Minnesota Public Utilities Commission

Staff Briefing Paper

Meeting Date: September 4, 2014 ..... ** Agenda Item # _____

Company: All Rate-Regulated Utilities

Docket No. E, G999/CI-12-1344
In the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities

Issues:
1. Should the Commission reconsider or reopen its *June 24th Order*?
2. If so, should the *June 24th Order* be modified?

Please Note: Minn. Rules 7829.3000, subp. 6, states that "[t]he commission shall decide a petition for rehearing, amendment, vacation, reconsideration, or reargument with or without a hearing or oral argument. The commission may vacate or stay the order, or part of the order, that is the subject of the petition, pending action on the petition.

Staff: Kevin O'Grady.....651-201-2218
Michelle Rebholz.....651-201-2206

The attached materials are work papers of Commission Staff. They are intended for use by the Public Utilities Commission and are based upon information already in the record unless noted otherwise.

This document can be made available in alternative formats (e.g., large print or audio) by calling 651-296-0406 (voice). Persons with hearing loss or speech disabilities may call us through their preferred Telecommunications Relay Service.

Relevant Documents

Commission *Order*..... June 24, 2014
CenterPoint Petition for Reconsideration .....July 14, 2014
Comments: Xcel .....July 24, 2014
Comments: Otter Tail Power .....July 24, 2014
Comments: Minnesota Power.....July 25, 2014
NIST Guide (Special Publication 800-122)..... April, 2010

Background

On March 5, 2012, Xcel filed a proposed privacy tariff, assigned to Docket 12-188. After receiving comments and considering the matter, the Commission opted to open a generic docket, the current docket. The Commission split the privacy inquiry into three tracks: first, on the FTC's Red Flags Rule; second, on Personally Identifiable Information (PII); and third, on Customer Energy Usage Data (CEUD).

On June 24, 2014, the Commission issued its *Order* related to Track 2, PII. That *Order* established a definition of PII and terms for protection of PII.

On July 14, 2014, CenterPoint Energy (CPE) filed a request for reconsideration of the Commission's *Order*.

On July 24, 2014, Xcel and Otter Tail Power (OTP) filed comments in support of CPE's petition.

On July 25, 2014, Minnesota Power (MP) filed comments in support of CPE's petition.

Rules Guiding Reconsideration

Commission rules make provision for reconsideration of an order:

> The commission shall decide a petition for rehearing, amendment, vacation, reconsideration, or reargument with or without a hearing or oral argument. The commission may vacate or stay the order, or part of the order, that is the subject of the petition, pending action on the petition. [Minn. Rules 7829.3000, subp. 6]

And Commission policy guides the motion to reconsider:

> Any action of the Commission may be reconsidered. However, only a Commissioner voting on the prevailing side may move to reconsider. If the motion to reconsider passes, then the matter is before the Commission. The Commission may then alter, amend, rescind, or uphold its previous decision. The same question cannot be reconsidered a second time. (Mason, sec. 457.2.) However, the Commission may at any time, on its own motion or upon the motion of an interested party, upon notice, reopen any case after issuing an order. (Minn. Stat. sec. 216B.25.) [Minnesota Public Utilities Commission, *Operating Procedures and Policy, Meeting Procedures*, issued February 1, 1995]

All five current Commissioners supported the motion codified in the *Order* and, as such, any one of them may offer a motion to reconsider.

Note that Minn. Stat. § 216B.27, Subd. 4, states: "[a]ny application for a rehearing not granted within 60 days from the date of filing thereof, shall be deemed denied." The 60th day is September 12, 2014.

Petition for Reconsideration

CenterPoint's petition requests reconsideration on three grounds: (i) that the definition of PII was overly broad; (ii) that the *Order* would create unintended consequences; and (iii) that a rulemaking is required. Xcel, MP and OTP filed comments in support of CPE's request. The discussion below is organized by topic as presented by CPE.

A. Overly Broad Definition of PII

CPE states that the definition of PII was suggested by staff and then modified on the day of the agenda meeting. Likewise, the standards and requirements adopted were modified on the day of the agenda meeting. Further, CPE states, the Commission's definition of PII is broad and open ended compared to the Minnesota Statute's definition of "personal information" and creates

substantial and unnecessary ambiguity and uncertainty.

CPE further states that the definition adopted by the Commission was never intended to be combined with the type of privacy and security requirements adopted in the Commission's *Order*. CPE alleges that "the Order imposes on utilities privacy and security requirements that exceed any legal privacy or security requirements applicable to any U.S. business."[1]

In Answers, Xcel agrees that the record would benefit from further development. Xcel states that due to the modifications made the day of the agenda meeting, parties had very little time to consider the potential costs and other implications of the proposed PII definition and other standards and requirements. Therefore, Xcel supports further exploration of the concepts and requirements contained in the *Order*.

MP, likewise, points to the definition of "personal information" in state statute and expressed its preference for that definition.

OTP agreed, stating:

> Specifically, Otter Tail agrees that it would be useful to clarify the scope and application of the Order's definition of "Personally Identifiable Information" ("PII"). As noted by CenterPoint, the Order can be construed to require utilities to maintain the same level of privacy protection for all forms of PII, including lower-risk, publically available information such as customer name and phone numbers. This is inconsistent with the risk-based approach described in the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53. While it may be implicit that utilities should construe the definition PII through NIST's risk-based approach, there is value in clarifying this point.[2]

Staff Comment

PII issues were subject to a notice and comment period. The Commission notice soliciting comments clearly asked for comments on the possible adoption of privacy standards, risk assessment protocols, and filing requirements for utilities as those pertain to PII. The order setting out the specific topics for comment was detailed and lengthy, and if some utilities now feel the record was thin on some issues, they had ample opportunity to build and supplement the record. The modifications to the decision options were largely minor, with wording changes

[1] Page 3, CPE petition for reconsideration.
[2] OTP comments, p. 1.

such as "prohibit" instead of "forbid." While the NIST PII definition was added in the modified decision options, it was a definition known and familiar to utilities. The Commission was well within its statutory authority when it adopted its own definition.[3]

Utilities point out that the NIST PII definition and the state statute definitions are different. However, different does not equal inconsistent or contradictory. No utility has given examples of situations where the Commission *Order* and state law are in direct conflict. Should such a situation present itself, the utility is free to include that in its compliance filing and explain how it proposes to resolve the conflict.

CPE also includes the argument that because a person's name, phone number, and address are in a telephone book, it is illogical to give that information protection under its privacy order. First, staff notes that under the Commission's rules, a person can have his or her information excluded from telephone directories.[4] Second, it is not the name, address, and telephone number by itself that is protected; it is the fact that a person should not be identified as a customer of a utility. An analogy is a person receiving public assistance from the state; the fact that they are a recipient of assistance is kept confidential even if that person's information is in the phone book.[5]

As to OTP's request for clarification, Staff prefers that OTP provide the exact clarifying language it would like the Commission to adopt.

B. The Order Creates Ambiguities and Unintended Consequences

CPE states that "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."[6] For example, the *Order* requires third party contractors to have equivalent or greater protection for customer data as the utility itself provides. This requirement imposes burdens on utilities greater than those placed on other businesses.

In answers to the petition, Xcel Energy agreed that the *Order* establishes ambiguous and overly broad standards.

---

[3] Minn. Stat. §216B.09, subd. 1, states: "The commission, on its own motion or upon complaint and after reasonable notice and hearing, may ascertain and fix just and reasonable standards, classifications, rules, or practices to be observed and followed by any or all public utilities with respect to the service to be furnished."
[4] Minn. Rules 7810.2900
[5] Minn. Stat. § 13.46.
[6] CPE petition, p. 4.

Staff Comment

Staff cannot entirely comment on this part of the reconsideration petition because portions of it include conclusory statements without supporting data. For example, CPE states that the requirement for utilities' third-party contractors to have equivalent or greater protections in place imposes a burden on utilities greater than those placed on other businesses. Yet CPE does not list the other industries that are not subject to this requirement, nor does it cite to statute, rule or relevant administrative decisions allowing other industries to get out of privacy requirements by contracting functions out to a third party.

Based upon the comments of the four utilities, Staff believes the utilities are not reading Ordering Paragraph 3 as a whole. That Paragraph requires utilities to adopt and document *reasonable* processes. Staff believes that the utilities' fears, that all PII data must be treated identically and could not be given treatment appropriate to its level of risk, are premature. The terms in Ordering Paragraph 3 ("maintain only the customer PII data needed," "the purposes for which it was collected," "appropriateness and adequacy,") clearly allow for flexibility and fact-specific application, as long as utilities justify such treatment in their compliance filings.

C. A Rulemaking is Required

CPE says Commission cannot adopt statements of general applicability and future effect without complying with the Minnesota Administrative Procedure Act. The actions contemplated by the Commission's *Order* require a rulemaking proceeding, where, in the words of CPE, "all issues can be thoroughly vetted to ensure against unintended consequences or excessive costs - costs which will ultimately be borne by ratepayers."[7]

MP agreed that the Commission should undertake a rulemaking.

Staff Comment

The Commission can issue generic orders, such as its privacy decision, without engaging in a rulemaking. Courts have stated that whether to proceed by rulemaking or adjudication is a decision left to the informed discretion of the agency.[8] Courts have agreed that they are poorly situated to distinguish between circumstances appropriate for rulemaking and circumstances appropriate for case-by-case decision-making.

[7] CPE petition, p. 4.

[8] In the Matter of an Investigation into Intra-LATA Equal Access and Presubscription, Contel of Minnesota, Inc. v Minnesota Public Utilities Commission, 532 N.W. 2d 583 (finding that the MPUC did not err when it established intra-LATA equal access and presubscription requirements through a generic order rather than a rulemaking).

This matter is clearly unsuitable for a rulemaking. Staff believes the order was adjudicatory in nature (by requiring a compliance filing from each rate-regulated utility), that each utility does not collect the same information from each customer nor maintain it in the same format, and that the compliance filings and comments that follow it may be an iterative, evolving process where the application of a utility's particular circumstances (size, service area, and other facts) will affect what specific compliance filings the Commission approves. CPE's petition cites no legal authority supporting a rulemaking.

Further, the legislature has acknowledged that the Commission's unique quasi-judicial status exempts it from the requirement in the Administrative Procedure Act that agencies adopt rules on request for matters of precedent. Minn. Stat. § 14.06(b) states:

> Upon the request of any person, and as soon as feasible and to the extent practicable, each agency shall adopt rules to supersede those principles of law or policy lawfully declared by the agency as the basis for its decisions in particular cases it intends to rely on as precedents in future cases. This paragraph does not apply to the Public Utilities Commission.

Finally, the Commission has the authority to rescind, alter, or amend any order it has issued.[9] The Commission can amend its *Order* at any later date if the compliance filings indicate that modifications are necessary.

D. Additional Staff Comment

Staff believes that it is useful to provide additional background regarding NIST's definition of PII and the framework provided by NIST's *Guide to Protecting the Confidentiality of Personally Identifiable Information* (*NIST Guide*).

Broad Context

The first paragraph of the *NIST Guide* provides broad context for the discussion:

> The escalation of security breaches involving personally identifiable information (PII) has contributed to the loss of millions of records over the past few years. Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail. Organizational harms may include a loss of public trust, legal liability, or remediation costs. To appropriately protect the confidentiality of PII, organizations should use a risk-based approach; as McGeorge Bundy once stated, -

[9] Minn. Stat. § 216B.25.

> "If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds." This document provides guidelines for a risk-based approach to protecting the confidentiality of PII. [*NIST Guide*, p. ES-1; footnotes omitted]

There are two points of particular interest encompassed within this statement. First, PII confidentiality breaches can be hazardous to *both* individuals *and* organizations. As such, and not to diminish the companies' concerns about the *Order*, it is in the companies' interest to embrace and continue to explore good data management practices in today's climate of rapidly evolving technology and less-rapidly evolving law. Second, reference is made to the importance of a risk-based approach to data management (as opposed to a standards-based approach). A risk-based approach recognizes that all data are not created equal in terms of sensitivity. This point will be addressed in more detail below.

Although the main focus of the *NIST Guide* is that of the confidentiality of PII, it also recognizes that confidentiality is related to information security in general. The *NIST Guide* makes reference to foundational principles of Fair Information Practices such as those developed by the Organization for Economic Co-operation and Development (OECD) and endorsed by the U.S. Department of Commerce. These principles are:

> **Collection Limitation** - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
>
> **Data Quality** - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
>
> **Purpose Specification** - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
>
> **Use Limitation** - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.
>
> **Security Safeguards** - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

> **Openness** - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> **Individual Participation** - An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.
>
> **Accountability** - A data controller should be accountable for complying with measures which give effect to the principles stated above. [*NIST Guide*, p. 2-3 & 2-4, emphasis in original]

Definition of PII

The definition of PII adopted by the Commission is one focal point of CPE's petition for reconsideration. Staff initially recommended the definition of PII stated by NIST in its, *Security and Privacy Controls for Federal Information Systems and Organizations*:

> information 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.) [Special Publication 800-53, Revision 4, April 2013, page B-16]

This definition differs slightly from the definition in the *NIST Guide*:

> any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. [*NIST Guide*, page ES-1]

Staff believes the two definitions are fundamentally the same, and Staff offered the first definition because it was cited in the most recent of the two documents (2013 as opposed to 2010). Subsequently, the Commission modified slightly the 2013 NIST definition to read:

> ~~information~~ 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.)

The *NIST Guide* provides examples of information that may be considered PII:

- Name, such as full name, maiden name, mother's maiden name, or alias

- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number [footnote 21: Partial identifiers, such as the first few digits or the last few digits of SSNs, are also often considered PII because they are still nearly unique identifiers and are linked or linkable to a specific individual.]

- Address information, such as street address or email address

- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people

- Telephone numbers, including mobile, business, and personal numbers

- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)

- Information identifying personally owned property, such as vehicle registration number or title number and related information

- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information). [*NIST Guide*, p. 2-2]

Of critical importance, the NIST and Commission definitions of PII make reference to distinguishing identity, tracing identity, and the degree to which data sources can be linked. The *NIST Guide* states:

> To *distinguish* an individual is to identify an individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data. In contrast, a list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual.
>
> To *trace* an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status. For example, an audit log containing records of user actions could be used to trace an individual's activities.
>
> *Linked* information is information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable. [*NIST Guide*, p. 2-1, emphasis in original]

CPE argued that the NIST definition proposed by Staff and modified by the Commission was never intended by NIST to be combined with privacy and security requirements such as those set forth in the *Order*. Staff can only glean NIST's intent from its documents but it appears to Staff that NIST clearly intended its definition to be consistent with its stated goals of addressing privacy and security:

> The purpose of this document is to assist … agencies in protecting the confidentiality of personally identifiable information (PII) in information systems. The document explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy using

> the Fair Information Practices, which are the principles underlying most privacy laws and privacy best practices. PII should be protected from inappropriate access, use, and disclosure. This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII. Organizations are encouraged to tailor the recommendations to meet their specific requirements. [*NIST Guide*, page 1-1]

Staff believes the Commission's requirements, as articulated in Ordering Paragraphs 3 through 9, can be read in a manner that is not inconsistent with the *NIST Guide*. The Commission's principals either echo NIST's guidance or offer additional guidance governing the utilities' relationships with their customers.

Staff believes the risk-based definitions of PII used by NIST and the Commission attempt to take into account the modern complexities of privacy and security issues by making provision for rapid technological change and for understanding the context in which data is collected and stored. CPE has argued that the Commission's definition of PII is open-ended. *Staff agrees that the definition is open-ended, but Staff believes this open-endedness is the core feature and chief benefit of defining PII as the Commission has chosen to do*. That is to say, the Commission's definition of PII is commensurate with the nature of the privacy problem. And to say that the definition is open-ended is not to say that it is formless or intractable.

Further, recognition of the open-endedness of threats to security and confidentiality may provide protection to businesses. Meeting the minimum requirements of statute may not be sufficient to protect a firm from exposure in a world where it is increasingly easy to argue that firms should know better. Plausible deniability is receding.

Risk-Based Approach

With respect to privacy and security, neither the Commission, the utilities, nor the utilities' customers function in a business-as-usual climate. Much of our information, personal and corporate, is now digitized, and technological improvements in data storage and computing power allow that data to be filtered, sifted and combined in ways most people do not fully understand. CPE's desire for certainty is understandable but, Staff believes, that desire must be balanced with the customers' need for the type of certainty and security that is associated with privacy.

Staff believes the core of CPE's concern can be viewed as the tension reflected in the difference between standards-based and risk-based approaches to information security. Standards typically

comprise bright-line guidance for decision-making (do not drive faster than 55 miles per hour), whereas a risk-based approach allows the decision-maker to account for context (drive safely with attention to road conditions). The bright-line standard has the advantage of clarity and certainty while the risk-based guidance has the advantage of flexibility to meet changing needs. NARUC, in the context of cyber security, summarizes the distinction between compliance-based (standards-based) and risk-based approaches:

> [C]ompliance only proves *compliance*; utilities' cybersecurity should be based in *risk management*. Risk management includes assessment, mitigation and continuous improvement, whereas compliance offers a view of cybersecurity at a fixed point in time, not a dynamic picture of it. Utilities may be compliant to the CIP [Critical Infrastructure Protection] standards and still not be secure. Utilities may also be secure but not be compliant to the CIP standards. One is not the guarantee of the other. [emphasis in original][10]

The *NIST Guide*, consistent with a risk-based approach, recognizes that there are varying degrees of risk associated with various elements of PII. The *NIST Guide*, in Section 3, discusses at some length factors that can be used to determine whether the impact or harm from PII disclosure is low, moderate or high:

Identifiability: degree of ease that PII can be used to identify specific individuals

Quantity of PII: breaches of 25 records may have greater impact that breaches of 25 million records

Data Field Sensitivity: Social Security numbers may be more sensitive than phone numbers and the two together may be more sensitive than each separate field

Context of Use: the purpose for which the data is collected and stored may be important; "For example, suppose that an organization has three lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general-interest newsletter produced by the organization. The second list is people who have filed for retirement benefits, and the third list is individuals who work undercover in law enforcement. The potential impacts to the affected individuals and to the organization are significantly different for each of the three lists." [*NIST Guide*, p. 3-4]

Obligations to Protect Confidentiality: regulations may dictate sensitivity

[10] Miles Keogh and Christina Cody, *Cybersecurity for State Regulators 2.0*, National Association of Regulatory Utility Commissioners, February 2013.

Access to and Location of PII: how information is stored, shared, and transported may affect the severity of a breach

Staff believes the *NIST Guide* clearly recognizes that not all elements of PII represent equal harm if exposed and it provides direction in assessing such distinctions.

Third-Party Disclosure

CPE has raised concerns with Ordering Paragraph 5 addressing the utilities' relationships with third-party contractors. That Paragraph states:

> Each rate-regulated electric and gas utility may provide necessary customer PII data to a contractor for a regulated purpose, so long as the contractor is required to provide equivalent or greater protection for the customer data, and the utility retains responsibility to the customer in the event of the contractor's unauthorized use or release of data.

CPE argues that this clause may require parties to share data protection practices, a sharing that could create new avenues for security breaches. Staff is unclear as to CPE's concerns regarding new avenues for security breaches. Staff understands that Paragraph 5 dictates that utilities shall only enter contracts with contractors where the utility can be satisfied that the contractor has taken *reasonable* steps to treat PII in a manner consistent with the utility's understanding of the potential harm associated with a breach. Guidance here can be taken from the banking industry, an industry long acquainted with information security. In 2013, the Office of the Comptroller of the Currency (OCC) issued a bulletin addressing third-party relationships. It summarizes its guidance as follows:

- A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.
- A bank should ensure comprehensive risk management and oversight of third-party relationships involving critical activities.
- An effective risk management process throughout the life cycle of the relationship includes
  * plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
  * proper due diligence in selecting a third party.
  * written contracts that outline the rights and responsibilities of all parties.
  * ongoing monitoring of the third party's activities and performance.
  * contingency plans for terminating the relationship in an effective manner.
  * clear roles and responsibilities for overseeing and managing the relationship

> and risk management process. … [11]

Staff believes the above practices are of benefit in governing all third-party business relationships and speculates that to a significant degree the utilities routinely engage, at least implicitly, in these practices as part of their ongoing business activities.

Additional guidance may be found in a whitepaper published by Kaspersky Lab (a leading cybersecurity firm).[12] There Michael Overly discusses three tools for addressing information security in vendor relationships. They are (i) vendor due diligence questionnaires, (ii) explicit contractual protections, and (iii) exhibits or statements of work that explicitly recognize security requirements.

Staff Concerns/Questions

Staff believes that the Commission's definition of PII is appropriate for the task at hand. However, Staff suggests that the Commission's definition of PII could be modified slightly. The first line of Ordering Paragraph 2 states:

> Personally Identifiable Information (PII) shall be defined as "customer PII data which can be …

To avoid the logical circularity (essentially, PII is defined as PII) the Commission may wish to strike the second PII in the line above. Staff believes all other subsequent references to "customer PII data" need not be modified.

Staff also suggests the Commission consider modifications to Ordering Paragraph 9 which states:

> Each rate-regulated electric and gas utility shall 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. Notice shall include the number of customers affected, date or period of breach, types of data inappropriately accessed, whether the source or cause of the breach has been identified and provided to law enforcement, steps taken to prevent similar breaches, and steps to redress the breach.

---

[11] Office of the Comptroller of the Currency, U.S. Department of the Treasury, OCC Bulletin 2013-29, October 13, 2013, http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

[12] Michael R. Overly, *Information Security and Legal Compliance: Finding Common Ground*, Kaspersky Lab, http://go.kaspersky.com/rs/kaspersky1/images/Information%20Security%20and%20Legal%20Compliance%202014.pdf?mkt_tok=3RkMMJWWfF9wsRonuK7MdO%2FhmjTEU5z16e4tUKK%2Bgokz2EFye%2BLIHETpodcMS8VlN6%2BTFAwTG5toziV8R7jFLs1p0NsQWRXi

Staff has three observations. First, it may be useful to clarify that "promptly notify" could explicitly account for the needs of law enforcement if delayed notification will aid a criminal investigation.

Second, the Commission may wish to reconsider whether *all* unauthorized use requires customer notification (Xcel and CPE expressed concerns with this issue). Here, Staff contemplates situations where a utility allows specific PII to be accessed by one internal department (say, billing) but not by another internal department (say, energy use forecasting). Staff's focus here is the notification requirement, not the access limitation principle expressed in Ordering Paragraph 3E. There may be a point at which customer notification may be too burdensome for the utility and where customers become insensitive to breaches and, perhaps, less able to distinguish the relatively harmless from the relatively harmful. It may be more consistent with the overall risk-based approach to recognize that the potential impact of a breach should be taken into account in determining whether customers should be notified.

Third, Staff suggests that customer notification may be unnecessary and/or unduly burdensome when a data breach involves only sufficiently encrypted data. Minn. Stat. § 325E.61, subd. 1, recognizes that breaches involving encrypted personal information are not subject to customer notification requirements. The European Union also relieves providers of electronic communications of the necessity to report security breaches of personal information to customers:

> [N]otification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent national authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.[13]

As a focal point for discussion of issues above Staff offers a modified version of Ordering Paragraph 9:

> Each rate-regulated electric and gas utility shall 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. Notice shall include the number of customers affected, date or period of breach, types of data inappropriately accessed, whether the source or cause of the breach has been identified and provided to law enforcement, steps taken to prevent similar breaches, and steps to redress the breach. <u>The notification required by this</u>

[13] European Union, Commission Regulation (EU) No 611/2013, Article 4, June 24 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:EN:PDF

> paragraph may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation. Where unauthorized use or release of customer PII data does not extend beyond the regulated portion of the enterprise the utility is not required to notify affected customers. Notification of a customer PII data breach to the customers concerned shall not be required if the utility has implemented appropriate technological protection measures (such as encryption), and that those measures were applied to the data exposed by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorized to access it.

Staff believes that the above language can be read as not inconsistent with Minn. Stat. § 325E.61, Subd. 1(a), which states:

> Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement …

Parties to this docket have not had an opportunity to comment on the language above.

Final Note

The Commission's *Order* requires the utilities to adopt *reasonable* processes to protect PII. It does not state that the processes must be *perfect*. The Kaspersky Lab whitepaper comments upon reasonableness:

> The concept of acting 'reasonably' is used in many state and federal laws in the United States, Australia, and many other countries. The related concept of acting so as to take 'appropriate' or 'necessary' measures is used in the European Union and many other areas. Together, they form the heart of almost every information security and data privacy law. A business must act reasonably or do what is necessary or appropriate to protect its data. Note that this does not require perfection. Rather, the business must take into account the risk presented and do what is reasonable or necessary to mitigate that risk. If a breach, nonetheless,

occurs, provided the business has established this basic requirement, it will not be generally found in violation of the applicable law or regulation.[14]

E. Commission Options

Issue 1: Should the Commission Reconsider or Reopen its *June 24th Order*?

1.a Grant CPE's petition for reconsideration.

1.b Deny CPE's petition for reconsideration.

1.c Take other action.

Staff recommends option 1.a if (i) the Commission wishes to defer deliberations to a future date or (ii) if the Commission wishes to consider the concerns raised by Staff.

Issue 2: Should the *June 24th Order* be Modified?

Note: If the Commission denies the petition (option 1.b) it need not take any action regarding Issue 2.

2.a Modify the Commission's *June 24th Order*:
(i) Delete Ordering Paragraph 2; and/or
(ii) Vacate the *Order* and initiate a rulemaking. (Staff note: Decision Options 2i and 2ii are Staff's interpretation of CPE's request.)

2.b Modify the first line of Ordering Paragraph 2 and Ordering Paragraph 9 to address the concerns raised by Staff.

2.c Defer deliberations regarding the *Order* to a future date (that is, toll the time period).

2.d Take other action.

Staff recommends option 2.b.

[14] See footnote 12.