PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Secure Sharing of Electric Distribution Grid Data

Dr. Paul N. Stockton
January 29, 2021

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Table of Contents

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

SECURE SHARING OF ELECTRIC DISTRIBUTION GRID DATA

Dr. Paul N. Stockton[1]

January 29, 2021

I. EXECUTIVE SUMMARY

Conflicts are deepening between two crucial goals: increasing the availability of grid data and protecting that data from foreign and domestic threats. To accelerate the development of small-scale distributed energy resources (DER) for Minnesota, and the achievement of carbon-free power generation in the State, energy developers need data on interconnection points and other information to help them develop and advance DER project proposals. But Russia and other potential adversaries seek detailed grid data as well. Their goal: develop attack plans that exploit specific points of vulnerability in the systems that distribute power to hospitals, water systems, and other facilities on which Minnesota's people and economy depend.

The Minnesota Public Utilities Commission (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" related to Docket Nos. E999/CI-20-800 and E002/M-19-685.[2]

The Commission's focus on these issues is timely and important. A number of other US State public utility commissions have issued regulatory guidelines and requirements for distribution utilities to share detailed information on their systems. However, none of these initiatives account for the increasingly severe threats to the grid posed by foreign nations and domestic terrorists, or for the risk that adversaries will exploit specific types of data to help design their attacks. Nor have any other State commissions established risk management frameworks to help them strike a balance between goals of data sharing and data protection and guide the development of risk mitigation measures that meet the priorities of both energy developers and utilities. The request for comments provides an opportunity for the Commission and grid stakeholders to reach consensus on how to fill these gaps in ways that best meet the needs of the State of Minnesota.

[1] Dr. Stockton provides strategic advisory services to Xcel Energy. Appendix A of this document summarizes his professional expertise on grid security.
[2] 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.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

The analysis that follows is structured to address the specific topics featured in the Commission's request. Key findings and recommendations:

Risks to grid security posed by expanded release of grid data. The Request for Comments asked: "What are the electric distribution grid and customer security issues related to public display or access to grid data; such as, distribution grid mapping, aggregated load data, and critical infrastructure?" Section II of these comments draws on the *National Counterintelligence Strategy of the United States, 2020-2022* and other authoritative US cyber threat assessments to explain why potential foreign adversaries seek to hold grid infrastructure at risk. This section also examines why these adversaries may selectively attack substations and other distribution infrastructure in Minnesota, either separate from or in conjunction with an attack on the Bulk Power System (BPS), due to devastating effects such attacks could have on Level 1 hospitals, water systems, and other facilities essential for public safety and the economy.

Domestic violent extremists can threaten the distribution grid as well. In particular, these terrorists may conduct physical attacks with high explosives and other kinetic weapons to cut off power to specific facilities, or – through coordinated attacks on multiple distribution substations – seek to create wide area, long duration blackouts. Section II reviews recent domestic attacks against grid infrastructure and emerging kinetic threats. This Section also analyzes how access to specific types of grid information, including feeder locations and maximum load data, can help foreign adversaries and domestic terrorists plan and execute their attacks.

Categorizing Sensitive Information. Based on emerging threats and adversary opportunities to exploit distribution grid data, Section III recommends that Commission and grid stakeholders build on existing criteria to identify Critical Electric Infrastructure Information (CEII) and modify those criteria to meet circumstances and goals specific to Minnesota. One promising option: modify the criteria developed for the BPS to fit Minnesota's distribution system needs. The BPS data protection requirements established by the North American Electric Reliability Corporation (NERC) apply only to that system, and not to the distribution grids that fall under State regulatory authorities. Nevertheless, rather than start from scratch, the Commission and grid stakeholders should explore how they could modify the BPS' CEII criteria and other existing data security models to serve Minnesota's needs.

Use Cases. Assessing the possible consequences of attacks on Minnesota's distribution grid can help clarify the stakes involved in the release of sensitive data. In particular, such consequence-based analysis can provide valuable context for efforts by the Commission and grid resilience stakeholders (including emergency management officials and critical facility operators) to strike a balance between the goals of giving energy developers expanded access to data and keeping that data out of the hands of potential attackers. Xcel Energy is providing under separate cover Appendix B, an example of how the cutoff of grid-provided power to a specific Twin Cities facility

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

could inflict catastrophic effects on public health and safety. Section IV proposes how the Commission can employ such consequence-informed analysis to help assess the risks of releasing sensitive data. This section also proposes the development of additional, stakeholder-led use cases that will help the Commission balance security goals with other objectives related to expanded access to sensitive data.

Risk Management Framework. Section V proposes the development of a framework for the Commission and grid stakeholders to use in evaluating the risks, costs, and benefits of providing access to electric distribution grid data publicly. The framework would be built around stakeholder assessments of (1) the types of data and level of detail most important to energy project developers, and (2) the potential consequences to Minnesota's population and economy if adversaries exploit that data to help plan and execute attacks on the distribution grid.

Models for Reconciling Information Sharing with Protection of Sensitive Data. Borrowing from existing models that limit the distribution of sensitive data, Section VI proposes a tiered access system to reconcile the competing goals of expanded information sharing with the protection of such data from foreign adversaries. Under the proposed system, energy developers would have access to data of greater sensitivity than the general public. Developers might also enter into voluntary Non-Disclosure Agreements (NDAs) with Xcel Energy and other utilities that specify the terms under which developers will use and protect sensitive data. These initiatives would require input from developers, as well as utilities and other stakeholders, to achieve consensus on such voluntary arrangements and broader strategies for tiered access.

Future Workshops. Section VII strongly recommends that the Commission host a workshop on information sharing and security. As noted above, developers and other stakeholders will be critical to developing tiered access concepts. Stakeholder participation will be equally important for reaching consensus on all of the other initiatives proposed in these comments. Fresh Energy, the Interstate Renewable Energy Council, Inc (IREC), the Edison Electric Institute, Xcel Energy, and other associations and utilities will have valuable insights on criteria for designating CEII, and for developing a risk management framework that reflects their information priorities. Important perspectives on grid security can also be provided by entities responsible for managing the consequences of severe distribution-level outages, including:

- Minnesota State, local, and tribal government agencies, including those responsible for homeland security and emergency management;
- Law enforcement, fire departments, and other public safety organizations;
- Operators of major hospitals, water systems, financial institutions, data centers, and other critical distribution system customers; and
- The Midwest Reliability Organization (MRO), which helps maintain the reliability of the region's BPS.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Section VII recommends how the Commission might structure a workshop that brings these and other stakeholders together to build consensus on how to expand access to grid data while also protecting that data from foreign adversaries and domestic threats.

II. EMERGING THREATS AND IMPLICATIONS FOR DATA PROTECTION

Xcel Energy's filing on "Hosting Capacity Analysis – Security and Confidentiality Considerations" noted that "the electric grid is both highly vulnerable to attack and attractive to potential adversaries due to the dependence of all other critical infrastructures on it."[3] In 2020, the Federal government provided new information on threats to the grid from Russia, China, and other nations designated by the Department of Energy (DOE) as "foreign adversaries."[4] The Federal government has also provided detailed assessments concerning the goals that adversaries seek by gathering data on US electric system topologies and other characteristics, implanting malware on critical electric infrastructure, and taking additional measures to prepare for possible attacks on the grid.

These assessments of foreign threats provide a foundation for assessing the potential risks of expanded data disclosures on Minnesota's distribution systems. Such assessments can also help Commissioners and grid stakeholders develop measures to mitigate these risks in ways that facilitate DER projects and help achieve other Commission goals.

A. FOREIGN ADVERSARY GOALS FOR GATHERING GRID DATA AND CONDUCTING OTHER "PRE-CYBERATTACK" OPERATIONS

Russia's SolarWinds attack is only the most recent example of aggressive, sophisticated adversary efforts to gain access to critical US data and networks. The Department of Homeland Security's (DHS) Cybersecurity & Infrastructure Security Agency (CISA), has stated that this advanced persistent threat poses a "grave risk" to government and critical infrastructure entities.[5] CISA notes that the adversary's initial objectives are "to collect information from victim environments."[6] But Suzanne Spaulding, the former head of cybersecurity for DHS, warns that Russian objectives "may

[3] Docket No. E002/M-20-812, *In the Matter of Xcel Energy's 2020 Hosting Capacity Analysis Report*, Initial Filing – Hosting Capacity Analysis Report, Attachment E: Hosting Capacity Analysis – Security and Confidentiality Considerations, November 2, 2020, p. 1.
[4] Department of Energy, *Securing the United States Bulk-Power System*, Request for Information, Federal Register, 85 FR 41023, July 8, 2020, https://www.federalregister.gov/documents/2020/07/08/2020-14668/securing-the-united-states-bulk-power-system. Note that DOE established this designation to help implement Executive Order 13920, *Securing the United States Bulk-Power System*, May 1, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/.
[5] Cybersecurity & Infrastructure Security Agency, Alert (AA20-352A), Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations, December 23, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-352a.
[6] *Ibid.*, p. 3.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

go beyond reconnaissance. Their goal may be to put themselves in a position to have leverage over the new administration, like holding a gun to our head to deter us from acting to counter Putin."[7]

Adversary efforts to seek such leverage lie at the heart of data collection campaigns against utilities in Minnesota and other states. According to the *National Counterintelligence Strategy of the United States, 2020-2022*, which provides the most detailed US Intelligence Community (IC) assessment of adversary goals in such cyber-related activities, "adversaries are conducting intelligence operations to exploit, disrupt, and damage U.S. and allied critical infrastructure and military capabilities during a crisis." Those efforts "likely are aimed at influencing or coercing U.S. decision makers in a time of crisis by holding critical infrastructure at risk of disruption."[8]

Holding the electric grid at risk would offer an especially potent source of leverage. The *Counterintelligence Strategy* warns that because of the importance of the US electric systems to the economy and public health and safety, those systems could offer a prime target. Indeed, "adversaries seeking to cause societal disruption in the United States could attack the electrical grid causing a large-scale power outage that affects many aspects of daily life."[9]

Other Federal threat assessments warn that adversaries may seek to cripple defense-related assets as well as hold the public survival at risk. The Office of the Director of National Intelligence has warned that Russia is "staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis" along with posing "a significant cyber influence threat" to shape US behavior.[10] Minnesota is home to a number of companies that directly contribute to US national defense and play key roles in Minnesota's economy.[11] Other nationally-critical industries in the State, including food processing and manufacturing, face mounting cybersecurity risks that could threaten public health and create massive financial losses for Minnesota companies.[12] Cyber adversaries can seek to attack all of these companies individually. However, by mapping the distribution grid, they can also seek to leverage the dependence of all of these industries on electric power and use targeted attacks on the electric system to jeopardize Minnesota's population and economy.

---

[7] Quoted in David Sanger et. al., "As Understanding of Russian Hacking Grows, So Does Alarm," *New York Times*, January 2, 2021.
[8] National Counterintelligence and Security Center (NCSC), *National Counterintelligence Strategy of the United States of America 2020-2022*, Washington, DC: NCSC, February 2020, pp. 8 and 6, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf. .
[9] *Ibid.*, p. 6.
[10] Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Washington, DC: ODNI, January 29, 2019, 5, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.
[11] Minnesota Aerospace and Defense Industries, https://mn.gov/deed/assets/aerospace-fact_tcm1045-402669.pdf.
[12] University of Minnesota Report Reveals Growing Threat of Cyberattacks to Food Safety, University of Minnesota, September 10, 2019, https://twin-cities.umn.edu/news-events/university-minnesota-report-reveals-growing-threat-cyberattacks-food-safety.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Two other threat-related factors also provide a basis for developing a risk management framework for sensitive grid data, and for creating risk mitigation measures to enable expanded but secure data sharing. The first is that of assessing adversary incentives to attack distribution grids versus the BPS. The vast majority of the analysis conducted by DOE, the Federal Energy Regulatory Commission (FERC), the Intelligence Community, and other Federal entities focuses on threats to the BPS. That focus reflects division of authority under the Federal Power Act, in which DOE and FERC responsibilities lie overwhelmingly with the BPS, while states exercise authority over distribution systems.

However, another factor drives the focus on the BPS for cybersecurity, including measures to define and protect critical electric information. Adversaries can design attacks on the BPS with the goal of creating cascading failures that black out multi-state regions of the US. Disruptions of distribution systems are typically seen as likely to produce localized effects (though the risks to BPS reliability posed by multiple, simultaneous attacks on distribution systems merits further analysis). Accordingly, from a national security perspective, the lion's share of Federal attention focuses on countering threats to the BPS and protecting sensitive BPS-related data.

That Federal focus makes it all the more vital for the Commission to continue partnering with utilities, energy developers, and other stakeholders to help secure distribution systems from attack. Given the adversary goals described in the *Counterintelligence Strategy*, especially that of holding at risk infrastructure essential for public safety and the economy, distribution systems offer potentially valuable targets. While the BPS generation and transmission assets provide power to distribution infrastructure, that infrastructure provides the "last mile" of service to police and fire stations, financial institutions, and other facilities and functions on which Minnesota's population and economy depend. From a state and local perspective, attacks on last-mile infrastructure could be just as consequential as disruptions of BPS reliability.

A second threat-related factor is also important in addressing the issues raised by Docket Nos. E999/CI-20-800 and E002/M-19-685 and by the Commission's request for comments. For BPS entities, NERC has established mandatory Critical Infrastructure Protection (CIP) standards, including for the protection of sensitive data. In particular, CIP-011-1, *Information Protection*, is structured "To prevent unauthorized access to 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."[13]

No such mandatory NERC standards apply to the distribution systems over which states have authority. The same is true of the CIP standards established by NERC for cyber and physical

[13] North American Electric Reliability Corporation, CIP-011-1, *Information Protection*, https://www.nerc.com/files/CIP-011-1.pdf. Note that NERC has issued subsequent modifications to CIP-011-1 to further clarify and expand upon the initial standard.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

security of critical electric infrastructure. The Idaho National Laboratory (INL), in research conducted for DOE, concludes that the resulting variations in state protection standards for distribution systems may create more favorable opportunities for attack than exist for striking the BPS.[14] Public utility commissions across the US are collaborating with distribution utilities to bolster the protection of critical electric infrastructure and reduce such attack opportunities. The National Association of Regulatory Utility Commissioners (NARUC) and other organizations are supporting their efforts with a growing array of analytic tools and recommendations.[15] In addition, utilities are taking voluntary measures above and beyond those required by mandatory standards to strengthen security. Now, in response to the Commission's request for comments, regulators, utilities, energy developers, and other stakeholders have an opportunity to accelerate such progress on the protection of critical distribution system data.

B. DOMESTIC THREATS

Foreign adversaries are not the only potential threats to Minnesota's distribution system. DHS and the Federal Bureau of Investigation (FBI) warn that domestic violent extremists (DVEs) pose major threats to critical infrastructure and other targets. While DVEs lack the cyber expertise and capabilities of nation state adversaries such as China and Russia, they have ready access to high explosives and other means of physical attack to damage or destroy critical distribution system assets. Access to information on the location of those assets could help ideologically-motivated attackers disrupt service to selected targets, including State facilities of interest to anti-government extremists. DVE groups may also use such data to launch coordinated attacks on multiple substations to achieve wide area, long duration blackouts in Minnesota.

FBI Director Christopher Wray testified in September 2020 that "The greatest threat we face in the homeland is that posed by lone actors radicalized online who look to attack soft targets with easily accessible weapons."[16] Potential grid targets vary in their vulnerability to such attacks. Consistent with NERC mandatory standards for physical security of BPS infrastructure, as well as with voluntary commitments to improved resilience, Xcel Energy and other utilities are hardening substations and other critical electric infrastructure against attack. However, it is impractical to

[14] Idaho National Laboratory, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, August 2016, pp. 11-12, https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

[15] See, for example, the National Association of Regulatory Utility Commissioners' *NARUC Cybersecurity Manual*, https://www.naruc.org/cpi-1/critical-infrastructure-cybersecurity-and-resilience/cybersecurity/cybersecurity-manual/; and NARUC, *Information Sharing Practices in Regulated Critical Infrastructure States Analysis and Recommendations*, June 2007, http://naseo.org/data/sites/1/documents/energyassurance/documents/NARUC_CIP_Information.pdf.

[16] Christopher Wray, Director, Federal Bureau of Investigation, "Worldwide Threats to the Homeland," Statement Before the Senate Homeland Security and Governmental Affairs Committee, Washington, D.C., September 24, 2020, https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-092420.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

build security perimeters (much less supplement them with guards) to defend the feeders and distribution infrastructure that provide the "last mile" of service to hospitals and other critical customers. Securing the information that might otherwise help lone actors target these softer targets can help impede DVE attack planning and execution. The same is true for attacks conducted by homegrown violent extremists (HVEs), who have been radicalized in U.S. but inspired to attack infrastructure and other targets by Al Qaeda, ISIS, and foreign terrorist organizations. [17]

Recent attacks on critical infrastructure illuminate the potential destructiveness of the use of easily accessible weapons. Since the high-powered rifle attack on transformers in the Metcalf, California substation in 2013, and the similar attack in 2016 on the Buckskin substation in central Utah, FERC, NERC, and the electric industry have intensified their efforts to counter the risks posed by small arms fire.[18] Rifle-inflected damage to substation transformers is especially concerning because replacing transformers is a lengthy process. The Department of Energy notes that transformers are "one of the most vulnerable components on the grid." While utilities do maintain some in reserve, transformers "are generally expensive, difficult to transport, and typically custom-made with procurement lead times of one year or longer."[19]

Terrorist groups can scale up the resulting threats to grid infrastructure by seeking to coordinate attacks on multiple substations. The "Lights Out" campaign exemplifies these risks. According to a December 2020 FBI affidavit that was mistakenly unsealed, white supremacists have been plotting to attack multiple substations with rifle fire.[20] One of the substations they were targeting was Xcel Energy's Midway facility outside of Colorado Springs, Colorado. The FBI affidavit stated that the group planned to strike additional substations in the southeastern United States. If extremist groups coordinated equivalent attacks against Minnesota substations, and utilities needed to replace multiple transformers within them, the state could face long duration, wide area power outages.[21]

---

[17] *Ibid.*
[18] Peter Behr, "Substation attack is new evidence of grid vulnerability," *E&E News*, October 6, 2016, https://www.eenews.net/stories/1060043920.
[19] Department of Energy, Addressing Security and Reliability Concerns of Large Power Transformers, https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers. While the report focuses on large power transformers, as opposed to smaller transformers used in many distribution substations, many of the vulnerabilities and replacement challenges cited in the report apply to both categories.
[20] Amy Forliti, "White supremacists plotted to attack US electric grid by shooting into power stations, FBI says," *US News*, December 22, 2020, https://www.usatoday.com/story/news/nation/2020/12/22/white-supremacists-plotted-attack-us-power-grid-fbi-says/4018815001/.
[21] Rick Sallinger "'Lights Out': Neo-Nazi Plot To Disable Power Grid Allegedly Included Attacking Substation In Colorado," *CBS Denver*, December 23, 2020, https://denver.cbslocal.com/2020/12/23/lights-out-neo-nazi-plot-disable-power-grid-allegedly-included-attacking-substation-colorado/.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

The FBI affidavit also stated that the plotters sought to gather data from DOE websites to help plan their attack.[22] Fortunately, DOE has stringent rules to protect CEII from unauthorized access. Equivalent data security measures, tailored to meet the needs of Minnesota while also facilitating energy development projects, will be essential to impede attack planning by extremist groups.

Lone actors and anti-government organizations also have easy access to the materials necessary to construct truck bombs and other improvised explosive devices (IEDs). These weapons can create especially destructive effects. In 2014, attackers placed a makeshift bomb next to a 50,000-gallon diesel tank at a substation near Nogales, Arizona. The bomb caused only minor damage because it failed to ignite the diesel fuel (which has a high flash point and is difficult to ignite). However, law enforcement officials stated that had there been a catastrophic explosion, as many as 30,000 customers could have lost power for an extended period.[23]

The December 2020 explosion in Nashville, TN, offers a more recent example of the destructiveness of IEDs and the regional effects lone actors can create. A recreational vehicle exploded in front of an AT&T Inc. switching station, knocking out a central node that directs data from users and businesses across telecom systems.[24] AT&T customers lost service across wide areas of Tennessee, Kentucky, and Alabama, and halted 911 call services and other critical functions. The company quickly established portable cell sites to accelerate restoration of service.[25] For distribution grid customers in Minnesota with power lines to more than one substation, utilities may also be able to rapidly restore service by re-routing power flows around damaged infrastructure. But critical facilities that depend on a single substation could lose power for extended periods.

Extremist groups could further disrupt power restoration and achieve wider area outages by coordinating IED attacks against multiple substations. In September 2017, a leader of the extremist organization Atomwaffen Division (AWD), issued a call to attack substations and bragged that he had a West Coast grid map provided by "someone with special permissions to get it." After another

[22] *Ibid.*
[23] Sean Holstege and Ryan Randazzo, "Sabotage at Nogales station puts focus on threats to grid," *AZ Central*, June 12, 2014, https://www.azcentral.com/story/news/arizona/2014/06/12/sabotage-nogales-station-puts-focus-threats-grid/10408053/. The law enforcement sources for the article did not specify the length of the outage that an explosion could have created. A number of factors determine outage durations, including the availability of alternative substations and power feeds to serve the stricken area, and possible use of mobile emergency assets to accelerate service restoration. In typical radial distribution systems, however, the catastrophic destruction of a critical substation could produce extended blackouts.
[24] David Umberti, "Nashville Bombing Exposes Weak Point for Business Communications," *Wall Street Journal*, December 28, 2020, https://www.wsj.com/articles/nashville-bombing-exposes-weak-point-for-business-communications-11609194817.
[25] Tali Arbel, "Nashville Bombings Spotlight Vulnerable Voice, Data Networks," *Associated Press*, December 29, 2020, https://apnews.com/article/service-outages-bombings-nashville-a14babd6748fea7c43ed396801aaabf7.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

AWD member claimed that the group was planning to use a cache of explosives to attack the grid and other targets, the FBI arrested five members across four different states in April 2020.[26]

DHS warns that lone actors and terrorist organizations may also use more advanced weapons in future attacks. While the use of rudimentary explosive devices will probably remain most common, "lone offenders could employ more sophisticated means, to include advanced and/or high-consequence IEDs" and other types of attacks." In particular, "terrorists and other criminal actors might look to unmanned aircraft systems (UAS) to threaten critical infrastructure."[27] Protecting locational information that attackers might use to target substations and other assets with these advanced weapons can make a significant contribution to the security of Minnesota's distribution grid.

C. SPECIFIC THREAT VECTORS AND IMPLICATIONS FOR DATA PROTECTION

The overall threat to Minnesota's distribution grid provides only the starting point to develop risk management frameworks and mitigation measures for sensitive grid data. To reach consensus on which categories of data pose the highest risks, and that therefore may require special protections (including systems for tiered access), the Commission, utilities, and other grid stakeholders should also account for the specific attack vectors that adversaries may employ and the categories of data that would be most useful for planning and conducting those attacks.

First, however, it will be useful to analyze the growing value of publicly available data to foreign adversaries. These adversaries will no doubt seek to steal protected grid data. However, artificial intelligence (AI) and other new analytic tools are enabling them to make increasingly effective use of "open source intelligence (OSINT)," that is, information that is publicly available via the internet and other sources.[28]

US researchers have identified a number of ways in which data gathered on the web can be used to profile the network structure and other structural characteristic of US power companies.[29] Dragos, a leading cybersecurity firm, has leveraged the Department of Defense's CARVER data matrix to identify categories of OSINT that attackers can find especially valuable for attack planning. One such category is "critical information" that "informs an adversary of the impact of an attack for the target's continued operation. A target's criticality is determined if its

[26] K. Campbell, "The Far-Right Domestic Extremist Threat to the Power Grid," *Homeland Security Today*, March 24, 2020, https://www.hstoday.us/subject-matter-areas/infrastructure-security/the-far-right-domestic-extremist-threat-to-the-power-grid/.
[27] *Homeland Threat Assessment*, Department of Homeland Security, October 2020 (9917-19), https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.
[28] Open Source Intelligence (OSINT): Issues for Congress, Congressional Research Service, December 5, 2007, https://fas.org/sgp/crs/intel/RL34270.pdf.
[29] Darren Hayes, Using Open Source Intelligence for Risk Assessment to the U.S. Power Grid, April 2017, https://www.researchgate.net/publication/316167221_USING_OPEN_SOURCE_INTELLIGENCE_FOR_RISK_ASSESSMENT_TO_THE_US_POWER_GRID.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

compromise or destruction has a highly significant impact in the overall organization and its ability to conduct business or operations." A closely related category is that of "effect information," that is, information about the amount of direct or indirect loss a target would have from an attack or compromise," and its ability to operate.[30] Under this framework, OSINT of special concern would include data that could help adversaries target grid attacks to disrupt service to Minnesota's critical public safety and economic assets.

Sophisticated new analytic tools are also increasing the value of publicly available data for grid attack planning. The US National Science and Technology Council has found that AI, machine learning, and other advances can help cyber defenders enhance their protection operations. But the council also notes that AI will help attackers make more effective use of the data they gather, by helping model a victim's systems, and develop plans to exploit the vulnerabilities that AI helps identify.[31] China has declared its intention to become the world leader in AI, and is committed to applying its expertise to "leapfrog" U.S. defense capabilities.[32] Russia is also ramping up its AI research and development efforts. The net effect of these analytic advances: publicly available information that once might have provided only a limited basis for cyber and physical attack planning is now increasingly valuable.

Adversaries may also combine cyberattacks with the physical destruction of transformers (which could take significant time to replace) to seek especially wide area, long duration blackouts. NERC's GridEx exercises, which constitute the premier exercise system for the electricity subsector, assume that adversaries will conduct such combined cyber-physical attacks.[33] Decisions on the release of sensitive grid data should account for the risks of enabling such combined attacks as well.

1. Data on Feeders and Other Distribution Assets that Serve Critical Loads

Knowledge of the specific systems that provide power to critical facilities will be especially valuable for holding public safety and the economy at risk in Minnesota and other states. Russia has used information gathering on distribution infrastructure in Ukraine to help create brief but

[30] Selena Larson, Open Source Intelligence, Dragos, Inc, December 2020, https://www.dragos.com/resource/open-source-intelligence/.
[31] AI and Cybersecurity: Opportunities and Challenges, National Science and Technology Council, March 2020, p. 5, https://www.nitrd.gov/pubs/AI-CS-Tech-Summary-2020.pdf. See also Greg Allen and Daniel Chan, Artificial Intelligence and National Security, Belfer Center for Science and International Affairs, July 2017, p. 24, https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.
[32] Elsa B. Kania , Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power, Center for a New American Security, November 2017, p. 4, https://s3.amazonaws.com/files.cnas.org/documents/Battlefield-Singularity-November2017.pdf?mtime=20171129235804.
[33] GridEx V Lessons Learned Report, NERC, March 2020, https://www.eisac.com/cartella/Asset/00008427/TLP_WHITE_GridEx_V_Public_After_Action_Report.pdf?parent=123814.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

widespread outages in 2015. After mapping the grid's operating systems and critical substations, attackers used the system's industrial control system (ICS) protocols to open circuit breakers, creating blackouts.[34] Russia's follow-on attack on Ukraine in 2016 employed malware that was still more difficult to detect, and included a wiper module that could "brick" grid control system components on a large scale.[35] Attackers also had the ability to deny or corrupt situational awareness data, making the grid extremely prone to cascading failures. In addition, recent analysis of the attack has revealed that these immediate effects were merely intended to be the precursors for an attempt at a more ambitious attack. Perpetrators intended to cause blackouts on a much wider scale by disabling the protective relay devices that were in place to stop power failures from cascading across the grid.[36]

We can expect Russia and other adversaries to employ all such tactics against US distribution systems, and (as in the case of the ongoing Dragonfly 2.0 campaign) to continue upgrading their attack capabilities. We should also expect adversaries to gather information on the distribution grid in Minnesota and other states to help target their attacks, and to select specific substations, feeders, breakers, protective relays and other assets for misoperation or disruption. But past attacks and ongoing reconnaissance efforts (including SolarWinds) offer only a hint of the reconnaissance-enabled attacks to come. While employing BlackEnergy, NotPetya, and other malware against power grids helps Russia build its expertise for cyberwarfare, US adversaries are almost sure to be holding their most destructive cyberweapons in reserve.[37] Doing so helps them prevent the US from gaining advance knowledge about those weapons and developing countermeasures to protect the grid. We can, however, limit the availability of information that could help adversaries target advanced weapons for maximum impact on Minnesota's public safety and economy.

Countering the adversary's exploitation of sensitive data will also require a strategic understanding of how asset mapping can assist attack planning. For example, protecting information on the location of feeders will impede Russian and Chinese efforts to map additional distribution grid nodes for attack. We should expect adversaries to map back from feeders to the substations that supply their power. The key reason: if adversaries can disable transformers and other substation

[34] "Alert (ICS-ALERT-17-206-01): CRASHOVERRIDE Malware," Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), July 25, 2017, https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01; "Alert (TA17-163A): CrashOverride Malware," US Computer Emergency Readiness Team (US-CERT), June 12, 2017, https://www.us-cert.gov/ncas/alerts/TA17-163A; Dragos, Inc, CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations, June 13, 2017, p. 8, available at https://dragos.com/blog/crashoverride/CrashOverride-01.pdf; and Defense Science Board (DSB), Task Force on Cyber Deterrence, Washington, DC: DOD, February 2017, p. 4, https://www.acq.osd.mil/dsb/reports/2010s/DSB-cyberDeterrenceReport_02-28-17_Final.pdf.
[35] Alert (TA17-163A): CrashOverride Malware," US-CERT, https://www.us-cert.gov/ncas/alerts/TA17-163A.
[36] Joe Slowik, CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack, Hanover, MD: Dragos, Inc., September 2019, p. 1, https://dragos.com/wpcontent/uploads/CRASHOVERRIDE.pdf.
[37] On Russia's use of BlackEnergy and NotPetya against Ukraine, see Laurens Cerulus, "How Ukraine Became a Test Bed for Cyber Weaponry," *Politico*, February 14, 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

equipment, they can create outages affecting wider areas (and for longer periods) than by striking individual feeders. Data protection strategies need to counter adversary efforts to aggregate discreet data points for comprehensive, pre-attack mapping of distribution systems.

2. Data to Assist Load Manipulation Attacks

Researchers have identified a new threat vector to the grid: the manipulation of loads to create grid instabilities.[38] Foreign adversaries can seek to cause drastic changes in load to create instabilities and power swings, and thereby cause outages and equipment damage. A number of studies have examined the risk that adversaries will seek to access large numbers of smart meters, and cause a widespread blackout by switching smart meter loads on and off repeatedly.[39] Manipulation of the growing load created by Internet of Things devices (including heavy-load systems such as heating and air conditioning systems), and by new load centers such as electric vehicle power charging stations, could also create major system instabilities.[40]

Data on peak substation transformer loads, peak feeder loads, maximum capacity for substations and feeders, and other load-related information could help adversaries maximize the effectiveness of such attacks. By gaining advanced knowledge of when Minnesota's distribution loads were likely to be at typically maximum levels, adversaries could time and structure their attacks to create especially disruptive power surges.

The Commission and grid stakeholders should also consider accounting for the risk that adversaries will combine load-manipulation attacks with other threat vectors. For example, in NERC's GridEx V exercise in November 2019, the blackout scenario included successful adversary disruption of the protective relays that help defend transformers and other critical grid equipment from power surge-induced damage. Load-related data could help adversaries time and target attacks that include protective relay disruptions and other threat vectors to achieve synergistic, mutually reinforcing effects on electric service to critical facilities.

---

[38] Sajjad Amini, et. al., "Dynamic Load Altering Attacks against Power System Stability: Attack Models and Protection Schemes," *IEEE Transactions on Smart Grid* (Volume: 9, Issue: 4), July 2018, https://ieeexplore.ieee.org/document/7723861; Athira Mohan et. al., A Comprehensive Review of the Cyber-Attacks and Cyber Security on Load Frequency Energies, 28 July 2020, file:///C:/Users/Paul%20Stockton/Downloads/energies-13-03860%20(4).pdf; Joy Johnson et. al., Power System Effect and Mitigation Recommendations for DER Attacks, October 2019, https://www.osti.gov/servlets/purl/1496989.

[39] Anca Gurzu, "Hackers threaten smart power grids," *Politico*, January 11, 2017, http://www.politico.eu/article/smart-grids-and-meters-raise-hacking-risks/; Department of Energy, Advanced Metering Infrastructure and Customer Systems, p. 69; Aaron Hansen, Jason Staggs and Sujeet Shenoi, "Security analysis of an advanced metering infrastructure," *International Journal of Critical Infrastructure Protection* (Volume 18), September 2017, p. 3.

[40] "Shock to the system: Electric car charging stations may be portals for power grid cyberattacks," *Tandon School of Engineering*, August 14, 2009, https://engineering.nyu.edu/news/shock-system-electric-car-charging-stations-may-be-portals-power-grid-cyberattacks.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Innovative means of attack could further leverage the availability of load data. One example lies in the use of information operations (IOs) to initiate customer-driven spikes in power consumption. A recent Chinese-edited journal article explores how adversaries can send fake discount notifications to customers that encourage them to time the recharging of their electric vehicles during the peak-demand periods. Using Greater London as a case study, the article describes how such IOs might indeed lead to unwitting consumers synchronizing their energy-usage patterns, and result in blackouts on a city-scale if the grid is heavily loaded.[41] Denying adversaries' access to load-related data can help counter such emerging threat vectors. Protecting data on the number of customers served by a given feeder or substation can also strengthen distribution system security. If adversaries learn that a feeder serves a very small number of customers, that provides an indicator that major hospitals or other critical loads in the vicinity rely on that specific feeder, enabling adversaries to refine their attack plans accordingly. Similarly, knowledge that a feeder serves an exceptionally large number of customers could help advisers design attacks to create mass effects on a region's population.

3. Recommendations for Further Analysis and Commission-Sponsored Discussions

Xcel Energy and other grid owners and operators are making crucial, large-scale investments in the resilience of their systems against cyber and physical attacks. But threats to their systems are diversifying and becoming increasingly severe. Alexander Gates, while serving as the acting director of DOE's Office of Cybersecurity, Energy Security, and Emergency Response, noted in 2020 that electric utilities and their government partners are making great strides in protecting the grid from attack. Yet, "despite all the progress made today, the cyberthreats to the sector are real and outpacing our collective solutions."[42]

Decisions on whether and how to protect sensitive grid data should reflect the evolving nature of the threat and adversary opportunities to exploit that data in new ways. The Commission's Request for Comments asks whether the Commission should host a workshop or facilitated discussion on issues related to public access to grid data. I strongly recommend that the Commission do so, and suggest that that those discussions include expert testimony on (1) emerging attack vectors against the distribution gird, and (2) how adversaries can use grid data to help plan and execute their attacks. Any such discussions should be conducted in ways that protect critical information and avoid giving adversaries a potential "roadmap" to design future attacks.

[41] Gururaghav Raman, et. al., "How weaponizing disinformation can bring down a city's power grid," *Plos One*, August 12, 2020, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0236517.
[42] Christian Vasquez, "DOE official: More money, power needed to protect grid," *E&E News*, August 6, 2020, https://www.eenews.net/energywire/stories/1063689119.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

III. CRITERIA FOR DESIGNATING SENSITIVE DATA

Based on Intelligence Community assessments of the threat, and opportunities for adversaries to use specific types of information to target their attacks for maximum effect, the Commission might consider options to establish criteria for identifying data that merits protection. The Staff Briefing Papers for the Commission on Docket E002/M-19-685 (June 11, 2020) note that the Commission has not issued an Order on the definition of critical energy infrastructure beyond referencing the FERC regulation in the Minnesota DER Interconnection Process (MN DIP 5.9).[43] Nor has the Commission yet established criteria to identify critical electric infrastructure information (CEII) applicable to Minnesota's distribution systems. The analysis below examines potential "building blocks" that might contribute to the development of such criteria: (1) Xcel Energy's current guidelines for identifying critical customers and protecting data on the infrastructure that serves them, including Xcel Energy's use of guidelines provided by DHS; and (2) NERC/FERC standards for designating CEII.

A. CRITERIA CURRENTLY EMPLOYED BY XCEL ENERGY

1. Existing Minnesota Statutes

As Xcel Energy noted in its 2020 Hosting Capacity Analysis, Minn. Stat. §13.37, subd. 1(a) provides criteria for classifying data as security information. Such data is likely to substantially jeopardize the security of information or property against tampering, improper use, illegal disclosure, trespass or physical injury. Minn. Stat. §13.02, subd. 9, and § 13.03, subd. 1, also specifies that this information constitutes "nonpublic data" as federal law treats it as "trade secret" under 18 USC §1839, because it reflects business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, methods, techniques, processes, programs, or codes, where reasonable measures have been taken to keep such information secret, and it derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.[44]

2. US Department of Homeland Security (DHS) Criteria

Xcel Energy's Hosting Capacity Analysis also notes that DHS provides additional guidance on protecting critical infrastructure information. DHS has identified 16 critical infrastructure sectors whose assets, systems, and networks are considered so vital to the United States that their

[43] Docket No. E002/M-19-685, *In the Matter of Xcel Energy's 2019 Hosting Capacity Analysis Report*, Staff Briefing Papers, June 11, 2020, p. 40.
[44] Docket No. E002/M-20-812, *In the Matter of Xcel Energy's 2020 Hosting Capacity Analysis Report*, Initial Filing - Hosting Capacity Report, Attachment E: Hosting Capacity Analysis – Security and Confidentiality Considerations, November 2, 2020, pp. 5-6.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Based on those DHS designations, Xcel Energy has developed categories of critical customers and associated feeders that the company has used as a basis for limiting the public release of grid data. They include:

- Critical Energy Infrastructure (similar to DHS Energy sector) on distribution feeders,
- Critical Hospital - Level 1 or 2 Trauma Center (similar to DHS Healthcare and Public Health sector) on distribution feeder,
- Critical Data Center (similar to DHS Communications and Information Technology sectors) on distribution feeder, and
- Critical Public Gathering Center (similar to DHS Commercial Facilities sector) on distribution feeder.

The above categories are essential but also incomplete as a basis for guiding the designation of sensitive grid data. Given Federal assessments of the goals that adversaries will seek to achieve in future cyberattacks, including jeopardizing public health and safety, water systems and other additional classes of targets (and grid data useful to attack them), the Commission and grid stakeholders should also consider including additional categories of critical, grid-dependent customers.

DHS' recent update of its list of critical infrastructure sectors provides a starting point to do so.[45] However, for Minnesota, not all of these sectors are equally important to the economy and public safety. Additional criteria will be needed to help determine critical customers and establish corresponding protections for data on the distribution systems that serve them.

The Commission might also consider developing criteria not only to restricting data on specific feeders (based on the critical loads they serve), but also for classes of information that should be protected for all feeders and other distribution infrastructure. One model to leverage for establishing such broader criteria lies in DHS' definition of critical infrastructure information, established pursuant to the Critical Infrastructure Information Act of 2002 (codified at 6 U.S.C. § 133) and the Department's Protected Critical Information (PCII) Program regulations (6 C.F.R. part 29). PCII is information not customarily in the public domain and that is related to the security of critical infrastructure or protected systems, including documents, records, communication networks, or other information concerning:

- Actual, potential, or threatened interference with, attack on, compromise or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct that violates Federal, State, local, tribal, territorial laws, harms interstate commerce of the United States, or threatens public health or safety;

[45] CISA, *Critical Infrastructure Sectors*, updated October 2020, https://www.cisa.gov/critical-infrastructure-sectors.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

- The ability of any critical infrastructure or protected system to prevent such interference, compromise, or incapacitation; including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; and
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.[46]

While this definition of critical infrastructure information is suitable for the purposes of the PCII program which involve the voluntary sharing and protection of such data between DHS and infrastructure owners/operators, it is far too broad and inclusive to use as criteria for identifying Minnesota's sensitive grid data. Energy developers require access that might be withheld under DHS' PCII information standards. A more narrowly focused, threat-informed approach will be necessary for the Commission to strike a balance between providing energy developers with the information they need and securing that information from Russia, China, and other adversaries.

B. FERC/NERC STANDARDS AND DEFINITIONS

NERC Critical Infrastructure Protection (CIP) Standard CIP-011-2 "Cyber Security — Information Protection," provides the foundation for actions by Bulk Electric System (BES) entities to identify and protect sensitive information.[47] In particular, the standard specifies the information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.[48] NERC's mandatory standards apply to BES entities.[49] Nevertheless, Commissioners may wish to consider how

[46] CISA, Protected Critical Infrastructure Information Program, https://www.cisa.gov/pcii-faqs.
[47] A note on terminology: in 2014, FERC approved NERC's definion of the Bulk Electric System (BES) as "all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy." This definition also specified certain exlusions of electric system infrastructure, including radial electric systems. NERC, *BES Definition Approved by FERC 3-20-14*, https://www.nerc.com/pa/RAPA/BES%20DL/BES%20Definition%20Approved%20by%20FERC%203-20-14.pdf. For a detailed and updated list of assets included in the BES, see NERC, *Bulk Electric System, Definition Reference Document*, Version 3, August 2018, https://www.nerc.com/pa/Stand/2018%20Bulk%20Electric%20System%20Definition%20Reference/BES_Reference_Doc_08_08_2018_Clean_for_Posting.pdf. DOE employs the term Bulk Power System (BPS) instead of BES. The BPS constitutes facilities and control systems necessary for operating an interconnected electric energy supply and transmission network (or any portion thereof), and electric energy from generating facilities needed to maintain transmission system reliability. As with the BES, the term does not include facilities used in the local distribution of electric energy. For a helpful discussion of the distinctions between the BES and BPS, see Midwest Reliability Organization, https://midwestreliability.org/contactus/Lists/FAQ/DispForm.aspx?ID=122
[48] CIP-011-2 – Cyber Security – Information Protection, NERC, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-011-2&title=Cyber%20Security%20-%20Information%20Protection&jurisdiction=null.
[49] CIP-002-5.1a – Cyber Security – BES Cyber System Categorization characterizes the BES and its system components that fall under NERC's cyber CIP standards. P.2. of CIP-011-2 specifies the facilities, systems and

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

elements of CIP-011-2 might be modified to help meet their distribution grid objectives in Dockets E999/CI-20-800 and E002/M-19-685, and address Minnesota-specific data protection challenges.

A key feature of CIP-011-2 is that while the standard mandates the identification of BES Cyber System Information, the standard provides only general guidance as to what would constitute such information. NERC emphasizes that an entity required to implement CIP-011-2 "has flexibility in determining how to implement the requirement." However, NERC also mandates that the applicable entities must explain their methods for identifying such information in the information protection program that they provide to NERC.[50] A similar combination of flexibility and detailed reporting could be useful for efforts by the Commission and stakeholders to help undergird data protection measures for the distribution grid.

The Federal Energy Regulatory Commission provides more detailed definitions that might be leveraged to support such efforts. Most valuable, FERC's Critical Energy/Electric Infrastructure Information (CEII) program provides specific ways of categorizing such information. The Commission defines CEII as "information related to or proposed to critical electric infrastructure" that is:

- generated by or provided to the Commission or other Federal agency other than classified national security information,
- that is designated as critical electric infrastructure information by the Commission or the Secretary of the Department of Energy pursuant to section 215A(d) of the Federal Power Act.

CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

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; and
4. Gives strategic information beyond the location of the critical infrastructure.

Critical energy/electric infrastructure means a system or asset of the bulk-power system, (physical or virtual) the incapacity or destruction of which would negatively affect:

- national security,
- economic security,
- public health or safety, or

equipment for Distribution Providers to which the standard applies. https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-002-5.1a&title=Cyber%20Security%20%E2%80%94%20BES%20Cyber%20System%20Categorization&jurisdiction=null.

[50] CIP-011-2, p. 13.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

- any combination of such matters.[51]

These categories provide a useful starting point to develop equivalent distribution-oriented counterparts for Minnesota. They align well with the disruptive effects that adversaries would attempt to achieve in striking the grid, and hence with the need to protect grid information that could help them achieve those objectives. If the Commission hosts a workshop to discuss the issues raised in the Request for Comments and associated Dockets, participants could use FERC's CEII definition as a basis to build consensus on whether and how equivalent definitions might be established to guide data release and protection standards for Minnesota's distribution grid.

IV. POTENTIAL ATTACK CONSEQUENCE: USE CASES TO SUPPORT COMMISSION AND STAKEHOLDER ANALYSIS

Assessing potential consequences of attacks on Minnesota's distribution grid is vital for developing a risk management framework for sensitive data. Led by DHS, a broad array of public agencies and private companies have adopted frameworks based on the formula of *risk = threat x vulnerability x consequences*, where:

- Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences;
- Threats are natural or man-made occurrences or actions that have or indicate the potential to harm life, information, operations, the environment and/or property;
- Vulnerability is the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard; and
- Consequences are the potential or actual effects of an event, incident, or occurrence, including "mission consequence" – that is, the effect of an incident, event, operation, or occurrence on the ability of an organization or group to meet a strategic objective or perform a function.[52]

[51] Federal Energy Regulatory Commission, Critical Energy/Electric Infrastructure Information (CEII), https://www.ferc.gov/enforcement-legal/ceii#:~:text=Critical%20energy%2Felectric%20infrastructure%20means,any%20combination%20of%20such%20matters.

[52] Department of Homeland Security, Risk Lexicon, September 2010, https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf. Within the category of threats, some applications of this formula include the probability of an event occurring. Other risk management frameworks include event probability as a separate variable. However, for cyberattacks and other manmade threats estimating the likelihood an event is inherently problematic. Attempting to anticipate adversary goals and intentions, and directly assess probabilities for the actions of intelligent antagonists, can produce ambiguous or mistaken risk estimates. Louis Cox, "Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks," *Risk Analysis*, November 2008, https://www.researchgate.net/publication/23464582_Some_Limitations_of_Risk_Threat_Vulnerability_Consequence_for_Risk_Analysis_of_Terrorist_Attacks.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

With Section II having assessed threats to the distribution grid, and Section III having analyzed the vulnerabilities that may be created by making sensitive grid data available to the public (and to US adversaries), the next step for developing a risk management framework is to assess potential attack consequences. Cyber-induced power outages could create widespread effects for Minnesota's population and economy. However, those effects would stem not just from the direct impact of power disruptions to homes and businesses, but also from the ripple effects of breakdowns in electricity-dependent infrastructure and critical facilities.

Appendix B provides the Commission with an analysis of how the cutoff of grid-provided power to a specific Twin Cities facility could inflict catastrophic effects on public health and safety. Xcel Energy is providing to the Commission the non-public Appendix B under separate cover.

If the Commission were to convene a workshop to address the issues raised in the Request for Comments, that event could also provide a forum for the discussion of additional use cases and opportunities to apply consequence-driven analysis to assist the Commission. Participants might include not only grid resilience stakeholders, but also representatives of agencies and facilites that provide services essential to public safety and Minnesota's economy. Electricity-dependent infrastructure system managers and their critical customers offer one such set of potential participants. State, local, and tribal emergency management agencies, fire and police departments, Non-Governmental Organizations responsible for mass care in Minnesota (consistent with Emergency Support Function 6) and other organizations might also be invited. These participants could help the Commission assess the potential consequences of targeted attacks on distribution feeders and other distribution infrastructure.

Over the longer term, it might also be useful to develop additional use cases to support consequence-informed risk management. The communications sector provides one such option, given its criticality and dependence on grid-provided power. Major Minnesota agriculture and food processing companies, data storage and processing, and companies that provide equipment and services critical for U.S. national defense might also be candidates for such consequence-based analysis.

The Minnesota Department of Public Safety's Homeland Security and Emergency Management organization, the Department of Health, and other agencies may be able to assist in the selection and buildout of such use cases. For example, by using the State's Threat and Hazard Identification Assessment (THIRA), and focusing on power disruptions that could have the greatest consequences, workshop participants might be able to identify priority use cases for further

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

analysis (and for special consideration in developing risk mitigation measures for sensitive grid data).[53] Options might include:

- Hospitals identified by the Minnesota Department of Health as Level 1 Trauma Hospitals, including Hennepin Healthcare (Minneapolis) and Regions Hospital (St. Paul);[54]
- State and regional emergency operations centers, major police and fire department headquarters, and 911 dispatch centers, and other public safety facilities;
- Grid distribution assets that serve especially large numbers of Minnesota residents and whose disruption could create mass effects;
- Minneapolis-St. Paul International Airport and associated infrastructure;
- Companies in the US Defense Industrial Base (DIB) that provide critical goods and services to the Department of Defense, whose feeders and supporting grid assets may be of special interest to foreign adversaries.

V. DEVELOPING AND APPLYING RISK MANAGEMENT FRAMEWORKS FOR SENSITIVE DATA

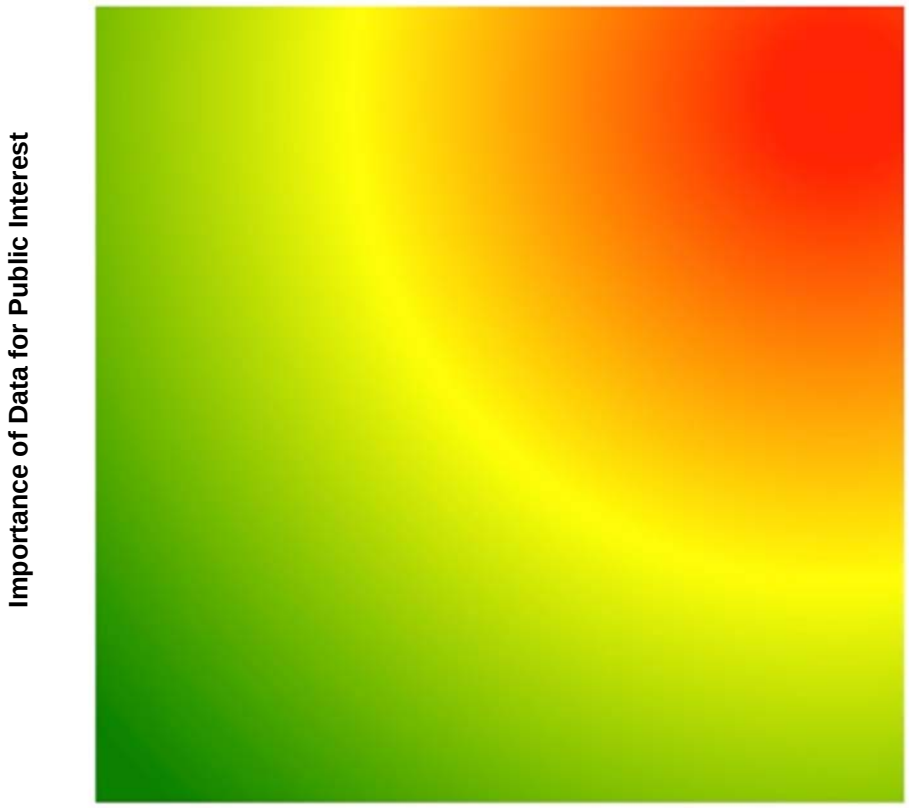
To help support Commission decisions on whether and how sensitive grid distribution data should be shared, one additional factor should be considered: the value of specific types of information for DER projects and other energy development efforts related to hosting capacity analysis. Not all categories of data will be equally important for developing of such projects. To strike a balance between the need to block adversary access to information helpful for attack planning, and the goals of increasing DERs and zero carbon generation, the Commission should account for both the sensitivity of that data *and* its criticality for project development. Such assessments can then provide the basis to develop risk mitigation plans and data sharing policies that help achieve both objectives.

Figure 1 illustrates how the two components of this balancing calculus might be incorporated. Along the bottom horizontal (x) axis of the graph, grid distribution data is aligned in terms the potential consequences of its exploitation by adversaries, from least consequential to catastrophic. Information on the right extreme of this x axis would constitute specific feeder locations, details on their maximum loads, and other data likely to be exceptionally valuable for disrupting service to Minnesota's hospitals, water systems, and other critical facilities. The vertical (y) axis represents data that could be useful for DER projects and other initiatives that rely on grid distribution system hosting. The lower end of that axis constitutes non-essential information. The upper extreme represents data that is absolutely essential for project development and execution.

[53] Threat and Hazard Identification Assessment, Minnesota Homeland Security and Emergency Management, https://dps.mn.gov/divisions/hsem/homeland-security/Pages/threat-hazard-risk-assess.aspx.
[54] Level 1 Trauma Hospitals, Minnesota Department of Health, https://www.health.state.mn.us/facilities/traumasystem/designatedhospitals.html.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Figure 1: Balancing the Need to Share Sensitive Data with the Imperatives to Protect It



The gradations of color in Figure 1 illustrate how these two data sets might be correlated to help frame data sharing and risk mitigation efforts. The areas in green represent information where clear-cut rules will be easy to establish. In the upper left hand corner, which represents data that is essential to DER projects and poses little or no risks of enabling high-consequence attacks, such data should be publicly available. Data in the lower right corner (of little value to DER projects but immensely helpful planning catastrophic attacks) should not be publicly available. The upper righthand corner provides the true challenge for developing data sharing and risk mitigation initiatives. That region of the graph constitutes information that is both essential to energy developers and valuable to China, Russia, and other foreign adversaries as well as domestic terrorists who may seek to jeopardize Minnesota's public safety and economy.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Input from energy developers and other grid stakeholders will be essential to help the Commission determine which specific types of data are vital for DER and other projects. The Commission should consider convening a workshop to help build consensus on these requirements. Based on stakeholder discussions, the workshop could then address an additional opportunity for progress: the development of specialized sharing policies, procedures and protocols to enable the sharing of sensitive and project-essential data.

VI. OPTIONS FOR SHARING SENSITIVE DATA: EXISTING MODELS AND NEW OPPORTUNITIES FOR TIERED ACCESS

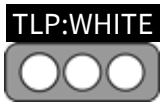
Decisions on expanding the availability of grid data do not have to follow an "all or nothing" approach. Instead, the Commission should consider employing two criteria to guide the selective release and protection of sensitive information: *need to know* and *need to protect.* Using the first criteria, the Commission might differentiate between information that could safely be provided to the general public, and higher risk information that would be released only to energy developers who require it to develop and execute DER and other projects. That approach would enable the development of a system for tiered access to grid data. Then, for developers who demonstrate a need to know, the Commission, utilities, and the developers themselves might collaborate to develop and implement measures to protect the sensitive data that utilities share.

A. EXISTING MODELS OF TIERED ACCESS

A number of systems exist for selective data sharing that the Commission might consider adapting to help meet Minnesota's requirements. Many organizations that help their infrastructure sectors manage the flow of sensitive data, including the Electricity Information Sharing and Analysis Center (E-ISAC), employ the Department of Homeland Security's Traffic Light Protocol (TLP) system. TLP users establish a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). Figure 2 illustrates this system for tiered access to information.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Figure 2: TLP System Data Categories and Sharing Guidelines

Color	When should it be used?	How may it be shared?
 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.
 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.**
 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.
 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.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

DHS' categories for defining TLP:RED and TLP:AMBER data are very general. So too are the categories of users designated for access to such information. That is understandable, given the multi-sector nature of the TLP system. To meet the needs of Minnesota, it might be possible to develop a more grid-specific version of the system to help guide and enable the sharing of sensitive hosting capacity-related information for developers with a need to know.

Additional models are being developed by other states and associations. NARUC's report on *Information Sharing Practices in Regulated Critical Infrastructure States: Analysis and Recommendations* (June 2007), provides a useful starting point to assess such efforts and explore how other state models might be adapted to meet the goals of the Commission. The report notes that some utility commissions use classification structures to protect CII. These structures typically allow a commission to segregate highly sensitive information from less sensitive information, providing higher levels of protection to the most sensitive information. While the report found that document classification systems were not yet common in state Public Utility Commissions (PUCs), Colorado's two-tiered classification system offers an example of how to differentiate between what the Colorado PUC calls "confidential" and "highly confidential" information. Higher levels of classification, such as "highly confidential" in Colorado's typology, imply greater protections and less public access to information. The report also reviews models developed by Texas and other states for categorizing and selectively limiting the availability of information.[55]

A more recent survey of such practices is provided by *Improving the Cybersecurity of the Electric Distribution Grid* (April 2019), which analyzes initiatives by PUCs to improve information sharing between utilities, commissioners, and their staffs.[56] The study does not address the focus of this white paper: that is, the development of policies and risk management mechanisms for the sharing of sensitive data between utilities and energy developers. Nevertheless, some of the strategies that PUCs are developing in partnership with their regulated utilities could provide useful models for secure utility-developer data sharing. Commission-hosted workshops might explore these options and how they could be applied to the issues raised in the Request for Comments.

The National Conference of State Legislators (NCSL) and the National Governors Association (NGA) are also exploring the challenges of sharing sensitive information, and seeking new ways to comply with State open government laws and other factors requiring expanded data availability with security concerns.[57] Finally, NERC's CIP-011-2 standard on Information Protection provides

[55] NARUC's report on *Information Sharing Practices in Regulated Critical Infrastructure States: Analysis and Recommendations*, June 2007, pp. 21-23, http://naseo.org/data/sites/1/documents/energyassurance/documents/NARUC_CIP_Information.pdf.
[56] *Improving the Cybersecurity of the Electric Distribution Grid*, Institute for Energy and the Environment, Vermont Law School, April 2019, https://www.protectourpower.org/resources/vls-iee-pop.pdf.
[57] Emily Dowd, Open Government Laws and Critical Energy Infrastructure, National Conference of State Legislators, January 2018, https://www.ncsl.org/research/energy/open-government-laws-and-critical-energy-infrastructure.aspx; Jessica Rackley, State Protections of Critical Entergy Infrastructure Information (CEII),

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

entities with the flexibility to create classification levels for sensitive information (including confidential, public, and for internal use only) as part of their information protection programs.[58] Future workshops might explore how power companies subject to these standards are developing new models for tiered access to data, and assess their potential applicability to meeting Minnesota's goals.

B. MECHANISMS FOR INFORMATION PROTECTION

As with tiered access, a growing number of models are emerging for the protection of sensitive grid distribution data shared by utilities. None of these models are fully adequate to address the issues raised by Docket Nos. E999/CI-20-800 and E002/M-19-685. However, taken together, they offer features that might help the Commission and grid stakeholders develop protection policies, protocols, and mechanisms for developers who have a need to know high-risk information.

The Public Service Commission of the District of Columbia (DC Commission) has addressed protection issues in its Power Path DC Order of June 5, 2020.[59] That Order primarily focuses on customer data access and protection issues, versus developer access to sensitive project development data. However, some of the recommendations made to the DC Commission might be applied to the latter topic. The Order notes that DC's Customer Impact Working Group (CIWG) recommended that the DC Commission work with Potomac Electric Power (PEPCO) to ensure that third-parties seeking access to customer data via an electronic interface with Pepco adhere to Pepco's cybersecurity standards for protection of this data. The CIWG also recommended that the DC Commission: (1) audit third parties' systems and processes to ensure compliance with these standards; and (2) ensure utilities and energy service providers develop policies and practices to address the integrity and confidentiality of customer data. In addition, Pepco recommended that the DC Commission consider directing Pepco to execute nondisclosure agreements (NDAs) with third parties in order to give the DC Commission insight into and confidence regarding third-party security and privacy standards and practices. However, Pepco cautioned that such NDAs "would in no way transfer to Pepco responsibility for a violation by or breach of a third party."[60]

The DC Order directed Pepco to execute NDAs with third parties for assurances on security and privacy standards. The Order did not, however, accept the recommendation that the DC

National Governors Association, July 2019, https://www.nga.org/center/publications/state-protection-of-critical-energy-infrastructure-information-ceii/.

[58] CIP-011-2, p. 13, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-011-2&title=Cyber%20Security%20-%20Information%20Protection&jurisdiction=null.

[59] Power Path DC Order, Formal Case No. 1130, *In the Mater of the Investigation into Modernizing the Energy Delivery System for Increased Sustainability*, Order No. 20346, Public Service Commission of the District of Columbia, June 5, 2020, https://edocket.dcpsc.org/apis/api/filing/download?attachId=104691&guidFileName=9adc85df-6c7e-4aac-ba88-33461a51c75a.pdf.

[60] *Ibid.*, pp. 4-5.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Commission audit third parties' systems and processes to ensure compliance with Pepco's cybersecurity standards, as "this is a responsibility of the utility."[61] These decisions reflect a specific set of customer data protection issues and DC-specific factors. Nevertheless, a workshop convened by the Minnesota Commission could include discussions of how equivalent NDAs, third party auditing, and other measures might be applied to the protection of sensitive hosting capacity-related data.

The California Energy Systems for the 21st Century (CES-21) offers another model of potential value. Again, CES-21 protection measures focus on a different problem than hosting capacity-related data. In close coordination with California's Public Utility Commission, Pacific Gas and Electric (PG&E), San Diego Gas and Electric (SDG&E), and Southern California Edison (SCE) are collaborating with US National Laboratories on modeling and simulation of threat and response operations to evaluate the impacts of cyber threats on substation equipment. That effort includes classified information.[62] It is exceedingly unlikely that Minnesota energy developers will ever need access to classified information to advance their DER projects. Nevertheless, some of the information protection efforts underway in CES-21 might offer lessons learned for initiatives to protect the very highest-risk data required for such projects.

Workshop discussions could include analysis of other emerging models as well. For example, the Green Button Connect My Data (CMD) Standard is the energy-industry standard for enabling easy access to, and secure sharing of, utility-customer energy- and water-usage data. Utilities employing standards-based Green Button can enable their customers to securely transfer their data to third-party solution providers who can further assist them in monitoring and managing energy or water usage.[63] The objectives served by Green Button are very different from those of sharing sensitive grid data between utilities and energy developers. As with the other models examined in this white paper, however, opportunities may exist to leverage and repurpose the security techniques used by Green Button, especially since these techniques have been vetted by the Department of Energy.[64]

One additional model merits special attention by the workshop: the development of a multi-step process for tiering and securing access to sensitive data. Drawing on and modifying

[61] *Ibid*., p. 5.
[62] *Improving the Cybersecurity of the Electric Distribution Grid*, pp. 15-16, https://www.protectourpower.org/resources/vls-iee-pop.pdf.
[63] Green Button Connect My Data (CMD) Standard, https://www.greenbuttonalliance.org/assets/docs/Collateral/2020-04%20Green%20Button%20CMD%20and%20Certification%20Data%20Sheet.pdf.
[64] Green Button, Department of Energy, https://www.energy.gov/data/green-button#:~:text=Green%20Button%20Connect%20My%20Data%20is%20a%20new%20capability%20which,in)%20customer%20consent%20and%20control.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

recommendations from utilities in California[65] and other states, the following steps might comprise an overall approach to information sharing and security in Minnesota:

- Energy developers and other stakeholders seeking potentially sensitive grid information would request access to that data and (1) provide data sufficient to validate the identity of the requestor, and (2) provide the reason for requesting access to the data and their intended use.
- The stakeholders would also need to demonstrate sufficient ability to protect the requested data using appropriate standards.
- Once the utility validates the identity of the stakeholder requesting sensitive data, and determines that their reason for requesting access meets the objective "need to know" criteria approved in advance by the Commission, then the utility would provide the stakeholder with an NDA to govern the release, use, and protection of that data.
- Once the NDA is executed, the stakeholder would be authorized to access the data in a secure fashion.

These proposed steps provide only a basis for further discussion by workshop participants, and are sure to require revisions and additional measures. Nevertheless, they offer a useful starting point for discussion.

C. USING THE RISK HEAT MAP TO GUIDE TIERED ACCESS

Workshop participants should also consider using the risk heat map provided in Section V to help build a system for tiered access to particular types of grid information. Table 1 provides a notional matrix to support the development of such a system. After determining the data necessary to further the public interest, under this approach, the Commission, energy developers, Xcel Energy, and other grid stakeholders could categorize each of those data on the basis of (1) benefit of public access versus (2) level of risk to grid security posed by the release of that data.

[65] Rulemaking 08-08-009, *Joint Petition of Pacific Gas and Electric Company, San Diego Gas & Electric Company, and Southern California Edison Company for the Modification of D.10-12-048 and Resolution E-4414 To Protect the Physical and Cybersecurity of Electric Distribution and Transmission Facilities*, Public Utilities Commission of the State of California, Order Instituting Rulemaking to Continue Implementation and Administration of California Renewables Portfolio Standard Program, December 10, 2018.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Table 1: Matrix for Tiered Access

Benefit of Public Access: 0 = lowest, least benefit 1 = moderate benefit 2 = significant benefit 3 = essential				
	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
Grid Security Level Risk: U = Unrestricted; CI = Confidential Information; CRI = Confidential Restricted Information				

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

VII. WORKSHOP RECOMMENDATIONS AND BROADER CONCLUSIONS

The Commission Staff Briefing Papers recognize that "the tension between information and privacy and security identified by the Commission in the 2019 Order remains."[66] This white paper offers recommendations to help resolve that tension, and facilitate expanded sharing of data for DER project development while also protecting that data from foreign adversaries and domestic threats. However, insights from energy developers will be essential to build out and improve upon these recommendations. The same is true of Xcel Energy and other grid stakeholders, including those who would be responsible for managing the consequences of potentially catastrophic attacks on feeders to water systems and other infrastructure. Most important, Commission staff and Commissioners themselves will have unique perspectives on how to strike the balance between information sharing and security within their overall vision for Minnesota's future. A workshop to share these perspectives and build consensus on the way ahead is a prerequisite for success.

[66] Docket No. E002/M-19-685, *In the Matter of Xcel Energy's 2019 Hosting Capacity Analysis Report*, Staff Briefing Papers, June 11, 2020, p. 40.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

APPENDIX A: PROFESSIONAL QUALIFICATIONS

Paul Stockton is the President of Paul N Stockton LLC, a security advisory firm based in Santa Fe, NM. Dr. Stockton helps electric and natural gas system operators and their government partners strengthen energy sector resilience against increasingly severe threats.

Expertise on grid resilience and emerging cyber threats. As Assistant Secretary of Defense for Homeland Defense from 2009-2013, Dr. Stockton led the development of DOD's Strategy for Mission Assurance, which highlighted the foundational importance of the electric system for US defense and launched new partnerships with industry and DOE. After leaving office, Dr. Stockton wrote a pioneering NARUC analysis differentiating grid reliability from resilience. He subsequently published a series of studies to help strengthen BPS cyber resilience. The ESCC and DOE are currently implementing recommendations from one such report, *Resilience for Grid Security Emergencies: Opportunities for Industry-Government Collaboration*. Most recently, his works include Strengthening *the Cyber Resilience of the North American Energy Systems* (the Wilson Center, September 20) and *Securing the Grid from Supply-Chain Based Attacks* (Idaho National Laboratory, September 2020). Dr. Stockton chairs DOE's advisory subcommittee on Grid Resilience for National Security. He is also a member of NARUC's Emergency Preparedness, Recovery, and Resilience Task Force, and conducts cyber and grid-related research as a Senior Fellow of the Applied Physics Laboratory of Johns Hopkins University.

Grid operations. While serving as Assistant Secretary, Dr. Stockton led Defense support for DOE and power companies affected by Superstorm Sandy, including the first-ever use of DOD cargo aircraft to transport restoration assets. Building on that operational experience in *Superstorm Sandy: Implications for Developing a Post-Cyberattack Power Restoration System*, Dr. Stockton supported the ESCC's development of the cyber mutual assistance system and other initiatives to enable power restoration "under fire." He is currently helping the Defense Advanced Research Projects Agency (DARPA) develop new options to meet requests for assistance from BPS entities, including National Guard and US Cyber Command support for blackstart restoration in wide-area outages. He has also helped industry leaders and their government partners build preparedness for emergency operations in the GridEx IV and V Executive Tabletops, serving as the facilitator and contributing to the design of the exercises.

Meeting political and regulatory challenges. Dr. Stockton has frequently testified before US congressional committees and closely collaborates with Members and staff on resilience issues. He has testified at FERC reliability technical conferences and other meetings, and provided regulatory filings on grid reliability and resilience pricing. Dr. Stockton has served on seven NARUC conference panels on improving metrics and regulatory frameworks. In addition, he has made presentations to the Harvard Electricity Policy Group and other organizations on redesigning wholesale markets to further incentivize resilience investments.

Command of technical issues. Dr. Stockton has deep expertise on threats to ICS and grid equipment and operations. He has a current TS/SCI clearance and presents at classified E-ISAC technical conferences. He conducts studies and briefings for DHS and other organizations on EMP,

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

GMD, natural gas-electric system interdependencies, and managing the risks of combined cyberattacks on communications systems, the financial services sector, and the power grid.

Dr. Stockton holds a PhD from Harvard University and a BA from Dartmouth College. He was twice awarded the Department of Defense Medal for Distinguished Public Service, DOD's highest civilian award. The Department of Homeland Security also awarded Dr. Stockton its Distinguished Public Service Medal.

PUBLIC DOCUMENT – NOT PUBLIC DATA HAS BEEN EXCISED
Appendix B is NOT PUBLIC IN ITS ENTIRETY

Appendix B

A USE CASE FOR ASSESSING POTENTIAL CONSEQUENCES OF DISTRIBUTION SYSTEM ATTACKS: [NAME]

Dr. Paul N. Stockton

January 29, 2021

Non-Public Treatment Justification

Appendix B of Attachment A of our filing is not public in its entirety pursuant to Minn. Stat. § 13.37, subd. 1(a). This information is Security Information under Minn. Stat. § 13.37, subd. 1(a) and therefore designated as "Not Public." The disclosure of this information could substantially jeopardize the security of information or property against tampering, improper use, illegal disclosure, trespass, or physical injury.

Pursuant to Minn. R. 7829.0500, subp. 3, the Company provides the following description of the excised material:

1. **Nature of the Material:** Use Case of disruption of electric service to a critical infrastructure customer. In particular, the Appendix outlines the essential services provided by one of our critical infrastructure customers and the potential consequences disruption of our electric service to that customer's operations would have.
2. **Author(s):** Dr. Paul N. Stockton
3. **Importance:** The information could be used to guide disruption of an essential, critical infrastructure service by providing insights into the consequences and implications of such a disruption.
4. **Date the Information was Prepared**: January 2021

Appendix B is pages 34 – 37 of Attachment A

[PROTECTED DATA BEGINS

PROTECTED DATA ENDS]