WINTHROP WEINSTINE

ATTORNEYS AND COUNSELORS AT LAW

July 14, 2014

Eric F. Swanson
Direct Dial: (612) 604-6511
Direct Fax: (612) 604-6811
eswanson@winthrop.com

VIA E-FILING AND U.S. MAIL

Dr. Burl W. Haar
Executive Secretary
Minnesota Public Utilities Commission
121 East Seventh Place, Suite 350
St. Paul, MN 55101

RE: In the Matter of a Commission Inquiry Into Privacy Policies of Rate-Regulated Energy Utilities
MPUC Docket No. E, G-999/CI-12-1344

Dear Dr. Haar:

Enclosed please find the Petition for Rehearing and Reconsideration for CenterPoint Energy Minnesota Gas. This document has been filed with the e-Docket system and served on the attached service list. Also enclosed is our Affidavit of Service.

Very truly yours,

WINTHROP & WEINSTINE, P.A.

/s/ Eric F. Swanson

Eric F. Swanson

Enclosures

Cc: Service List

9283782v1

BEFORE FOR THE MINNESOTA PUBLIC UTILITIES COMMISSION
121 Seventh Place East, Suite 350
St. Paul, Minnesota 55101-2147

In the Matter of a Commission Inquiry Into Privacy Policies of Rate-Regulated Energy Utilities

MPUC Docket No. E, G-999/CI-12-1344

AFFIDAVIT OF SERVICE

STATE OF MINNESOTA)
) ss.
COUNTY OF HENNEPIN)

Mary G. Holly, of the City of Lake Elmo, County of Washington, the State of Minnesota, being first duly sworn, deposes and says that on the 14th day of July, 2014, she served the attached **Petition for Rehearing and Reconsideration** to all said persons on the attached Service List, true and correct copies thereof, by E-Filing and/or by depositing the same enclosed in an envelope, postage prepaid in the United States Mail in the post office at Minneapolis, Minnesota.

/s/ Mary G. Holly
MARY G. HOLLY

Subscribed and sworn to before me this
14th day of July, 2014.

/s/ Jane E. Justice
Notary Public

My Commission Expires: January 31, 2015

9283841v1

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Tamie A.	Aberle	tamie.aberle@mdu.com	Great Plains Natural Gas Co.	400 North Fourth Street Bismarck, ND 585014092	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Michael	Ahern	ahern.michael@dorsey.com	Dorsey & Whitney, LLP	50 S 6th St Ste 1500 Minneapolis, MN 554021498	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Kristine	Anderson	kanderson@greatermngas.com	Greater Minnesota Gas, Inc.	202 S. Main Street Le Sueur, MN 56058	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Arnie	Anderson	ArnieAnderson@MinnCAP.org	Minnesota Community Action Partnership	MCIT Building 100 Empire Drive, Suite 202 St. Paul, MN 55103	Paper Service	No	SPL_SL_12-1344_Interested Parties
Julia	Anderson	Julia.Anderson@ag.state.mn.us	Office of the Attorney General-DOC	1800 BRM Tower 445 Minnesota St St. Paul, MN 551012134	Electronic Service	Yes	SPL_SL_12-1344_Interested Parties
Martin S.	BeVier	bevi0022@umn.edu		4001 Grand Ave South # 3 Minneapolis, MN 55409	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Emma	Berndt	emma.berndt@opower.com	Opower	1515 N. Courthouse Rd. 8th Floor Arlington, VA 22201	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Scott	Bohler	scott.bohler@ftr.com	Frontier Communications Corporation	2378 Wilshire Blvd Mound, MN 55364-1652	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Jon	Braman	N/A	Bright Power, Inc.	11 Hanover Square, 21st floor New York, NY 10005	Paper Service	No	SPL_SL_12-1344_Interested Parties
Sheri	Brezinka	sbrezinka@usgbcmn.org	USGBC-Minnesota Chapter	5353 Wayzata Blvd Suite 350 Minneapolis, MN 55416	Paper Service	No	SPL_SL_12-1344_Interested Parties

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Peter	Brown	N/A	Minnesota Tenants Union	2121 Nicollet Ave Ste 203 Minneapolis, MN 55404	Paper Service	No	SPL_SL_12-1344_Interested Parties
Michael J.	Bull	mbull@mncee.org	Center for Energy and Environment	212 Third Ave N Ste 560 Minneapolis, MN 55401	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Cesar	Caballero	Cesar.Caballero@windstream.com	McLeodUSA Telecommunications Services, LLC	4001 Rodney Parham Little Rock, AR 72212	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Richard	Carter	rick.carter@lhbcorp.com		371 Water Street Excelsior, MN 55331	Paper Service	No	SPL_SL_12-1344_Interested Parties
Brent	Christensen	bchristensen@mnta.org	Minnesota Telecom Alliance	1000 Westgate Drive, Ste 252 St. Paul, MN 55117	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Andrew	Clearwater	N/A	Future of Privacy Forum	919 18th Street N.W. Suite 901 Washington, DC 20006	Paper Service	No	SPL_SL_12-1344_Interested Parties
Roger	Colton	roger@fsconline.com		34 warwick road belmont, ma 02478	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Ian	Dobson	ian.dobson@ag.state.mn.us	Office of the Attorney General-RUD	Antitrust and Utilities Division 445 Minnesota Street, 1400 BRM Tower St. Paul, MN 55101	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Steve	Downer	sdowner@mmua.org	MMUA	3025 Harbor Ln N Ste 400 Plymouth, MN 554475142	Electronic Service	No	SPL_SL_12-1344_Interested Parties

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Jennifer	Edwards	jedwards@mceee.org	Center for Energy and Environment	212 3rd Ave. N. Ste 560 Minneapolis, MN 55401	Paper Service	No	SPL_SL_12-1344_Interested Parties
Sharon	Ferguson	sharon.ferguson@state.mn.us	Department of Commerce	85 7th Place E Ste 500 Saint Paul, MN 551012198	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Janne	Flisrand	janne@mngreencommunities.org	MN Green Communities	c/o Flisrand Consulting 2112 Dupont Ave. S Minneapolis, MN 55405	Paper Service	No	SPL_SL_12-1344_Interested Parties
Bill	Gullickson	wdgvc76@yahoo.com		1819 Colfax Avenue S Minneapolis, MN 55403	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Burl W.	Haar	burl.haar@state.mn.us	Public Utilities Commission	Suite 350 121 7th Place East St. Paul, MN 551012147	Electronic Service	Yes	SPL_SL_12-1344_Interested Parties
Ryan	Hentges	ryanh@mvec.net	Minnesota Valley Electric Cooperative	125 Minnesota Valley Electric Dr Jordan, MN 55352	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Mike	Hickey	N/A	National Federation of Independent Business/MN	380 Jackson Street, Suite 780 St. Paul, MN 55101	Paper Service	No	SPL_SL_12-1344_Interested Parties
Caroline	Horton	N/A	Aeon	901 N. 3rd St. Suite 150 Minneapolis, MN 55401	Paper Service	No	SPL_SL_12-1344_Interested Parties
Lori	Hoyum	lhoyum@mnpower.com	Minnesota Power	30 West Superior Street Duluth, MN 55802	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Paula	Johnson	paulajohnson@alliantenergy.com	Alliant Energy-Interstate Power and Light Company	P.O. Box 351 200 First Street, SE Cedar Rapids, IA 524060351	Electronic Service	No	SPL_SL_12-1344_Interested Parties

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Craig	Johnson	N/A	League of Minnesota Cities	145 University Ave. W. Saint Paul, MN 55103-2044	Paper Service	No	SPL_SL_12-1344_Interested Parties
Joel	Johnson	joel@mrea.org	Minnesota Rural Electric Association	11640 73rd Ave N Maple Grove, MN 55369	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Steve	Kismohr	skismohr@mwalliance.org	Midwest Energy Efficiency Alliance	20 N. Wacker Drive Suite 1301 Chicago, IL 60606	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Andrea	Krukowski	andrea@imt.org	Institute for Market Transformation	1707 L Street NW Ste 1050 Washington, DC 20036	Paper Service	No	SPL_SL_12-1344_Interested Parties
Nicolle	Kupser	nkupser@greatermngas.com	Greater Minnesota Gas, Inc.	202 South Main Street P.O. Box 68 Le Sueur, MN 56058	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Douglas	Larson	dlarson@dakotaelectric.com	Dakota Electric Association	4300 220th St W Farmington, MN 55024	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Kevin	Lewis	kl@bomampls.org	Greater Minneapolis BOMA	Suite 610 121 South 8th Street Minneapolis, MN 55402	Paper Service	No	SPL_SL_12-1344_Interested Parties
Todd	Liljenquist	N/A	Minnesota Multi Housing Association (MHA)	1600 West 82nd Street, Suite 110 Minneapolis, MN 55431	Paper Service	No	SPL_SL_12-1344_Interested Parties
Alison	Lindburg	lindburg@fresh-energy.org	Fresh Energy	408 St. Peter St Ste 220 St. Paul, MN 55102	Paper Service	No	SPL_SL_12-1344_Interested Parties
John	Lindell	agorud.ecf@ag.state.mn.us	Office of the Attorney General-RUD	1400 BRM Tower 445 Minnesota St St. Paul, MN 551012130	Electronic Service	Yes	SPL_SL_12-1344_Interested Parties

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Kevin	Marquardt	Kevin.Marquardt@CenterPointEnergy.com	CenterPoint Energy	800 LaSalle Avenue, Floor 14 Minneapolis, Minnesota 55402	Electronic Service	No	SPL_SL_12-1344_Interested Parties
J.B.	Matthews	N/A	Cushman & Wakefield/NorthMarq	3500 American Blvd W - #200 Minneapolis, MN 55431	Paper Service	No	SPL_SL_12-1344_Interested Parties
Bridget	McLaughlin	bmclaughlin@mncee.org	Center for Energy & Environment	212 3rd Ave N Ste 560 Minneapolis, MN 55401	Electronic Service	No	SPL_SL_12-1344_Interested Parties
David	Moeller	dmoeller@allete.com	Minnesota Power	30 W Superior St Duluth, MN 558022093	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Andrew	Moratzka	apmoratzka@stoel.com	Stoel Rives LLP	33 South Sixth Street Suite 4200 Minneapolis, MN 55402	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Greg	Palmer	gpalmer@greatermngas.com	Greater Minnesota Gas, Inc.	PO Box 68 202 South Main Street Le Sueur, MN 56058	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Adam	Pyles	adam.pyles@centerpointenergy.com	CenterPoint Energy	800 LaSalle Avenue PO Box 59038 Minneapolis, MN 554590038	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Phyllis	Reha	phyllisreha@gmail.com		3656 Woodland Trail Eagan, MN 55123	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Richard	Savelkoul	rsavelkoul@martinsquires.com	Martin & Squires, P.A.	332 Minnesota Street Ste W2750 St. Paul, MN 55101	Electronic Service	No	SPL_SL_12-1344_Interested Parties

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Kevin	Saville	kevin.saville@ftr.com	Citizens/Frontier Communications	2378 Wilshire Blvd. Mound, MN 55364	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Janet	Shaddix Elling	jshaddix@janetshaddix.com	Shaddix And Associates	Ste 122 9100 W Bloomington Frwy Bloomington, MN 55431	Paper Service	No	SPL_SL_12-1344_Interested Parties
Brendon	Slotterback	brendon.slotterback@minneapolismn.gov	City of Minneapolis	350 S 5th Street, Room M315 Minneapolis, MN 55415	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Peggy	Sorum	peggy.sorum@centerpointenergy.com	CenterPoint Energy	800 LaSalle Avenue PO Box 59038 Minneapolis, MN 554590038	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Ron	Spangler, Jr.	rlspangler@otpco.com	Otter Tail Power Company	215 So. Cascade St. PO Box 496 Fergus Falls, MN 565380496	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Cary	Stephenson	cStephenson@otpco.com	Otter Tail Power Company	215 South Cascade Street Fergus Falls, MN 56537	Electronic Service	No	SPL_SL_12-1344_Interested Parties
SaGonna	Thompson	Regulatory.Records@xcelenergy.com	Xcel Energy	414 Nicollet Mall FL 7 Minneapolis, MN 554011993	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Jason	Topp	jason.topp@centurylink.com	CenturyLink	200 S 5th St Ste 2200 Minneapolis, MN 55402	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Gregory	Walters	gjwalters@minnesotaenergyresources.com	Minnesota Energy Resources Corporation	3460 Technology Dr. NW Rochester, MN 55901	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Patricia	Whitney	N/A	St. Paul Assn of Responsible Landlords	2197 Silver Lake Road NW New Brighton, MN 55112	Paper Service	No	SPL_SL_12-1344_Interested Parties

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
Elizabeth	Wilson	N/A	Humphrey School of Public Affairs	130 Humphrey School 301 19th Ave. S Minneapolis, MN 55455	Paper Service	No	SPL_SL_12-1344_Interested Parties
Josh	Winters	N/A	MPIRG	2722 University Ave SE Minneapolis, MN 55414	Paper Service	No	SPL_SL_12-1344_Interested Parties
Robyn	Woeste	robynwoeste@alliantenergy.com	Interstate Power and Light Company	200 First St SE Cedar Rapids, IA 52401	Electronic Service	No	SPL_SL_12-1344_Interested Parties

BEFORE THE MINNESOTA PUBLIC UTILITIES COMMISSION
121 Seventh Place East, Suite 350
St. Paul, Minnesota 55101-2147

Beverly Jones Heydinger	Chair
David C. Boyd	Commissioner
Nancy Lange	Commissioner
Dan Lipschultz	Commissioner
Betsy Wergin	Commissioner

In the Matter of a Commission Inquiry Into Privacy Policies of Rate-Regulated Energy Utilities	MPUC Docket No. E, G-999/CI-12-1344 **PETITION FOR REHEARING AND RECONSIDERATION**

Pursuant to Minnesota Statutes § 216B.27 and Minnesota Rules Part 7829.3000, CenterPoint Energy - Minnesota Gas ("CenterPoint Energy" or "Company") files this Petition For Rehearing And Reconsideration of the Minnesota Public Utilities Commission's ("Commission") June 24, 2014 Order Requiring Utilities to Adopt and Document Processes Regarding Personally Identifiable Information and Other Action ("Order") in the above-captioned matter.

INTRODUCTION

CenterPoint Energy takes the issue of customer privacy extremely seriously and seeks to work cooperatively with all interested parties to help safeguard the privacy and security of personal information of its customers. For example, as the Company has discussed in prior comments, all of the Company's data systems that hold personal information on its customers are assessed and managed according to CenterPoint Energy's Cyber Security Plan ("Plan") and related IT policies and procedures.

CenterPoint Energy Inc.'s Houston electric operations developed that Plan as a component of a grant from the United States Department of Energy ("DOE"). However, the Plan has been implemented across the CenterPoint operations, including the Minnesota Gas operations. Moreover, the DOE conducts an annual assessment of the Company's execution of the Plan for the Houston electric operations, including annual site visits. The site visits include a review of documentation that the Plan is being implemented as approved by DOE and verification that any cyber security deficiencies or areas of concern from the previous site review are being addressed. Any necessary improvements identified in these reviews are also implemented across the Company's regulated operations data systems, including those utilized by the Minnesota Gas operations.

CenterPoint Energy also takes compliance with Commission Orders extremely seriously. For that reason, the Company has already invested substantial time and effort in analyzing the Commission Order and attempting to determine the implications of the Order on the Company, its operations and its customers. CenterPoint's efforts lead it to respectfully request reconsideration of the Order in three respects.

First, the Order establishes a definition of "Personally Identifiable Information" ("PII"), suggested by Staff and then modified on the day of the Commission Agenda Meeting on this matter. That definition would apply to all rate-regulated energy utilities. The Order then seeks to establish a number of standards and requirements, again modified on the day of the Commission Agenda Meeting, that all rate-regulated energy

utilities must follow going forward regarding their handling and use of "customer PII data."

Unfortunately, when compared to the Minnesota Statutes definition of "personal information," the Commission's definition of "PII" is broad and open-ended. Moreover, when combined with the Commission's specific standards and requirements, this definition creates substantial and unnecessary ambiguity and uncertainty. Those ambiguities and uncertainties, in turn, create difficulty in determining how to comply with the Commission Order (if compliance is even possible) without imposing significant costs and potentially hindering the ultimate goal of protecting sensitive customer data.

As discussed below, the Order's definition of PII – sourced from the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53 – was never intended by NIST to be combined with privacy and security requirements such as those set forth in the Order. Rather, the broad definition was intended to serve as a starting point for companies to consider in developing risk-based and risk-appropriate privacy and security controls. As a result of using the SP 800-53 definition of PII outside of its intended purposes, the Order imposes on utilities privacy and security requirements that exceed any legal privacy or security requirements applicable to any U.S. businesses, including those widely accepted to handle personal information that is much more sensitive than that handled by utilities, such as banks, credit card companies and other financial institutions, hospitals, health care plans, and federal government agencies and their contractors. While excessively costly and burdensome on both utilities and their

customers, the Order's requirements do not enhance the privacy or security of customer information.

Second, other aspects of the Commission Order are either ill-defined, creating ambiguity and potentially imposing significant costs, or fashioned in a manner that could have the unintended effect of *increasing* the risk of security breaches. For example, the Order requires that before providing any of the Commission-defined PII information to third party contractors, utilities would need to require each contractor to provide "equivalent or greater protection for the customer data" as the utility itself provides. In adopting this requirement, the Commission again imposes burdens on utilities greater than those placed on other businesses. Moreover, it remains unclear how utilities can verify that its contractors have "equivalent or greater protections in place" without substantial sharing of multiple parties' data protection practices – sharing that could create new avenues for security breaches.

Third, the Commission cannot adopt statements of general applicability and future effect without complying with the Minnesota Administrative Procedure Act. As discussed below, the actions contemplated by the Commission's Order require a rulemaking proceeding, where all issues can be thoroughly vetted to ensure against unintended consequences or excessive costs – costs which will ultimately be borne by ratepayers. Further, failure to follow the proper procedure can invalidate the Commission's actions, ultimately providing no benefit to any of the concerned parties or the Commission.

Therefore, CenterPoint Energy respectfully requests that the Commission reconsider its Order and open a rulemaking proceeding to address the customer data privacy issues addressed in the Order. Alternatively, and without waiving its procedural objections, the Company submits that the Commission must, at minimum, reconsider its definition of PII and clarify various aspects of its Order.

I. THE COMMISSION DEFINITION OF PII IS OVERLY BROAD FOR THE PURPOSES OF THIS DOCKET.

The Order establishes the term "personally identifiable information," crafted on the day of the Commission Agenda Meeting and adapted from a definition used by the National Institute of Standards and Technology ("NIST"), to be used throughout the new requirements established by the Order. Parties orally raised concerns on the record regarding this definition. Specifically, parties raised concerns regarding how this definition would interplay with the list of "Commission principles" and other potential ordering points, and what challenges or difficulties might arise that would ultimately impose new costs on the utilities and their ratepayers. For example, while a customer's name, address and phone number may constitute PII, that information is readily and publicly available through any number of other sources, including the white pages or the most rudimentary internet search. Upon reviewing the Order, the concerns raised by parties at the Commission Agenda Meeting were well founded.

In its Order, the Commission creates its own adaption of a NIST definition, as follows:

> Personally Identifiable Information (PII) shall be defined as "customer PII data which can be used to distinguish or trace the identity of an individual

> (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.)."[1]

The definition of PII is extremely broad and encompasses data ranging from a Social Security number to information that is publicly available such as an individual's name, telephone number and email address, to other known and yet-unknown data that could be used, by itself or in combination with other data, to identify or trace an individual. The Commission adopted this broad NIST-based definition of PII despite the Commission's own rightful observation, with respect to utilities' collection and use of Social Security numbers, that there is "no reason why state utilities should be subject to standards more restrictive than those imposed on other state businesses."[2] This rationale is equally applicable to the broader definition of personal information.

Like other businesses' practices, utilities' personal information practices must reflect the nature of the business, the sensitivity of personal information processed by utilities, and the nature of utilities' personal information practices. The Commission's decision to broadly apply the SP 800-53 definition of PII to utilities is contrary to this risk-based approach. In fact, NIST developed the SP 800-53 definition of PII to apply to federal agencies and their contractors, arguably the only organizations whose information practices are likely even more sensitive than those of financial institutions and health-

[1] Order, p. 5 (sourcing NIST SP 800-53).
[2] Order (p. 6).

related entities.[3] The SP 800-53 definition is meant to serve as a departure point for those organizations to assess their privacy and security practices and then follow SP 800-53, SP 800-122 and other NIST resources to select and implement privacy and security controls that the organizations determine to be commensurate with their risk-based requirements.[4] NIST never intended the definition of PII, in its entirety, to apply to a specific set of privacy and security requirements such as those established by the Order and other privacy and data security laws employ significantly narrower definitions.[5] The definition is also much broader than the definition of "personal information" found in Minnesota Statutes, as discussed further below.[6]

CenterPoint Energy respectfully submits that the Commission must keep in mind the purpose and use of the NIST definitions and guidelines.[7] The NIST SP 800-53 PII definition is broad because it is associated with NIST publications/guides that give

[3] SP 800-53, Rev. 4 Ch. 1 p. 2 ("The purpose of this publication is to provide guidelines for selecting and specifying security controls **for organizations and information systems supporting the executive agencies of the federal government** to meet the requirements of FIPS Publication 200.") (Emphasis added.)

[4] NIST states in SP 800-53 that "organizations analyze and apply each privacy control with respect to their distinct mission/business and operation needs based on their legal authorities and obligations. ***Implementations of the privacy controls may vary based upon this analysis***." NIST Special Publication 800-53, Rev. 4 (April 2013, updated January 15, 2014) at J-4 (emphasis added). SP 800-122 further notes that "All PII is not created equal. PII should be evaluated to determine its PII confidentiality impact level … so that appropriate safeguards can be applied to the PII. The PII confidentiality impact level – low, moderate, or high – indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed." NIST Special Publication 800-122 (April 2010) at ES-2.

[5] For example, the Commission's definition of PII is broader than the definitions of personal information applicable to banks and other financial institutions under the federal Gramm-Leach-Bliley Act ("GLBA") and federal and state regulations implementing the act which, among other things, explicitly excludes publicly available information from the scope of its privacy and security requirements). *See* 15 U.S.C. §§ 6801-6809; 16 C.F.R. Parts 313, 314; 12 C.F.R. Part 30; 12 C.F.R. Part 208 and 225, etc. The definition is also broader than that applicable to health care providers and health plans under the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") and the U.S. Department of Health and Human Services ("HHS") regulations that implement these laws. *See* 45 C.F.R. Parts 160, 164; 45 C.F.R. §§ 164.400-414.

[6] *See* Minn. Stat. § 325E.61.

[7] There appeared to be confusion during the Commission Agenda Meeting as to whether utilities were already "required" to comply with NIST guidelines. They are not. However, companies such as CenterPoint Energy have certainly considered the NIST guidelines in efforts such as the development of its Cyber Security Plan.

organizations significant leeway in adopting safeguards based on the sensitivity of the information they possess. In this context, a broad definition makes sense to allow organizations to consider the full array of information they may possess in designing their risk-based approach to privacy and security. However, these NIST documents do *not* require specific safeguards for the entire scope of the PII an organization may collect and possess and the PII definition in SP 800-53 does not reflect the scope of information that should be subject to specific controls or restrictions. Instead, the NIST definition and guidelines achieve a balance – providing a broad definition of PII, while not imposing mandates but retaining flexibility.

NIST designed SP 800-53 to provide guidelines for selecting and configuring controls for organizations to manage security and privacy risks (similarly, SP 800-122 is intended to provide guidelines on the development and implementation of a risk-based approach to protecting the confidentiality of PII). NIST addresses this flexibility explicitly, noting that:

> "[o]rganizations analyze and apply each privacy control with respect to their distinct mission/business and operation needs based on their legal authorities and obligations. Implementations of the privacy controls may vary based upon this analysis."[8] "***All PII is not created equal***. PII should be evaluated to determine its PII confidentiality impact level … so that appropriate safeguards can be applied to the PII. The PII confidentiality impact level – low, moderate, or high – indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed…. Organizations should apply appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level."[9]

[8] NIST Special Publication 800-53, Rev. 4 at J-4 (emphasis added).
[9] NIST Special Publication 800-122 (April 2010) at ES-2.

The balance and flexibility achieved by the NIST definitions of PII and guidelines is lost when the Commission's broad definition of "PII" is combined with specific privacy and security requirements such as certain of the Order's requirements, without regard for the sensitivity and risk associated with that data. For example, the Order requires that a utility:

- collect and maintain **only** the PII needed to perform its regulated utility business functions;
- share **any** PII data for a purpose other than related to regulated utility service only after the utility obtains explicit, written consent from the customer that includes a clear statement of the information to be shared and with whom it will be shared;
- control and limit access to **any** PII data to those employees who need it for an identified business purpose;
- not provide **any** necessary PII to a contractor for a regulated purpose, unless the contractor is required to provide equivalent or greater protection for the PII by which the utility must abide (by implication, including the non-discretionary Commission principles); and
- promptly notify affected customers, the Commission, the Department, and the Attorney General's Office in the event of an unauthorized use or release of customer PII data.[10]

Given the Commission's broad definition of PII, each of these requirements raises concerns, imposes unreasonable burden and likely imposes excessive costs. For example, the Commission requires that utilities "shall control and limit access to customer PII data to those employees who need it for an identified business purpose."[11] By its terms, the Order requires CenterPoint Energy to control and limit access to virtually all information it has regarding its customers, including publicly available information, to only "those

[10] *See* Order, p. 7.
[11] *Id.*

employees who need it for an identified business purpose." While access controls are an important element in safeguarding the privacy and security of personal information, access limitations within any organization, including a utility, must be tailored to the sensitivity of the PII. Strict access controls are justified for sensitive PII, not for all PII. Even SP 800-53 does not, for example, recommend "least privilege" access controls for low-risk PII.[12] In contrast, the Order mandates access controls for **all** PII. Again, CenterPoint Energy is aware of no equivalent federal or state law mandating such broad restrictions, and there is no justification in imposing this requirement on utilities. The Company has not had sufficient time to determine how it would comply with such a requirement or what it would cost to achieve such compliance and no public interest is served or protected by restricting employee access to publicly available information.

The Order further requires that:

> in the event of an unauthorized disclosure or use of customer PII data, a utility will be obligated to promptly notify its affected customers, the Commission, the Department, and the Office of the Attorney General. In its notice, the utility should include at least the following information: the number of customers affected; the date or period of the breach; the types of data inappropriately accessed; and whether the source or cause of the breach has been identified and provided to law enforcement officials.[13]

By its plain language, and given the breadth of the definition of PII, the Order requires a utility to notify affected customers and others in the event that employees who do not "need it for an identified business purpose" access virtually any personal information on any CenterPoint Energy customer, even in the most benign of circumstances such as an employee accessing customer name, address and e-mail

[12] *See* SP 800-53, Rev. 4 p. 108.
[13] *Id*. (emphasis added).

information if that employee does not "need it for an identified business purpose."[14] This requirement does not enhance the privacy or security of the information. Moreover, this requirement likely compromises the safeguarding of privacy and security by encouraging over-notification of customers, triggering confusion and frustration as customers receive notifications of "unauthorized disclosures" that pose no privacy or security risk, and desensitizing them to incidents that do. Further, this aspect of the Order again imposes yet to be determined costs, either of notifications or of putting in place stringent limitations to access.

As is the case with the handling of Social Security numbers, the Minnesota legislature has already determined the appropriate circumstances in which Minnesota residents should be notified of privacy and security breaches, by enacting the state's breach notification law. There is no reason for the Commission to substitute its own judgment for that of the legislature on this issue, or to require Minnesota utilities to comply with requirements that are far more demanding than those applicable to other Minnesota businesses. The statutes provide that:

> Any person or business that maintains data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[15]

[14] In this regard, CenterPoint Energy would note that the Order fails to exempt from the definition of a reportable breach an incident that results from inadvertent access to personal information by an employee or contactor, if there is no further misuse of the information – an exemption common in breach notification laws, or to provide similar common exemptions. *See*, *e.g.*, 45 C.F.R. §§ 164.400-414.

[15] Minn. Stat. § 325E.61, subd. 1(b).

The statutes impose the notification obligation in situations deserving of such notification by also establishing an appropriately tailored definition of "personal information," as follows:

> "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:
>
> (1) Social Security number;
>
> (2) driver's license number or Minnesota identification card number; or
>
> (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[16]

When it considered the issue of Social Security numbers, the Commission found that it could "ascertain no reason why state utilities should be subject to standards more restrictive than those imposed on other state businesses."[17] The same logic should apply here -- Minnesota Statutes already define personal information and impose requirements to give customers notice in the event of an unauthorized use or disclosure of the information. There has been no showing that Minnesota utilities should face more stringent requirements that any other Minnesota business in this regard.

The Commission's overly broad definition of PII causes further mischief when applied to the matter of sharing PII with contractors. The Order states:

---

[16] *Id*., subd. 1(e).
[17] Order, p. 6.

> The Commission will allow a utility to share necessary customer PII data with a contractor for a regulated business purpose, so long as the contractor is required to provide equivalent or greater protection for the customer data.[18]

Combining this requirement with the Commission's definition of PII again leads to absurd results that do not advance the public interest. Under the plain language of the Order, before CenterPoint can share even publicly available information such as a customer's name, address and telephone information with a contractor who may be engaged to paint a customer's meter, CenterPoint will need to require the contractor to provide "equivalent or greater protection for the customer data" as CenterPoint itself provides. As noted above, CenterPoint Energy has in place a Cyber Security Plan developed to meet DOE requirements and annually reviewed by the DOE including on-site visits. It is utterly impracticable for CenterPoint Energy to require each of its third party contractors to have in place such extensive data protection requirements before providing the basic information necessary so that those contractors can assist CenterPoint Energy in performing its regulated utility services.[19]

For all of these reasons, the Commission must reconsider this matter and adopt a definition of "PII" appropriate for the uses to which the Commission intends.

II. OTHER ASPECTS OF THE COMMISSION ORDER CREATE AMBIGUITIES AND UNINTENDED CONSEQUENCES.

In addition to the difficulties created by the Commission definition of "PII," other aspects of the Order create ambiguities or unintended consequences that require

[18] Order, p. 7 (emphasis added).
[19] Moreover, any such requirements will undoubtedly disadvantage small businesses who lack the resources necessary to employ sophisticated cyber security plans.

reconsideration. For example, the Order prohibits utilities from sharing customer information with third party contractors unless "the contractor is required to provide equivalent or greater protection for the customer data" as that provided by the utility itself.[20]

In addition to the practicability requirements discussed above, the Order does not specify how utilities will demonstrate to the Commission that it has "required" its contractors to "provide equivalent or greater protection" than the utility itself. Certainly, having contractors to commit to protect all PII is a generally reasonable requirement when combined with an appropriate definition of PII. However, in CenterPoint Energy's experience, many companies understandably refuse to provide specific or detailed information on the measures they have taken to protect and secure data. After all, the more that is known about any companies' specific cyber security measures, the greater risk of an eventual security breach. Moreover, the Company cannot independently verify the efficacy of any third party's security measures without incurring substantial new costs that will be borne by ratepayers. Even then, full and independent verification that a contractor has "equivalent or greater protection" in place may be impossible without also disclosing CenterPoint's owns specific data protection measures to its contractors – again increasing, not reducing, the risk of security breaches. For those reasons, rather than mandating a comparison to assure "equivalent or greater protections," data privacy and security measures more typically require service providers obtaining PII data to conduct

[20] Order, p. 7 (emphasis added).

themselves "in accordance with reasonable policies and procedures" to protect any sensitive customer data.[21]

III. MINNESOTA ADMINISTRATIVE PROCEDURE ACT REQUIRES THE COMMISSION TO FOLLOW THE RULEMAKING PROCESS IN THIS INSTANCE.

CenterPoint Energy respectfully submits that the infirmities in the Commission Order addressed above could have been avoided had the Commission followed appropriate procedures. There can be no doubt that in its Order the Commission has adopted statements of "general applicability and future effect" – the Minnesota Administrative Procedure Act's definition of a rule.[22] First, the Order establishes the term "personally identifiable information," adapted from a definition used by the NIST,[23] to be used throughout the new requirements established by the Order. Specifically, the Commission defines PII as follows:

> Personally Identifiable Information (PII) shall be defined as "customer PII data which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.)." (Source: NIST's Security and Privacy Controls for Federal Information Systems and Organizations; 800-53; April 2013). [24]

The Order then uses that definition to establish "the principles and guidelines that the Commission will require utilities to follow, as set forth below," including:

---

[21] For example, the Red Flags Rule states, with regard to oversight of service provider arrangements, "Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft."

[22] Minn. Stat. § 14.02, subd. 4.

[23] Order, p. 5.

[24] Order, p. 5 (emphasis added).

- Requiring utilities to adopt and document the internal processes used to collect and protect customer PII data, after ensuring that the processes used are consistent with the protections set forth in NIST's Guide to Protecting the Confidentiality of Personally Identifiable Information (800-122; April 2010);

- Requiring that utilities collect and maintain only the customer PII data needed to perform its regulated utility business functions;

- Requiring utilities to give the customer clear and accurate information about how the customer PII data will be used and protected;

- Requiring utilities to use customer PII data solely for the purposes for which it was collected, unless prior written consent is clearly given by the affected customer, with that written consent including "a clear statement of the information to be shared and with whom it will be shared" and the consent effective "for no more than one year or the contract term, subject to renewal," unless earlier revoked by the customer;

- Requiring that utilities control and limit access to customer PII data to those employees who need it for an identified business purpose;

- Requiring utilities to submit its customer notice to the Commission for review;

- Requiring that, to the extent that utilities must share customer PII data with a contractor for a regulated business purpose, the utility must first ensure that the contractor will provide "equivalent or greater protection for the customer data" but that, regardless, the Commission will hold utilities responsible to the customer in the event of a contractor's unauthorized use or release of data; and

- Requiring all utilities to make compliance filings within 60 days "showing that it has policies consistent with this Order."[25]

By its terms, the Order (1) applies to all rate-regulated energy utilities and (2) imposes a series of specific requirements with respect to utilities' collection and use of the newly defined term "customer PII data." Moreover, since the definition of PII and the specific requirements being placed on utilities were distributed and then modified on

[25] *Id*., pp. 6-7.

the day of the Commission Agenda Meeting in this matter, the Order imposes these new requirements with little information regarding the costs, burdens, unintended consequences, potential pitfalls and substantial ambiguities regarding just what these new "requirements" mean and how they will be enforced. Due process to all concerned parties, including utility customers, demands more.

As Minnesota Statutes make clear:

> "Rule" means every agency statement of general applicability and future effect, including amendments, suspensions, and repeals of rules, adopted to implement or make specific the law enforced or administered by that agency or to govern its organization or procedure.[26]

The requirements set forth in the Order fit squarely within this definition.[27] However, a Commission Order imposing such requirements without following rulemaking procedures is invalid.[28] As both the legislature and the Minnesota Supreme Court have recognized "all rules, including interpretative rules, must be adopted in accordance with the Minnesota Administrative Procedure Act."[29]

To the extent the Commission believes that new statements of general applicability and future effect promulgated by this Commission are required on customer privacy issues, a Minnesota Statutes Chapter 14 rulemaking proceeding provides the vehicle for accomplishing that task. Through the rulemaking process, all parties will have the ability to comment in writing and present relevant evidence bearing on the need

---

[26] Minn. Stat. § 14.02, subd. 4 (emphasis added).
[27] The legislature has listed several exceptions to the requirement to follow rulemaking procedures. None of them apply here. Minn. Stat § 14.03 (listing exceptions to the rulemaking procedural requirements).
[28] *Johnson Bros. Wholesale Liquor Co. v. Novak*, 295 N.W.2d 238 (Minn. 1980).
[29] *White Bear Lake Care Center v. Minnesota Dep't of Pub. Welfare*, 319 N.W.2d 7, 8-9 (Minn. 1982), citing Minn. Stat. § 14.45 ("In proceedings under section 14.44, the court shall declare the rule invalid if it finds that it violates constitutional provisions or exceeds the statutory authority of the agency or was adopted without compliance with statutory rulemaking procedures.") (Emphasis added.)

for and reasonableness of these new requirements. Such a process allows the Commission to be deliberative, to act where necessary and reasonable to achieve its desired objectives, and to establish clear and well-grounded rules.

In contrast, in the current proceeding Commission Staff and the Commission first presented the Commission's definition of "PII" and the associated new requirements on the day of the hearing, modifying those requirements in real time during the hearing. The Minnesota Administrative Procedure Act simply does not allow for such *ad hoc* rulemaking.

CONCLUSION

All parties and the Commission agree on the importance of protecting the privacy and security of sensitive customer data. Indeed, CenterPoint Energy and others have already commented on the many requirements in place in federal and state law to protect against unauthorized use or release of such data. Given that substantial body of existing law, any further steps to help ensure against identity theft requires careful and measured action to avoid creating unintended consequences or imposing excessive costs. CenterPoint Energy respectfully submits that the Order fails to deliver such a careful and measured action.

Further, to the extent that the Commission sees a need for it to act in this arena by imposing new requirements on utilities that have general applicability and future effect, Minnesota law requires that the Commission follow the processes established by the Minnesota Administrative Procedure Act. That process provides a thorough vetting of

the need for and the reasonableness of any proposed Commission action – something not provided by the process followed to date.

Therefore, for all of the reasons discussed above, CenterPoint Energy respectfully requests that the Commission reconsider its Order in this matter, that it specifically reconsider its definition of "PII," and that it open a rulemaking docket to address these critical issues.

Dated: July 14, 2014

WINTHROP & WEINSTINE, P.A.

By: /s/ Eric F. Swanson
Eric F. Swanson

225 South Sixth Street, Suite 3500
Minneapolis, Minnesota 55402
(612) 604-6400

ATTORNEYS FOR CENTERPOINT ENERGY MINNESOTA GAS

9256153v5