: Cost-Benefit Analysis

2020 Cost-Benefit Analysis	Total ($MM)
Benefits	**$12.7**
Lower Interconnection Costs for Developers	$0.2
Increased Efficiency of Processing DER Interconnection Applications	$6.0
GHG Emission Reductions	$6.5
Costs	**$3.0**
Pre-Application Report Integration with HCA	$1.0
Incremental Cost for Risk of an Attack	$2.0
Net Benefit (Benefits – Costs)	**$9.7**
Benefit-Cost Ratio	**4.2**

Costs

Pre-Application Report Integration with HCA: Xcel estimates that fully integrating the Pre-Application Report with the HCA would take one year to implement and would cost between $600,000 and $1.2 million.[226]

Incremental Cost for Risk of an Attack: There are several pieces of information within the Pre-Application Report (listed below) that have security concerns associated with publishing them.

- Substation and feeder peaks loads
- Substation and feeder capacities
- Distance between site and substation
- Protective devices and regulators between site and substation
- Conductor types between site and substation

Regarding these data elements, Xcel could estimate the incremental cost from risk of an attack, on a critical asset (e.g., substation) using the expected risk value calculated in the Risk-Benefit Framework. The probability of a successful attack on the asset would then be multiplied by the economic consequence (in dollars) of an attack on the asset to determine the total cost. For example, if the probability of a successful attack on a distribution substation transformer was 10 percent due to revealing more information about it (e.g., substation transformer peak load or capacity), the cost to replace the damaged substation transformer was $10 million,[227] and the attack resulted in a severe

[226] Xcel Energy. 2020. HCA Report. Attachment F, p. 16.

[227] Utility Dive. "Xcel assesses non-wires alternatives to distribution upgrade as it enters new proceedings in Colorado, Minnesota." January 30, 2020. Available at: https://www.utilitydive.com/news/xcel-assesses-non-wires-alternatives-to-distribution-upgrade-as-it-enters-n/571290/.

power outage resulting in economic damages of $10 million to customers, then the incremental cost from the risk of an attack would be $2 million (10% x $20 million).

Other Costs: Other costs, such as the cost to make the substation transformers more resilient to physical attack, because of publishing more information about them, could also be included in the total cost.

Total Costs: However, assuming no additional costs (e.g., grid resilience), and that the actual cost to integrate the data fields in the Pre-Application Report with the HCA map costs $1 million, the estimated total cost to the ratepayer would be $3 million.

Benefits

To determine the benefits (in dollars) of incorporating the Pre-Application Report data into the HCA map, we could analyze the lower interconnection costs for DER developers, and any incremental increases in Xcel's efficiency in processing DER interconnection applications. The Commission recently fined Xcel $1 million for numerous complaints over delays in connecting solar projects to the grid.[228] This incident highlights the economic value of making additional information available to developers that could help inform their interconnection applications and streamline the MN DIP.

Benefits to Developers Regarding Lower Interconnection Costs: We could use the number of Pre-Application Reports in a given year as a proxy. For example, Xcel processed 368 Pre-Application Report requests in 2020. With each report costing $300, this resulted in a total cost to developers of $110,400, which would be saved because of the integration of the Pre-Application Report with the HCA. There would also be a corresponding time savings for the electric utility engineer who has to process the Pre-Application Reports. Assuming it takes five hours for an Xcel engineer who is paid $50 per hour (e.g., approximately $100k per year) to process each report, the time savings for processing the 368 reports in 2020 would equal $92,000. Thus, the total cost savings to Xcel and the DER developers would be $202,400 or approximately $200,000.

Increased Efficiency of Processing DER Interconnection Applications: In 2020, Xcel received 2,901 solar PV interconnection applications and interconnected 1,539 solar PV projects.[229] If Xcel were to share more grid information on its HCA map, this could lead to higher quality developer interconnection applications, help to reduce the number of applications Xcel receives, and/or increase Xcel's ability to process more applications. Reducing Xcel's project interconnection queue could save DER developers time and money by expediting approval of their projects and helping them to meet their project deadlines. The savings accrued for developers, the reduced time for Xcel engineers to process interconnection applications, and the avoided costs (e.g., fines) for Xcel not meeting its interconnection and utility customer performance rating targets, would result in economic benefits to ratepayers. All

[228] Energy Central News. "State regulators fine Xcel Energy $1M over dispute with solar developers." January 22, 2021. Available at: https://energycentral.com/news/state-regulators-fine-xcel-energy-1m-over-dispute-solar-developers?utm_medium=eNL&utm_campaign=DAILY_NEWS&utm_content=400384&utm_source=2021_01_25.

[229] Xcel Energy. *2020 DER Interconnection Report*. Docket No. E999/PR-21-10. (March 15, 2021).

these benefits from a streamlined interconnection process could be added together to provide a total benefit.

For purposes of this example, we will focus on the benefits gained from an Xcel engineer more efficiently processing interconnection applications. For example, if it takes three months for an Xcel engineer earning $50 per hour to complete a full system interconnection study while working on it half-time (e.g., 20 hours per week), the total value of her time would be $12,000 per application. In 2020, Xcel interconnected roughly 1,500 solar PV projects. Theoretically, if the same engineer reviewed all these interconnection applications, the total cost for her time would be $18 million. Assuming the integration of the Pre-Application Report with the HCA led to greater efficiencies processing interconnection applications, and that now the same engineer could review each application in two months, instead of three, the total value of her time would be $8,000 per application. This results in a new total cost for her to process 1,500 interconnection applications of $12 million, a savings of $6 million.

Emission Reductions: Additional benefits could include increased DER project installations, and the corresponding reduction in greenhouse gas emissions. For example, in 2010, Xcel estimated that the annual avoided emissions costs (including CO_2, SO_x) in the year 2020 was $26.34 per MWh.[230] The average annual capacity factor of Minnesota solar facilities in 2018 was approximately 19 percent.[231] Applying this capacity factor to the 1,539 solar PV projects (≤ 1 MW) interconnected in 2020 results in generation from these solar PV systems of roughly 246,762 MWh. Thus, there were emission reduction benefits worth approximately $6.5 million (246,762 MWh x $26.32/MWh) in 2020. However, there would have to be a direct link between this value and revealing additional grid data on the HCA map, which led to an incremental deployment of solar PV systems on the grid.

In this example, there is a net benefit, as shown in Table 18, to the ratepayer of integrating the information from the Pre-Application Report into the HCA.

5. Models for Information Sharing

5.1. Introduction

Regulators are tasked with designing effective models to share data. Accessible energy-use data can help customers better manage their energy bills, local governments to measure the effectiveness of

[230] Xcel Energy Public Service Company of Colorado. 2010. *2009 Demand-Side Management Annual Status Report.* p. 99. Available at: https://www.xcelenergy.com/staticfiles/xe/Regulatory/CODSM2009AnnualStatusReport.pdf.

[231] Orr, Isaac. 2020. "Federal Data Confirms Minnesota Solar Panels Don't Work Well in Winter." American Experiment, Energy and Environment. Available at: https://www.americanexperiment.org/federal-data-confirms-minnesota-solar-panels-dont-work-well-in-winter/.

energy programs more effectively, and energy service providers to better design new services.[232] In order to be effective, these models must weigh the benefits and risks associated with providing secure access to data. Effective models for information sharing can decrease this risk while still allowing access to valuable data. These models should be built upon standards and principles that govern secure and useful access to data.

While not specific to energy, DHS has provided principles that have been used globally. Its Fair Information Practice Principles (FIPPs) are used to guide many data-sharing policies.[233] The FIPPs include eight principles: "Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing."[234] Together, these principles guide how the DHS treats PII. When applying these principles, the following questions regarding data-sharing should be considered:

1. Who needs access to the data and why?
2. Who is responsible for granting access to the data?
3. How can the data be delivered securely and efficiently (e.g., streamlined process)?

Answers to these questions can help provide a framework for sharing information. An effective data-sharing model must be transparent, clearly stating data access requirements for different data user groups (e.g., academic researcher), identify what information is confidential, and the criteria, if any, for accessing the confidential information.

5.1.1. When and How to Protect Data

The "Need-to-Know" and the "Need-to-Protect" principles can help regulators decide when and how information needs to be protected.[235] Using the "Need-to-Know" criteria would help to determine when customers who require sensitive information should receive it. In the context of hosting capacity, this might include energy developers who need to know specific distribution grid data (e.g., substation capacity) to develop and implement DER projects. The "Need-to-Protect" criteria could, for example, restrict data on specific feeders based on the criticality of the loads they serve (e.g., critical customer groups). This data could then be accessed under an NDA, or in another secure manner, as the utility and/or Commission sees fit.

[232] American Council for an Energy-Efficient Economy (ACEEE). 2020. "Facilitating Access to Community Energy Usage Data." Available at: https://www.aceee.org/toolkit/2020/02/facilitating-access-community-energy-usage-data.

[233] Teufel III, Hugo. 2008. *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security.* DHS. Available at: https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[234] Ibid.

[235] Xcel Energy. *Response to Notice distribution Grid and Customer Security*. Docket Nos. E002/M-19-685 and E999/CI-20-800. (January 29, 2021). Appendix B, p. 23.

To protect data, third parties requesting it may be required to register for data access, log into web portals, sign an NDA, or meet other screening criteria as defined by the party providing access. Each of these security measures protects data in a separate way. For example, requiring users to register for web portal access allows the utility to verify the users, monitor user activity, and question suspicious behavior. Alternatively, NDAs prevent users from sharing data, thereby limiting the potential for another party to misuse the data. In short, data-sharing models determine who can access a given set of data and outline the conditions for such access. Additionally, frameworks such as a Risk-Benefit Framework (Section 4.2) can be used to determine when to apply different data security measures.

5.2. Types of Data-Sharing Models

5.2.1. Overview

The most basic model for information sharing is one that simply determines if information can be made public.[236] Once the decision is made to withhold public access to data, other ways of sharing the information should be considered. These data-sharing methods range from a simple email or phone call to an in-person consultation or tiered-access using a web portal. The following sections describe different models for data-sharing.

5.2.2. Data Classifications

Once data is identified as sensitive, it can be classified according to the level of damage that could result from its release. For example, the United States Government groups "classified" into three categories."[237]

> Top Secret: Applied if the data's release could be expected to cause "exceptionally grave damage to the national security."[238]
>
> Secret: Applied if the data's release could be expected to cause "serious damage to the national security."[239]
>
> Confidential: Applied if the data's release could be expected to cause "damage to national security."[240]

Additionally, some information may be categorized as sensitive but unclassified, meaning that the data is "not classified for national security reasons, but that [it] warrants/requires administrative control and

[236] Google Inc*. Mobility Best Practice: Tiered Access at Google.* Available at: https://lp.google-mkto.com/rs/248-TPC-286/images/eBook%202%20-%20Tiered%20Access_v5%20-%20Google%20Cloud%20Branding.pdf.

[237] Quist, Arvin. 1993. *Security Classification of Information Volume 2. Principles for Classification of Information. Chapter 7 Classification Levels*. Oak Ridge National Laboratory.

[238] Ibid.

[239] Ibid.

[240] Ibid.

protection from public or other unauthorized disclosure for other reasons."[241] The classification of data is often derived from the risk associated with its release (e.g., risk-based). However, classification can also be derived from other measures, such as which parties have access to it. For example, the Minnesota Government Data Practices Act established several classifications for accessing non-public data.[242]

> Private: "data identifying an individual that are only available to the individual or with the individual's consent (Minn. Stat. § 13.02, subd. 12)."[243]
>
> Confidential: "data identifying an individual that are not available to anyone outside the entity holding the data, including the individual (Minn. Stat. § 13.02, subd. 3)."[244]
>
> Non-public: "data on a business or other entity that are only available to the subject of the data or with the subject's consent (Minn. Stat. § 13.02, subd. 9)."[245]
>
> Protected non-public: "data on a business or other entity that are not available to the subject of the data or anyone else outside the entity holding the data (Minn. Stat. § 13.02, subd. 13)."[246]

Data can be classified in a variety of ways according to different criteria. These classifications can be used to inform models for information sharing.

5.2.3. Tiered Access to Information

Once data has been classified, it can be broken into tiers to determine who should access information and how they should access it. Figure 21 displays how a tiered-access model might function. In this example, data that is sensitive is assigned a classification based on its security level. The security level determines if the information needs to be protected, and if it does, by what mechanism. For example, certain grid data might have a moderate security restriction level, in which case, an NDA could provide third-party access to the data.

[241] The Office of Cybersecurity. 2021. "Sensitive but Unclassified Information (SBU)". Available at: https://fam.state.gov/fam/12fam/12fam0540.html.

[242] Minnesota House of Representatives. 2010. "Minnesota Government Data Practices Act: An Overview." Available at: https://www.house.leg.state.mn.us/hrd/pubs/dataprac.pdf.

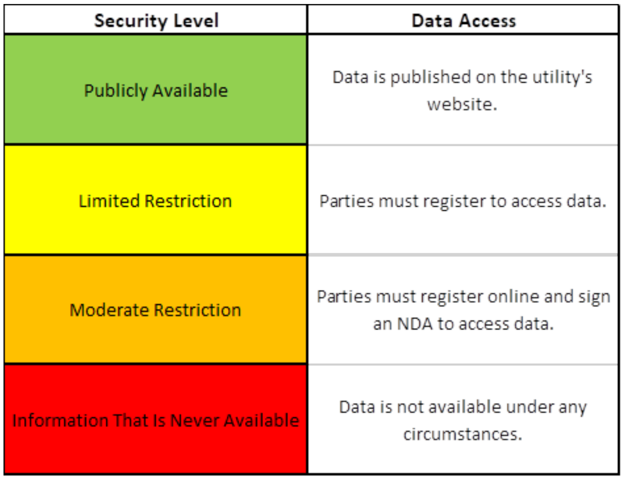
[243] Ibid.

[244] Ibid.

[245] Ibid.

[246] Ibid.

Figure 21: Tiered Access to Information



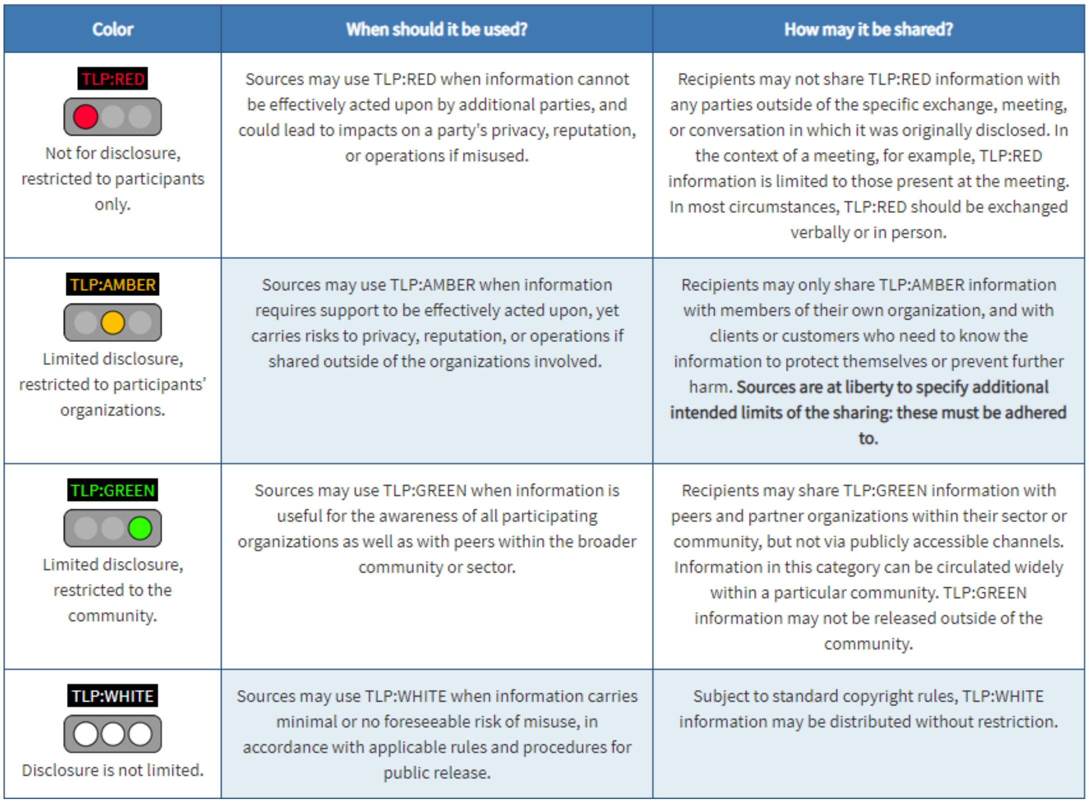
Security Level	Data Access
Publicly Available	Data is published on the utility's website.
Limited Restriction	Parties must register to access data.
Moderate Restriction	Parties must register online and sign an NDA to access data.
Information That Is Never Available	Data is not available under any circumstances.

At a national level, DHS uses the traffic light protocol (Figure 22) to determine when and how sensitive information can be shared.[247] This risk-based, tiered system restricts the spread of sensitive information by limiting who can discuss and reference it. When the traffic light is green, for example, information can be shared within a community. When the traffic light is red, information may only be shared by the parties that participated in the exchange where the information was originally disclosed. Information with the red designation should only "be exchanged verbally or in person" under most circumstances.[248]

[247] DHS Cybersecurity & Infrastructure Security Agency. "Traffic Light Protocol (TLP) Definitions and Usage." Available at: https://www.cisa.gov/tlp.

[248] Ibid.

Figure 22: Traffic Light Protocol



Color	When should it be used?	How may it be shared?
TLP:RED ● ○ ○ Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER ○ ● ○ Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN ○ ○ ● Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE ○ ○ ○ Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Source: DHS Traffic Light Protocol. https://www.cisa.gov/tlp

The type of information can also play a role in a tiered-access model. For example, aggregated data at the community level could be published on the utility's website, while aggregated data at the zip code level could require prior registration. Similarly, data might only be made available to certain parties under certain conditions. As discussed in Chapter 3, the Commission ruled in Docket No. E, G999/CI-12-1344 that access to CEUD is tiered based on whether the customer has given consent.[249] In this case, there are two tiers of data available, with more granular information only being provided if a customer opts to allow their data to be shared.

The tiered access information sharing model is dynamic in the sense that it can be applied in many ways. It is also flexible because it can account for any number of tiers based on the use case. In one sophisticated example of tiered access, Google is considering temporal tiered-selection where team members can "voluntarily move across trust tiers in real-time, dropping tiers when access is no longer

[249] *In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities,* Docket No. E,G-999/CI-12-1344. (June 17, 2013).

needed (e.g., to be at 'fully trusted' for the next two hours only)."[250] By having tiers, additional information becomes available in a manner appropriate with its risk.

5.2.4. Models for Accessing Energy Data

While third parties may be reasonably required to protect information, the way in which information is shared plays a critical role in its overall security. For example, in some cases, a simple email or phone call may be enough to securely transmit information. However, other situations may require a different mode for securely sharing sensitive information, such as requiring a third-party to go to a secure location before gaining access to the information. More frequently, however, data is made available online via a web portal or platform. In the 2020 New York Department of Public Service (DPS) Staff Whitepaper Regarding a Data Access Framework, the DPS noted that, "when considering what cybersecurity protections need to be in place for access to energy-related data, it is necessary to evaluate the means in which that data will be transmitted or accessed."[251] Different models or platforms may provide increased ease of access or protection for data. The DPS whitepaper lists the following five ways for sharing energy data online.[252]

1. *Direct Connection to Data Custodian IT System*: In most cases the "Data Custodian" is the utility. In this case, the data custodian provides a third-party requesting data with direct access to its IT system (not a data portal). Both parties must ensure that proper data security procedures are in place. The DPS notes that this connection will entail the "highest level of cybersecurity requirements."[253]

2. *Centralized Data Warehouse*: In this system, an alternative location is developed to store and access energy data. This could be a portal or platform and would need to be built by the data custodian. The third-party requesting the data would still need to meet certain requirements. These requirements would be based on how the data would be accessed, either "through a direct connection or through a platform or portal."[254]

3. *Secondary Access Platform or Portal*: A secondary access platform or portal would take data from the data custodian's IT system and place it on a platform or portal as needed. Essentially, the secondary access point would transmit data between the IT system (where the data is stored) and the third-party (where data is received). There is significant variability in the cybersecurity requirements for this type of platform. These requirements would depend on whether the data is public and what cybersecurity measures both the third-party and the data custodian have in place.

[250] Google Inc*. Mobility Best Practice: Tiered Access at Google.* Available at: https://lp.google-mkto.com/rs/248-TPC-286/images/eBook%202%20-%20Tiered%20Access_v5%20-%20Google%20Cloud%20Branding.pdf.

[251] New York Department of Public Service (NY DPS). *Department of Public Service Staff Whitepaper Regarding a Data Access Framework*. Case 20-M-0082, (May 29, 2020). p. 25.

[252] Ibid.

[253] Ibid.

[254] Ibid.

4. *Public Platform*: On a public platform, all data is protected using aggregation or anonymization before being made available. This type of platform would not require the third-party to register before accessing it. An example of this would be the current Utility Energy Registry in New York.[255] Third parties can access aggregated and anonymized data without registration or cybersecurity protections in place. Since the data is already public, there is no need to protect it.

5. *Secure Portal or Platform*: Under this system, sensitive data is stored on separate servers, and third parties can access it using a secure portal/platform such as Green Button Connect. The DPS described the secure platform as representing a "lower risk" because of the separation of servers and "because many of these secure access points have been designed with cybersecurity and privacy controls built in."[256]

Developing a secure and accessible access mechanism for transferring third-party information could be an important step for Minnesota to take as it seeks to further support the growth of DERs. Each of the data release mechanisms above should be analyzed with respect to their security and the ease of data accessibility. In choosing a mechanism, Minnesota Commissioners should consider the burden placed on the utility to create the mechanism, the security of the customer information, and the need to provide developers with access to energy information. Finally, models for information sharing in other states can give insight into national best practices.

5.2.5. Green Button

Green Button is a specific example of a model used for sharing CEUD in many states.[257] The Green Button Standard was developed by the North American Energy Standards Board (NAESB) with the support of the DOE, the National Institute of Standards and Technology (NIST), and the White House Office of Science and Technology Policy. These industry standards are designed to define the "data exchange protocol for the transfer of energy usage information between a utility and a third-party with customer authorization."[258] The listing of the standards themselves is proprietary information. The standards inform the Green Button model, which is used as a model for data-sharing by many utilities in North America.

The Green Button model has two main sub-programs: Green Button Download My Data (DMD) and Green Button Connect My Data (CMD).[259] CMD provides energy customers and third parties with a secure and automated way to access standardized energy usage data. CMD enables utility customers to

[255] New York State Energy Research and Development Authority. "Utility Energy Registry." Available at: https://utilityregistry.org/app/#/.

[256] NY DPS. *Department of Public Service Staff Whitepaper Regarding a Data Access Framework*. Case 20-M-0082, (May 29, 2020). p. 26.

[257] North American Energy Standards Board. "The NAESB Energy Services Provider Interface Model Business Practices Information Page." Available at: https://www.naesb.org/ESPI_Standards.asp.

[258] Ibid.

[259] Green Button Data. "Green Button Connect My Data". Available at: https://www.greenbuttondata.org/cmd.html.

both access their own data and to conveniently authorize third parties to do the same. Utility data can also automatically be uploaded to these CMD platforms. Once on the platform, CMD secures the data and ensures its integrity and accuracy, while DMD provides downloadable data that complies with the consistent data format provided by the Green Button Standard. Utilities receive Green Button Certification after the Green Button Alliance confirms that the utility has properly implemented the Green Button Standard and provided consistently formatted data.

5.3. Benchmarking Sharing Hosting Capacity Map Data

Table 20 depicts how utilities across the United States share energy data, including hosting capacity map information, in a variety of ways.[260] Even utilities within the same state can differ on their requirements for sharing hosting capacity information. For example, both the New York and California IOUs have different protocols for accessing hosting capacity map data. In California, both PG&E and SDG&E require registration and user logins to access their hosting capacity maps while SCE provides open access. In New York, most of the IOUs require registration and user log-in to access their hosting capacity maps, while NYSEG/RG&E and O&R do not.

Several utilities require NDAs to receive what they determine to be confidential or trade secret information. In Minnesota, all the utilities require an NDA to access sensitive information in their Pre-Application Reports except for Dakota Electric. In California, the IOUs are not requiring an NDA to access hosting capacity or pre-application report data but require NDAs for the release of CEII on a "need-to-know" basis. To date, the California IOUs have not designated any data CEII per the CPUC process.

Table 20: Models for Information Sharing Pre-Interconnection

	MN IOUs				NY IOUs					CA IOUs					
Data Sharing Model	Dakota Electric	MN Power	Otter Tail	Xcel Energy	Central Hudson	Con Ed	National Grid	NYSEG/ RG&E	O&R	PG&E	SCE	SDG&E	Pepco	HECO	NV Energy
HCA Map Open Access				●			●	●	●		●		●	●	
Web Portal (HCA /System Data)					●	●	●	●	●	●		●			●
Pre-application Report	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Non-Disclosure Agreement		●	●	●											

[260] *Sensitive Information Classification and Sharing Workshop*. Docket No. E002/M-19-685. (March 31, 2021).

5.4. Models for Data-Sharing in Minnesota

5.4.1. Sharing Sensitive Customer Information

In Minnesota, aggregated customer information is shared with third parties through the utilities. This decision was established in Minnesota Docket No. E,G999/CI-12-1344.[261] In this docket, the Commission decided that "utilities that already have a practice for releasing CEUD to third parties after taking steps to anonymize the data—for example, by aggregating that data with other customers' data before releasing it—should file these practices with the Commission."[262] This left the final decision in the hands of the utility. Most of the utilities currently provide access to aggregated CEUD data.[263] The exception is Dakota Electric, which provides "member account information, such as electric consumption, billing and collections, and credit history" to members either in-person or over the phone if specific identification is given.[264] Moreover, none of the utilities release specific individual CEUD without customer consent.[265] Most of the utilities in Minnesota are using a tiered-access system based on whether the customer has given consent. With customer consent, third-party requestors gain access to more granular information. However, if they have not received consent, then they only get access to appropriately aggregated information.

5.4.2. Sharing System Information: The MN DIP Process

Utilities in Minnesota apply a tiered-access approach to sharing information with third parties during the DER[266] interconnection process (e.g., MN DIP).[267] Before going through the MN DIP, developers may use the hosting capacity map to gain public interconnection information. Next, the developers may begin the MN DIP interconnection process by signing an NDA and receiving a Pre-Application Report, which details non-public, site-specific information. Finally, the most detailed interconnection information is available during the MN DIP process. Xcel notes that even CEII information may be available and emphasizes that the "MN DIP does not identify which distribution grid information is designated as CEII, but does provide for another level of protection for this critical infrastructure information."[268] Figure 23

[261] *In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities,* Docket No. E,G-999/CI-12-1344. (June 17, 2013).

[262] *Order Adopting Open Data Access Standards and Establishing Further Proceedings*. Docket Nos. E,G-999 and M-19-505. (November 20, 2020) p. 4.

[263] Minnesota Department of Commerce. *Staff Briefing Papers-CORRECTED. Docket 16-777. (*July 16, 2020). pp. 76-77.

[264] *Dakota Electric Association Comments in Response to October 30, 2020 Notice of Comment Period. 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 Nos. E999/CI-20-800 and E002/M-19-685. (January 29, 2021) p. 7.

[265] Minnesota Department of Commerce. *Staff Briefing Papers-CORRECTED. Docket 16-777. (*July 16, 2020). p. 77.

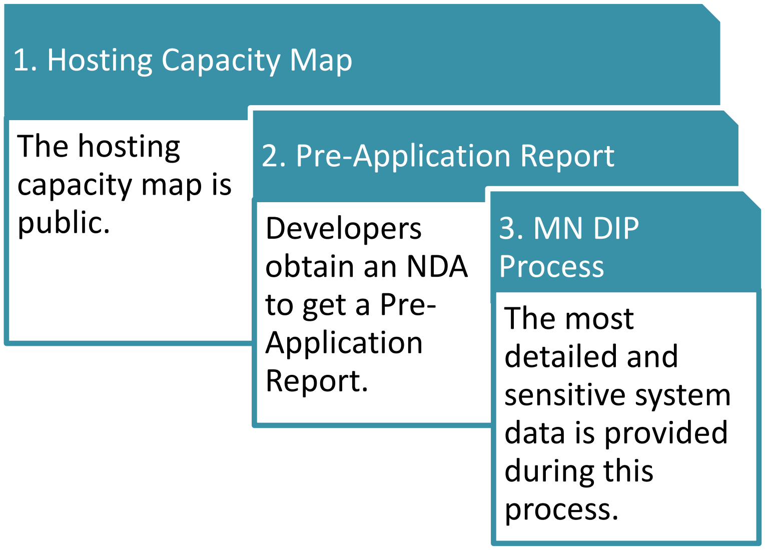
[266] Only DER projects up to 10 MW are considered as part of the MN DIP process.

[267] MPUC. "Distributed Energy Resources Interconnection Process (MN DIP)." Available at: https://mn.gov/puc/assets/MN%20DIP_tcm14-431769.pdf.

[268] *Xcel Energy Comments. Response to Notice Distribution Grid and Customer Security Docket Nos.* E002/M-19-685 and E999/CI-20-800. (January 29, 2021). p. 17.

summarizes how this approach uses tiered methods to protect more detailed information from public access.

Figure 23: Tiered-Access Interconnection in Minnesota



1. Hosting Capacity Map

The hosting capacity map is public.

2. Pre-Application Report

Developers obtain an NDA to get a Pre-Application Report.

3. MN DIP Process

The most detailed and sensitive system data is provided during this process.

5.4.3. *Tiered-Access Approach for Sensitive Grid Data*

Xcel proposed a matrix that uses a tiered-access approach to balance grid security with public benefits (Figure 24).[269] The matrix applies Xcel's "internal policy on information lifecycle management" to distribution grid data access to develop grid security risk levels.[270] These internal criteria put data into three categories based on the risk associated with disclosure of the data.

1. Unrestricted (U) – includes information that may or must be provided to the public, and internal company information where public disclosure is unlikely to cause harm.
2. Confidential Information (CI) – information where unauthorized disclosure has the potential to cause harm.
3. Confidential Restricted Information (CRI) – information where unauthorized disclosure has the potential to cause significant harm.[271]

These criteria are applied to the x-axis of the matrix. On the y-axis, a ranking of zero through three is applied based on the increasing benefit of public access to the data. In addition, each location on the matrix is given a label, which distinguishes whether the data is public, and assigns safeguards in

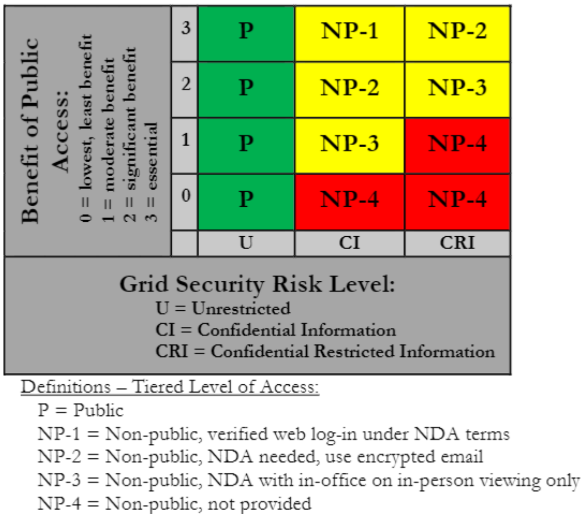
[269] Id., p. 16.

[270] Id, p. 10.

[271] Id., pp. 8-9.

proportion to the balance between grid security and public benefit. For example, data that is considered unrestricted and essential is public (U, 3, P). Conversely, data that is considered confidential restricted information, and which would create a significant benefit to the public, is provided only with an encrypted email and an NDA (CRI, 3, NP-2).

Figure 24: Xcel's Proposed Tiered-Access Framework



Benefit of Public Access:				
	3	P	NP-1	NP-2
	2	P	NP-2	NP-3
	1	P	NP-3	NP-4
	0	P	NP-4	NP-4
		U	CI	CRI

0 = lowest, least benefit
1 = moderate benefit
2 = significant benefit
3 = essential

Grid Security Risk Level:
U = Unrestricted
CI = Confidential Information
CRI = Confidential Restricted Information

Definitions – Tiered Level of Access:
P = Public
NP-1 = Non-public, verified web log-in under NDA terms
NP-2 = Non-public, NDA needed, use encrypted email
NP-3 = Non-public, NDA with in-office on in-person viewing only
NP-4 = Non-public, not provided

Source: Xcel 1.29.21 Comments on Distribution Grid Security and Customer Privacy, p.10.

In summary, the Minnesota utilities provide a tiered approach to sharing both customer and interconnection information. Customer energy information is shared based on customer consent, and interconnection information is shared using a series of security screens. Xcel has proposed using a matrix tool to assess data in a tiered-access framework.

5.5. Models for Data-Sharing in New York

5.5.1. Sharing Sensitive Customer Information

There are currently several models for sharing different types of information in New York. While each utility's DSIP outlines its specific plans for sharing data, the DSIP Order established the process by which utilities should share information.[272] Specifically, each utility with AMI was required to set a timeline for implementing Green Button Connect. Utilities without AMI were directed to identify other methods for sharing customer data with third parties. To date, the New York IOUs have struggled to implement

[272] NY DPS. *Department of Public Service Staff Whitepaper Regarding a Data Access Framework.* Case 20-M-0082. (May 29, 2020) p. 5.

Green Button Connect, with only three of the utilities currently utilizing it, and both data requestor and customer opt-in being minimal.[273]

The utilities are required to provide customer data for both municipalities and public use.[274] To support community choice aggregation, utilities provide municipalities with aggregated data, customer contact information, and detailed customer energy-usage data. For public use of customer data, the New York State Energy Research and Development Authority (NYSERDA) maintains the Utility Energy Registry (UER) with support from the utilities.[275] The UER is an online database platform that provides streamlined public access to aggregated, community-scale, utility energy data. Semi-annually, the utilities provide aggregated data for the platform and remove data that does not pass the privacy screens (e.g., 15/15 for residential customers, and 6/40 for nonresidential customers). This platform is considered a "starting point" for energy data access and is expected to evolve over time.[276]

5.5.2. Sharing System Information

In addition to each utility's hosting capacity map, each utility currently maintains one or more portals to share useful grid information. The New York PSC has determined that the types of system data that should be shared include:

- Distributed System Implementation Plans
- Capital Investment Plans (via the JU web site or the DPS DMM)
- Planned Resiliency/Reliability Projects (via the JU web site or the DPS DMM)
- System Reliability Statistics
- Hosting Capacity
- Beneficial Locations for DERs (partially available)
- System Load Forecasts (partially available)
- Historical System Load Data (partially available)
- Opportunities for Non-Wires Alternatives (partially available)
- Distributed Generation Queued for Interconnection
- Installed Distributed Generation
- System Interconnection Request (SIR) Pre-Application Information [277]

The Commission has directed the utilities to make all this information publicly available online. Currently, data requestors must visit each of the utilities' websites to access their data, but recently the

[273] Id., p. 6.

[274] Id., p. 5.

[275] NY DPS. *In the Matter of the Utility Energy Registry, Order Adopting Utility Energy Registry*. Case 17-M-0315. (April 20, 2018).

[276] NY DPS. Department of Public Service Staff Whitepaper Regarding a Data Access Framework. Case 20-M-0082. (May 29, 2020). p. 7.

[277] NY DPS. *Department of Public Service Staff Whitepaper Regarding a Data Access Framework.* Case 20-M-0082. (May 29, 2020). p. 9.

Commission ordered the creation of a centralized portal that would gather each of the utilities' information in one place.

5.5.3. Order Implementing an Integrated Energy Data Resource

The REV Track One Order in New York acknowledges the importance of data availability for the future adoption of DER and customers' management of their energy use.[278] This served as an essential motivation for the Commission's Order Implementing an Integrated Energy Data Resource (IEDR) in February 2021.[279] The IEDR will be a centralized online resource that "securely collects, integrates, and provides useful access to a large and diverse set of energy-related information on one statewide data platform."[280] Furthermore, the Commission ordered that the platform provide access to both standardized customer, and system energy data, while expanding useful access of such data to all types of entities. To date, NYSERDA has led the process, which has involved stakeholder collaboration with a broad range of input. A full list of the data items recommended by DPS for inclusion in the IEDR are listed in Appendix B of its White Paper.[281]

A main item which the DPS used to inform its decision on what information should be available was the creation of a minimum viable data set (MVDS). This dataset was built by a group of DER industry members and consultants in 2019, with input from DPS and NYSERDA. The group was called the DER industry group, and a main outcome of their collaboration was a report that summarized the "most basic set of utility-sourced information needed to accelerate DER market animation."[282] Table 21 shows the types of data included in the MVDS.[283]

Table 22: MVDS Data Categories and Elements

Grid Condition/Performance Data	Business Case/Market Data	Customer Data
System Elements	Distribution Network Value- Tariff	Customer Class
Hosting Capacity Analysis	Distribution Network Value - Non-Wires Solution	Tariff
Network Demand	Bulk Power Market Value	Bill
Voltage & Power Quality	Distribution Investment Plan	Interval Usage
Reliability Statistics	Other	Location

[278] NY DPS. *Reforming the Energy Vision, Order Adopting Regulatory Policy Framework and Implementation Plan.* Case 14-M-0101. (February 26,2015).

[279] NY DPS. *Order Implementing an Integrated Energy Data Resource*. Case 20-M-0082. (February 11, 2021).

[280] Id., p. 2.

[281] Id., Appendix B.

[282] NY DPS. *Department of Public Service Staff Whitepaper Recommendation to Implement an Integrated Energy Data Resource*. (May 29, 2020). p. 6.

[283] Id., p. 8.

Source: NY DPS Staff IEDR Whitepaper, p.8.

The report also noted that most of the data listed in Table 22 was already publicly available. However, the DER Industry Group emphasized that the needed information was only currently accessible though "disparate sources."[284] The group also stated that "the significant differences in the meaning, format, attributes, and integrity of their respective data is an inconsistency that presents a barrier to DER market animation as it severely hinders DER developers' ability to effectively and efficiently use the data that they obtain from those sources."[285] These comments, in part, motivated the Commission to order the IEDR be created as a single, all-encompassing platform with standardized information.

To guide the IEDR, a corresponding data access framework was released that provided an outline on how data would be accessed and detailed key terms and data quality standards.[286] NYSERDA recommended that the Commission adopt this framework in regards to the IEDR; however, the Commission required that the IEDR comply with a new data access framework that has yet to be released.[287] In the proposed framework, an entity seeking data would need to be certified as "data-ready." This certification would only be granted if the entity met all the requirements of the Commission, utilities, and DPS. With this certification, the entity would become an authorized energy service entity (ESE). Next, the entity would detail its "purpose for accessing the data, the mechanism by which the data are being accessed or transmitted, and the data type for which access is being requested."[288] The provider (a group processing the entity's request) would utilize a matrix to determine the requirements for accessing the requested data based upon these three conditions.[289]

Purpose: During this step, the provider would determine if the entity should have access to unconsented data. Valid purposes for access to unconsented data include: (1) providing or reliably maintaining customer-initiated service; (2) including compatible uses in features and services to the customer that do not materially change reasonable expectations of customer control and ESE data sharing; or (3) disclosure pursuant to Commission Order and/or State, Federal and Local Laws or regulations.[290] Entities with a Purpose that did not meet these conditions would receive anonymized or aggregated data.

[284] Ibid.

[285] Ibid.

[286] NY DPS. *New York Department of Public Service Department of Public Service Staff Whitepaper Regarding a Data Access Framework*. Case 20-M-0082. (May 29, 2020).

[287] NY DPS. *Order Implementing an Integrated Energy Data Resource*. CASE 20-M-0082. (February 11, 2021).

[288] NY DPS. *New York Department of Public Service Department of Public Service Staff Whitepaper Regarding a Data Access Framework*. Case 20-M-0082. (May 29, 2020). p. 23.

[289] Id., pp. 24-31.

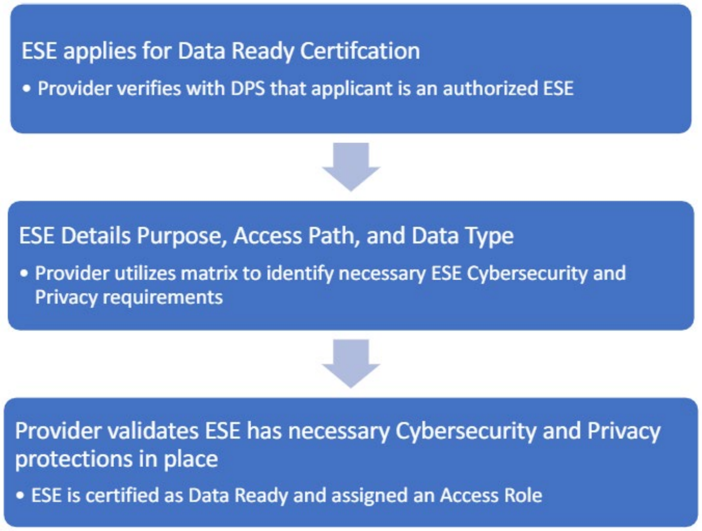
[290] Id., p. 24.

Transmittal or Access Mechanism: The provider would take into consideration how the data will be accessed or transmitted. This could be as simple as an email or it could involve access through a secure portal/platform. Ultimately, it is up to the provider to determine how the entity will access the data.

Data Type Requested: The type of data requested by an entity will determine the necessary privacy requirements. DPS outlines a risk-based approach based on the risk associated with releasing sensitive data and maintains the customers right to share their data. Furthermore, data is broken into two categories: (1) system data and (2) customer data. Customer data would include customer contact information, CEUD, and billing data. System data would include information about the components and activity on the distribution system. Notably, the framework is clear that for "system data, except for those pieces of system data that may impact customer privacy or critical infrastructure protection, there should be no protections on the availability of such data because it is aggregated data itself. Since it is not CEUD, it is not subject to customer consent."[291]

Once the matrix has been used to determine the necessary steps and protections, the entity would receive an access role which would determine the types of data they could access, and how they could access it. Figure 25 outlines this process.[292]

Figure 25: Data Ready Certification Process


ESE applies for Data Ready Certifcation
• Provider verifies with DPS that applicant is an authorized ESE
ESE Details Purpose, Access Path, and Data Type
• Provider utilizes matrix to identify necessary ESE Cybersecurity and Privacy requirements
Provider validates ESE has necessary Cybersecurity and Privacy protections in place
• ESE is certified as Data Ready and assigned an Access Role

Source: NY DPS Staff IEDR Whitepaper, p.31.

A Pilot Data Platform, like the IEDR, has been launched with the Orange and Rockland Utility. The platform automates the process for providing data to DER developers, among other functions, and the

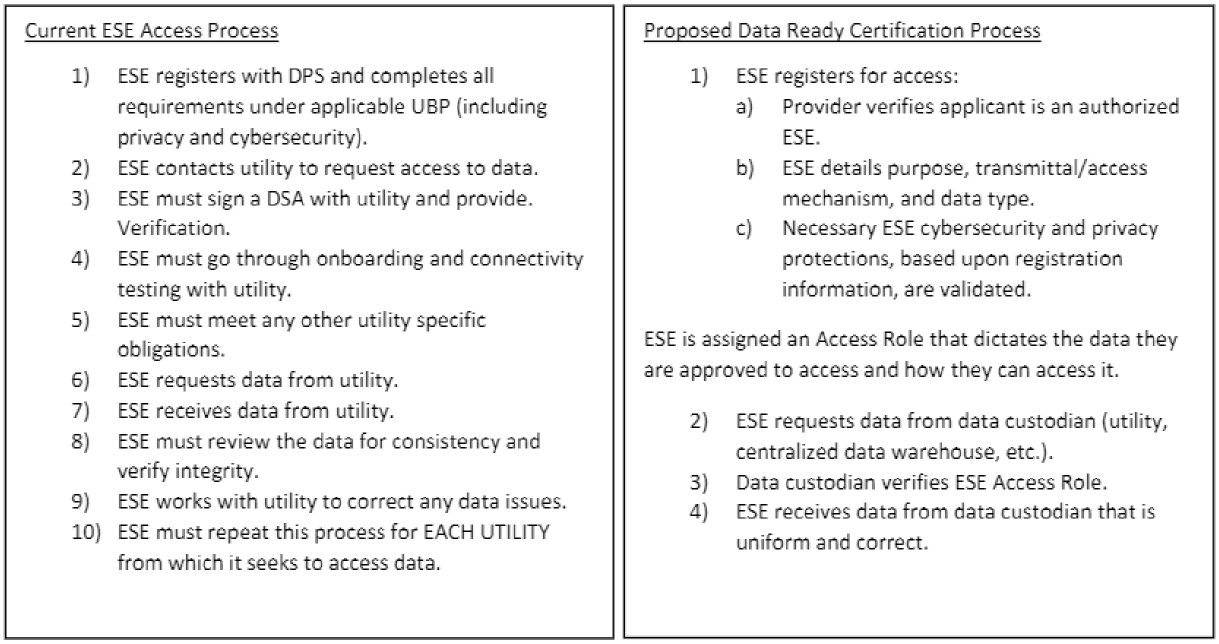
[291] Id., p. 31.

[292] Ibid.

development and rollout of the platform costs $240,000.[293] To obtain access to the Pilot Data Platform, a DER provider "must be registered with the DPS, comply with the applicable Uniform Business Practices provisions, and complete and submit the DER Provider Pilot IEDR Registration Form."[294] The pilot's early results have been positive.[295] Lastly, the IEDR will be implemented over 2 phases.[296] Phase 1 has a total budget cap of $13.5 million and will include designing, implementing, and managing the IEDR. Phase 2 does not yet have a budget and will include further improvements to the IEDR.

Figure 24 summarizes the differences between the current model in New York, and the new one outlined in the proposed Data Access Standards.[297]

Figure 26: Proposed vs. Current Data Access Framework in New York



Current ESE Access Process

1) ESE registers with DPS and completes all requirements under applicable UBP (including privacy and cybersecurity).
2) ESE contacts utility to request access to data.
3) ESE must sign a DSA with utility and provide. Verification.
4) ESE must go through onboarding and connectivity testing with utility.
5) ESE must meet any other utility specific obligations.
6) ESE requests data from utility.
7) ESE receives data from utility.
8) ESE must review the data for consistency and verify integrity.
9) ESE works with utility to correct any data issues.
10) ESE must repeat this process for EACH UTILITY from which it seeks to access data.

Proposed Data Ready Certification Process

1) ESE registers for access:
   a) Provider verifies applicant is an authorized ESE.
   b) ESE details purpose, transmittal/access mechanism, and data type.
   c) Necessary ESE cybersecurity and privacy protections, based upon registration information, are validated.

ESE is assigned an Access Role that dictates the data they are approved to access and how they can access it.

2) ESE requests data from data custodian (utility, centralized data warehouse, etc.).
3) Data custodian verifies ESE Access Role.
4) ESE receives data from data custodian that is uniform and correct.

Source: NY DPS Staff IEDR Whitepaper, p.18.

In summary, New York is in the process of developing a resource that would streamline the process for accessing information. While the creation of the IEDR is still very much a work in progress, the reasons for its development are apparent. By streamlining the data release process, the NY PSC seeks to lessen

[293] NY DPS. Department of Public Service Staff Whitepaper Recommendation to Implement an Integrated Energy Data Resource. Case 20-M-0082. (May 29, 2020) pp. 5-7.

[294] NY DPS. "Distributed Energy Resource Regulation and Oversight." Available at: https://www3.dps.ny.gov/W/PSCWeb.nsf/All/EAB5A735E908B9FE8525822F0050A299.

[295] NY DPS. *Department of Public Service Staff Whitepaper Recommendation to Implement an Integrated Energy Data Resource.* (May 29, 2020), p. 8.

[296] Order Implementing an Integrated Energy Data Resource. Case 20-M-0082. (February 11, 2021). pp. 15-22.

[297] NY DPS. *New York Department of Public Service Department of Public Service Staff Whitepaper Regarding a Data Access Framework*. (Case 20-M-0082). (May 29, 2020), p. 18.

the burden of collecting interconnection data and decrease the number of times utilities must go through data access protocols with third parties.

5.6. Models for Data-Sharing in California

5.6.1. Sharing Sensitive Customer Information

The CPUC's Order on September 23, 2013, authorized third-party access to customer energy data to "provide higher quality, standardized data to encourage the market for DERs."[298] The order required third parties that requested data to be pre-approved by utilities as a trusted vendor. This allowed groups such as developers to become a trusted vendor, request access to a specific customer's data, and then tailor their offer to the needs of that customer. As described by the DPS, this order increased the "value of potential products" and maximized "the value derived from these DERs."[299]

In 2014, the CPUC released its Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data While Protecting Privacy of Personal Data (Rulemaking 08-12-009).[300] In its ruling, the CPUC explained that access to energy data can advance policy goals and it explicitly listed seven goals including the "deployment and integration of cost-effective distributed resources and generation, including renewable resources."[301]

In addition to identifying goals, the order established a tiered-access approach to customer information within California. Government entities and academic researchers were allowed access to anonymized data, while other groups were granted access to aggregated data without customer consent. The CPUC also detailed a process for requesting and releasing customer energy data.[302] It included requiring a single point of contact for energy data requests, requiring the utilities to publish a list of all requests and their purpose, and establishing a clear timeline for the utility's response to data requests. Entities seeking access to data are also required to provide their purpose for accessing data; a description of the data requested; an address, name, and phone/email; and are required to execute a standard NDA (apart from local governments on certain conditions). Finally, the Order established an Energy Data Access Committee and standard formats and mechanisms for utility data release. Today, one of the ways in which third-party data is authorized for release is through the "click-through authorization process,"

[298] NY DPS. *Department of Public Service Staff Whitepaper Recommendation to Implement an Integrated Energy Data Resource*. Case 20-M-0082. (May 29, 2020). p. 20.

[299] Ibid.

[300] NY DPS. *Decision Adopting Rules to Provide Access to Energy Usage and Usage-Related Data While Protecting Privacy of Personal Data.* Decision 14-05-016. (May 1, 2014).

[301] Id., p. 21.

[302] Id., Attachment A, p. 1.

which allows customers to easily authorize their utility to share their energy data with third parties.[303] The California IOUs recently proposed improvements to the process including expanding it to bring in DER and energy management providers, improving data delivery, and delivering data within 90 seconds. The potential benefits of the proposal include streamlining the processes for: (1) customers to authorize service providers to access their data and (2) utilities to transfer customer data quickly and efficiently to such authorized DER and energy management service providers.[304] The Commission is expected to decide on the utilities' proposals in early 2021.

5.6.2. Sharing System Information

Each of the California IOUs have a web portal which gives access to several types of information including the hosting capacity maps which have been discussed. For example, PG&E offers a Distribution Investment Framework (DIDF) map and a PV RAM map. PG&E describes the use of the DIDF map as a location to "show assumptions and results of the distribution planning process that yield grid needs related to distribution grid services," while the purpose of the PV RAM map is to show selected electric distribution lines, substations, and transmission lines paired with general electric system information.[305] For PG&E, both maps require user registration. Similarly, SDG&E requires registration to access its ICA map (which includes a locational net benefits layer).[306] SCE takes a slightly different approach. On its interactive portal, it provides the following information:

- General locations of SCE distribution circuits, substations, sub-transmissions systems;
- Load and DER Integration Capacity Analysis (ICA) results (e.g., hosting capacity);
- Current, queued, and total distributed generation interconnections amounts;
- Downloadable datasets for DER developers, with Application Programming Interface (API) capabilities;
- Locational Net Benefit Analysis (LNBA) results; and
- Grid Needs Assessment (GNA), Distribution Deferral Opportunity Report (DDOR).[307]

In addition to maps, utilities in California follow an interconnection process known as Rule 21 to help developers connect DERs to the grid. Each IOU is responsible for implementing an interconnection

[303] Kim, Anne Y. 2021. California's Grid Modernization Report to the Governor and Legislature. CPUC. p. 64.

[304] Ibid.

[305] PG&E. "Distribution-Resource Planning Data Portal." Available at: https://www.pge.com/en_US/for-our-business-partners/distribution-resource-planning/distribution-resource-planning-data-portal.page?ctx=large-business.

[306] SDG&E. "Accessing the Map." Available at: https://www.sdge.com/more-information/customer-generation/enhanced-integration-capacity-analysis-ica.

[307] SCE. *Integration Capacity Analysis (ICA) User Guide.* Available at: https://ltmdrpep.sce.com/drpep/downloads/ICAUserGuide.pdf.

procedure in Electric Rule 21 as established in Interconnection Rulemaking (R.17-07-007).[308] By having a robust ICA map, both utilities and developers can move through the interconnection process more swiftly. In some ways, the process is very similar to the MN DIP process. It includes an optional Pre-Application Report for additional system information, and the potential release of CEII information during the interconnection process. The applicant may also be required to sign an NDA.[309] Similar to Minnesota, this represents a tiered-access approach to information sharing. Additional information is supplied to the developer during the interconnection process to help streamline DER development.

In summary, California utilizes a tiered-access system to release both interconnection and customer data. However, California provides a considerable amount of information in support of DER deployment early in the pre-interconnection process, which helps to accelerate DER interconnection.

5.7. Models for Data-Sharing in New Hampshire

New Hampshire, similar to New York, is in the midst of a proceeding that would establish an online energy data platform to provide a variety of energy-use information to ratepayers, third parties, and IOUs.[310] The State's Office of Consumer Advocacy has proposed six core use datasets including, "billing, [time-of-use], demand study, multi-state and utility, multi-fuel, and a Statewide index, the last dataset referring to the idea that the SB284 platform will act as a single source of truth for all electricity and other fuel information in the State."[311] The platform intends to incorporate a tiered-access system. The New York DPS has noted that it is "monitoring this proceeding closely to ensure that the state will be able to exchange lessons learned to encourage the adoption of these platforms in both states," as the potential New Hampshire platform is very similar to the in-progress IEDR in New York.[312]

5.8. Comparison of Energy Access Platforms

Table 23 reviews and compares some of the fundamental elements incorporated into each state's energy access platforms. All the states discussed, use some form of tiered access to release standardized data to third parties. One notable difference between the states is the recent development of single-access platforms. While both New Hampshire and New York have not fully implemented a single-access platform, both seek to streamline the process of data-sharing by limiting the number of locations where data is stored.

[308] CPUC. "Rule 21 Interconnection." Available at: https://www.cpuc.ca.gov/General.aspx?id=3962.

[309] PG&E. *Electric Rule No. 21: Generating Facility Interconnections.* p. 89. Available at: https://www.pge.com/tariffs/assets/pdf/tariffbook/ELEC_RULES_21.pdf.

[310] Ibid.

[311] Ibid.

[312] Ibid.

Table 23: Overview of Energy Access Platforms

State	Standardized Data	Single Access Platform	Tiered Access
Minnesota	Established in the November 2020 Order	No	Tiered access to customer data based on customer consent and MN DIP process with increased security for CEII information.
New York IEDR	Data will be standardized in the IEDR	Yes	Proposed data-access framework uses a matrix to determine what level of information is shared with a requesting party.
California	Utilities use or model their data standards like Green Button Connect	No, each utility has a website	Increased security for CEII information and segmented aggregation screens for customer information.
New Hampshire (Proposed)	Data will be standardized	Yes	The platform intends to incorporate a tiered-access system.

5.9. Guiding Principles for Tiered Access

After reviewing the various practices used by states for releasing information to third parties, we recommend that the Commission consider the following two recommendations.

Firstly, the Commission should consider a risk-based, tiered-access approach that transparently shares energy data. Each case study discussed provided criteria for restricting access to highly sensitive information. While we do not necessarily recommend the tiered-access approach as proposed by Xcel, we do recognize that having protections in place for highly sensitive information should be required. We also recommend that the criteria for evaluation be transparent and that the development of such criteria include an array of input from a diverse group of stakeholders.

Secondly, we recommend that the Commission consider approaches that expedite the process for accessing data. As described in Section 5.5, the process proposed in New York by which entities become "data ready" and receive an "access role" could expedite data access for all parties involved. In the case of Minnesota, parties that repeatedly interconnect could save time by only being screened for security requirements on an annual basis. Establishing this user access role could increase the security for sharing data but the user registration process should not be overly burdensome for the parties involved.

6. Recommendations

Striking the right balance between Xcel's grid and customer security and confidentiality concerns around publishing sensitive hosting capacity map data and the public benefits in having access to this information to increase DER deployment can be challenging.

Synapse developed the recommendations below to help Minnesota find that balance. To develop them, we worked with the Department to host two stakeholder workshops on grid and customer security; conducted an extensive literature review; benchmarked the hosting capacity data-sharing practices of leading utilities in this space; sent a survey to Minnesota DER developers and other interested parties; and spoke with utility representatives and risk management experts. As a result of Synapse's findings, our recommendations regarding the privacy and security implications of Xcel's HCA and public-facing map are as follows.

In the short-term, we recommend the Commission take the following actions:

- Allow Xcel to only redact load data when a feeder violates the 15/15 aggregation standard and require Xcel to publish on its map, and in its tabular spreadsheet, all other HCA data.
- Require Xcel to create a transparent process for how third parties can access CEII, on a "need-to-know" basis, with appropriate protections (e.g., NDA) in place.
- Allow Xcel to only redact feeders included in the HCA if they satisfy one or more of the following criteria: (1) are connected to a dedicated customer or (2) are connected to critical infrastructure or serve a critical customer.
- Require Xcel to provide more detailed rationale (e.g., beyond "security concern") for justifying not publishing feeder and substation capacities.

In the longer-term, we recommend the Commission take the following actions:

- Require Xcel to provide an unblurred HCA map, which shows its distribution feeders, behind a verified web login portal that is open to the public (e.g., does not require an NDA).
- Encourage Xcel to consider a tiered-access approach that helps streamline and does not make requirements to access non-public grid data unnecessarily burdensome.
- Encourage Xcel to engage in a transparent, Risk-Benefit/Cost-Benefit Framework stakeholder process to help determine whether specific, sensitive grid data should be published on its HCA map, and how secure access to sensitive grid data, deemed non-public, should be provided.
- Require Xcel to estimate the level of effort and cost to incorporate each specific piece of data in the Pre-Application Report that is currently not in the HCA map, where technology requirements (e.g., querying and search functionality) rather than security concerns are the limiting factor (e.g., distance from site to substation).

These recommendations should help to balance the grid and customer security concerns and data access requirements of all parties involved.

7. Conclusion

Hosting capacity maps provide information that benefits a wide range of users. Use cases for these maps range from helping developers interconnect DERs to providing locational information to industry advocates who wish to increase the amount of DERs deployed on the grid for the public good. As regulators seek to support these use cases, there has been a noticeable shift throughout the United States towards increasing the amount of information available on hosting capacity maps. Seven states already have functioning hosting capacity maps, while five more are significantly enhancing the functionality of their maps.

As states continue to increase the data provided on their hosting capacity maps, they must determine what information should be publicly disclosed. For example, some information like CEUD or CEII may be confidential. States have employed a range of strategies to protect this type of information. These strategies have included redacting critical information, aggregating customer data, and developing tiered-access systems that provide access to sensitive information with appropriate protections in place. Furthermore, frameworks such has the Risk-Benefit Framework can be used to weigh the benefit of public data release with the risk of its misuse. It is important to develop a transparent model that allows for the robust sharing of information. States such as New York, California, and New Hampshire have all taken steps to ramp up the ease of accessing data while balancing the need for its security.

Minnesota is currently in the process of increasing the information displayed on its hosting capacity map. The lessons learned and recommendations discussed in this report are designed to help Minnesota regulators make informed decisions based on current industry standards and practices. By employing an appropriate model for information sharing, Minnesota will be able to balance its ability to support increasing amounts of DERs on the grid with the need to protect grid and customer security.

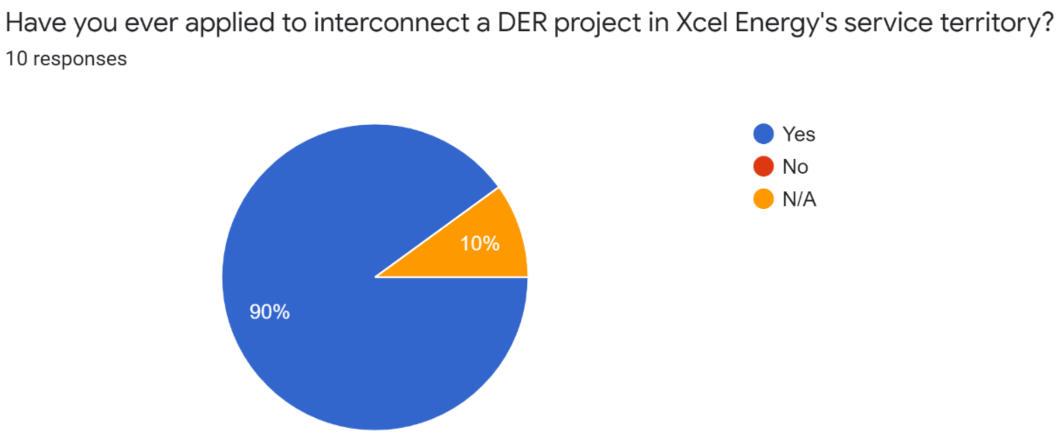
APPENDIX A. Pre-Application Report Data

Table A.1 compares the information currently provided in Xcel Energy's Pre-Application Report with the information contained in its hosting capacity analysis in both map and tabular formats.

Table A.1. Comparison of Pre-Application Report data elements with HCA

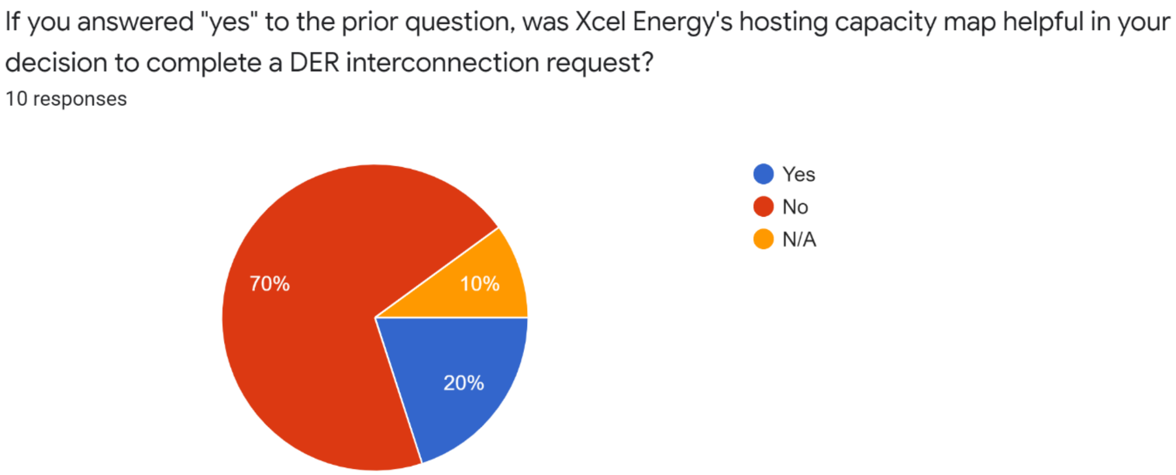
Pre-application Data Element	Information Available on Map	Information Available in Tabular Format	Notes
Substation Name	Yes	Yes	N/A
Transformer Name	Yes	Yes	N/A
Transformer Rating	No	No	Privacy/Security Concerns
Transformer Peak	No	No	Privacy/Security Concerns
Transformer DML	Yes	Yes	N/A
Transformer Absolute Min	Yes	Yes	N/A
LTC or Regulator	Yes	Yes	N/A
Transformer Existing Gen	Yes	Yes	N/A
Transformer Queued Gen	Yes	Yes	N/A
Transformer Gen Capacity	No	No	Security concerns and significant technology requirements; equation would need to be implemented within the map or prior to map creation
Distance from site (PCC) to substation	No	No	Significant technology requirements; query function would need to be built into Hosting Capacity Map
Feeder Name	Yes	Yes	N/A
Feeder Rating	No	No	Privacy/Security Concerns
Feeder Peak	No	No	Privacy/Security Concerns
Feeder DML	Yes	Yes	N/A
Feeder Absolute Min	Yes	Yes	N/A
Feeder Voltage	Yes	No	N/A
Feeder Existing Gen	Yes	Yes	N/A
Feeder Queued Gen	Yes	Yes	N/A
Feeder Gen Capacity	No	No	Security concerns and significant technology requirements; equation would need to be implemented within the map or prior to map creation
Nominal Voltage at PCC	Yes	No	N/A
Network or Radial	Yes	Yes	N/A
# of Phases	Yes	No	N/A
Distance to 3 phase circuit	No	No	Significant technology requirements; query function would need to be built into Hosting Capacity Map
Protective devices and regulators between site and substation	No	No	Security concerns and significant technology requirements; query function would need to be built into Hosting Capacity Map
Conductor between site and substation	No	No	Security concerns and significant technology requirements; query function would need to be built into Hosting Capacity Map

APPENDIX B. Developer Survey Results



Have you ever applied to interconnect a DER project in Xcel Energy's service territory?

10 responses



If you answered "yes" to the prior question, was Xcel Energy's hosting capacity map helpful in your decision to complete a DER interconnection request?

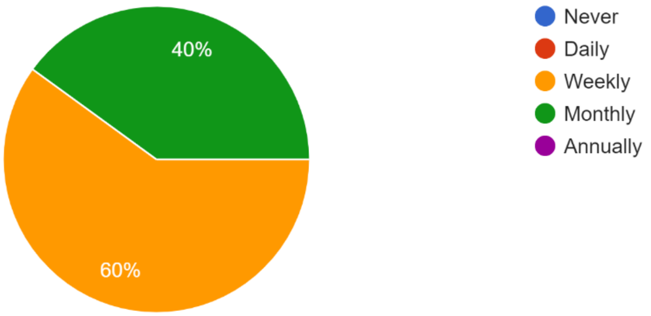
10 responses

If you answered “yes” to the prior question, please explain what you used the hosting capacity map for and what value it provided. (4 responses)

1. We utilized the map to identify the size and scope of a project which could be interconnected at the selected location.
2. We used it to help indicate capacity, but it never seems to be up-to-date and the capacity available seems to inconsistently change.
3. I used the map, but it was so old that I did NOT trust the data.
4. To see if my project would fit or if the grid was at capacity.

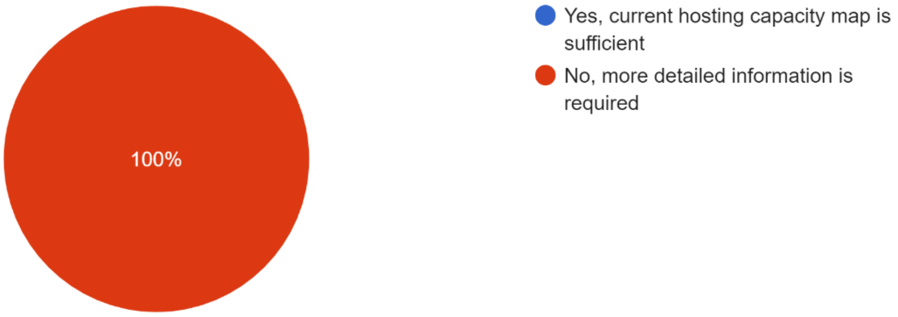
How often do you use Xcel Energy's hosting capacity map?

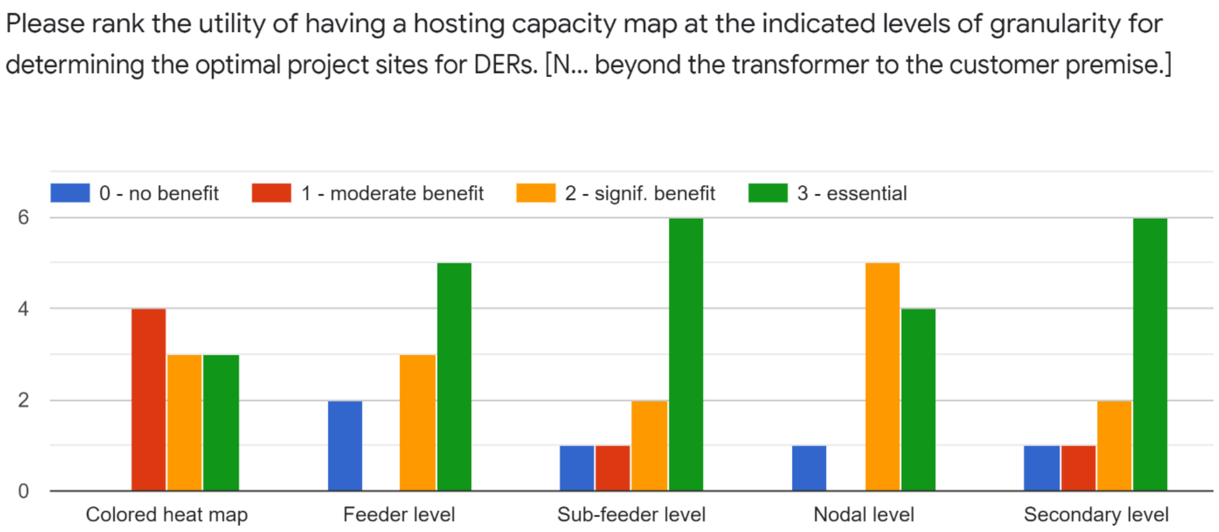
10 responses



Is the current hosting capacity map sufficient to meet DER developers needs or does it require more detailed information?

10 responses





Please rank the utility of having a hosting capacity map at the indicated levels of granularity for determining the optimal project sites for DERs. [N... beyond the transformer to the customer premise.]

Please explain your rationale behind the designations you chose in the prior question. (10 responses)

1. As detailed of information as possible is essential to ensuring we can accurately and efficiently develop projects. Other regions and utilities have extraordinarily more detailed data than Xcel, which provides a significant benefit to DER development.

2. Sub-feeder level data is the basic level of data needed to make informed decisions about siting DER. Nodal level would be even more powerful and would enable utilization of an actual value-based approach to DER siting, such as true locational marginal pricing. Secondary level would provide an even stronger level of clarity about capacity, but these benefits are limited as compared to Nodal level data and could dramatically increase the complexity of analysis.

3. Customers need to be able to trace the power lines from a specific address to a specific node where hosting capacity analysis data are provided. Without being able to trace a line from an address to the node with hosting capacity data, the map does not give all customers data necessary to optimally design and site DERs.

4. The more we know the better to get good projects sited.

5. All of this information is HIGHLY valuable but totally useless if 16+ months old...

6. More granularity would help avoid surprise charges for customers that want to have solar.

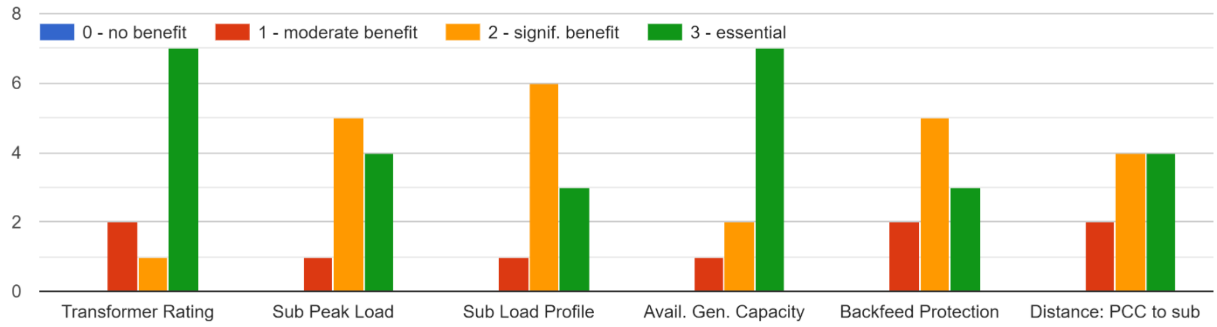
7. We need to know at the customer level if they can have net metered DER.

8. I use it for behind-the-meter projects, so it's nice to know what you're gonna be up against early on in the project. The most useful information to me is existing transformer size, voltage/phase, and secondary conductor size.

9. Information was inaccurate beyond a very general level.

10. Most of the needed content is there, it just needs to be updated more often. We view displaying substation transformer size as being critically important, however we understand there are potentially security issues with doing that as well as other formal methods to acquire that information.

Please rank the importance of having the following grid data available on a hosting capacity map for determining the optimal project sites for DERs at the substation level...tation, Gen = generation, PCC = point of common coupling]



Please explain your rationale behind the designations you chose in the prior question. (10 responses)

1. As detailed of information as possible is essential to ensuring we can accurately and efficiently develop projects.

2. All of this data is highly valuable for planning DERs. Without transformer ratings, peak load, and Available Generation Capacity, you can't really do much. The other piece of information that feels key is Minimum load/ daytime load.

3. The substation data listed is essential to determining if the substation can support additional DERs. Providing substation data is particularly important because Xcel's hosting capacity analysis does not currently evaluate substation constraints.

4. We need to know how much electricity can flow and where how etc.

5. This would significantly increase our ability to assess out projects and give the community we serve an accurate idea of what they're in for.

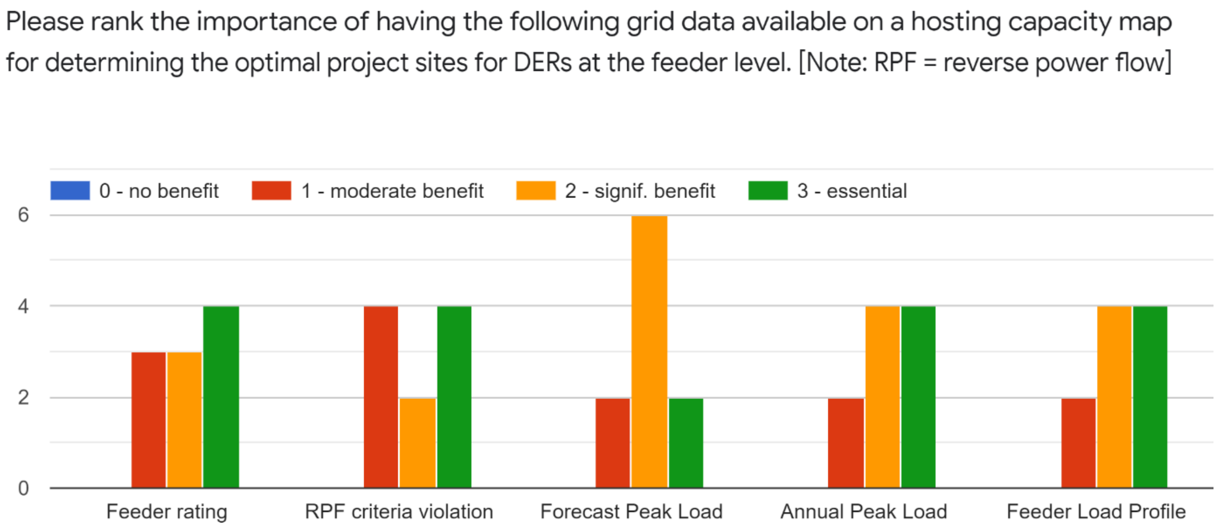
6. N/A to my projects - you should invalidate my responses to the previous question as this form would not let me submit without putting something on each line.

7. Knowing the limits allows for better design considerations on our end.

8. The main one is transformer size. That comes into play more often than the rest of them but still all are helpful.

9. Initial screening is the only utility from the system at the current time.

10. If the available generation capacity was able to be trusted, that would be essential, but as of now we pretty much ignore it. The more information provided up front, the fewer questions we will have tying up Xcel's time and higher quality projects we will be attempting to push through.



Please rank the importance of having the following grid data available on a hosting capacity map for determining the optimal project sites for DERs at the feeder level. [Note: RPF = reverse power flow]

Please explain your rationale behind the designations you chose in the prior question. (10 responses)

1. As detailed of information as possible is essential to ensuring we can accurately and efficiently develop projects.

2. All of this data is extremely valuable. Without the essential items, you can't really do much.

3. Criteria violations and load profiles are essential to understanding how to design projects to avoid certain constraints, both technologically and temporally.

4. See above.

5. Again - this is all crucial info!

6. N/A to my projects - you should invalidate my responses to the previous question as this form would not let me submit without putting something on each line.

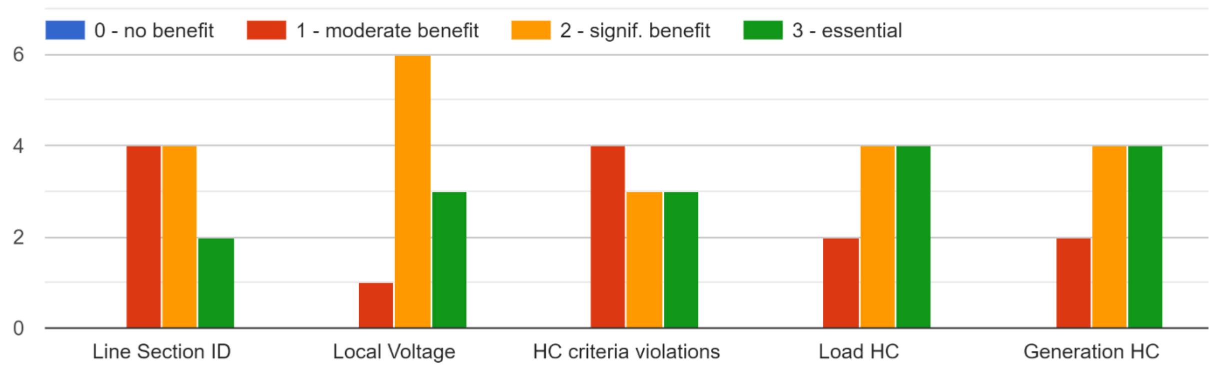
7. Knowing the limits allows for better design considerations on our end.

8. At this time, I see less benefit from these attributes but still very valuable information.

9. Would establish a threshold for further due diligence.

10. This information is more helpful to BESS decisions, and we have not engaged in such a system in this market as of yet.

Please rank the importance of having the following grid data available on a hosting capacity (HC) map for determining the optimal project sites for DERs at the sub-feeder/line level.



Please provide a detailed explanation of your rationale behind the designations you chose in the prior question. (10 responses)

1. As detailed of information as possible is essential to ensuring we can accurately and efficiently develop projects.

2. The last three items help define the key opportunity and constraints at the sub-feeder level. ID of line sections and local voltage information is extremely valuable, but not quite as key.

3. Criteria violations and load profiles are essential to understanding how to design projects to avoid certain constraints, both technologically and temporally.

4. See above.

5. Meh - this is pretty far in the weeds for a rooftop installation. We don't do the large fields.

6. Local voltage would help projects move more quickly.

7. Knowing the limits allows for better design considerations on our end.

8. At this time, I see less benefit from these attributes but still very valuable information.

9. These issues can be largely addressed by interconnection upgrades.

10. These in conjunction with the public queue and other sourced data help complete a full picture of an interconnection scenario so that we aren't submitting projects directly into a woodchipper.

In addition to the information above, are there any other grid data that would be useful for inclusion in the hosting capacity map? Please explain.

1. Visibility into the scope and potential budget required to upgrade a given location for a given project or project range would be significantly helpful, even if the data was an estimate or range pending final quoting and confirmation.

2. When do we transition from asking "how much solar can fit on the existing system" to asking "how do we build a system based on solar"?

3. Transformer secondary voltage and phase, and secondary conductor sizing.

4. More general information on the status of other distributed generation projects in the queue; schedule for grid improvements, if any, based on the approved Integrated Distribution Plan.

5. More clarity on existing protective devices and the listed limiting element that restricts further capacity would be nice. Maybe if transformer ratings cannot be disclosed, then classify the substation on the HCM into ranges like (10 MVA-20 MVA), specially to identify the smaller substations that have like a 3 MVA transformer, and the large substations that can likely take on a great deal more projects even though it may appear saturated.