STATE OF MINNESOTA
BEFORE THE PUBLIC UTILITIES COMMISSION

Beverly Jones Heydinger	Chair
David C. Boyd	Commissioner
Phyllis Reha	Commissioner
J. Dennis O'Brien	Commissioner
Betsy Wergin	Commissioner

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

Comments of Roger Colton on Behalf of Legal Services Advocacy Project

The Minnesota Public Utilities Commission (the Commission) has requested comments on whether it should take actions regarding customer data privacy practices by Minnesota's public utilities. The Commission's Order requested comments on, inter alia, the preparation and filing of Privacy Impact Statements (PIAs), the preparation and filing of Information Security Plans (ISPs), and the continuing collection and use of customer Social Security Numbers (SSNs).

On behalf of the Legal Services Advocacy Project (LSAP), I respectfully submit these comments in the above-referenced docket. I am a principal in the firm Fisher, Sheehan & Colton, Public Finance and General Economics, of Belmont, Massachusetts. I specialize in law and economic consulting, energy regulation, and consumer economics. Over the course of more than 25 years, I have provided expert testimony, comments, and analysis for public utilities, regulators, nonprofit organizations, and state and local government agencies, in countless utility regulatory proceedings in numerous states and provinces around the United States and Canada.

The Legal Services Advocacy Project is a statewide division of Mid-Minnesota Legal Aid, representing the interests of low-income Minnesotans through legislative and administrative advocacy, research, and community education activities.

My comments on behalf of LSAP are set forth in Attachment A below. Based on the data and analysis presented in Attachment A to these comments, which by this reference thereto is incorporated herein as if fully set forth, on behalf of LSAP, I urge the Commission to adopt certain recommendations regarding the privacy policies of rate-regulated energy utilities, as set forth in Attachment A.

August 30, 2013

Respectfully submitted,

ON BEHALF OF:
LEGAL SERVICES ADVOCATE PROJECT
(LSAP)

Roger D. Colton
Fisher, Sheehan and Colton
Public Finance and General Economics
34 Warwick Road
Belmont, MA 2478
617-484-0597

STATE OF MINNESOTA
BEFORE THE PUBLIC UTILITIES COMMISSION

Beverly Jones Heydinger	Chair
David C. Boyd	Commissioner
Nancy Lange	Commissioner
J. Dennis O'Brien	Commissioner
Betsy Wergin	Commissioner

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

Actions to Protect the Privacy of Minnesota Gas and Electric Customers: Comments Presented on Behalf of The Legal Services Advocacy Project (LSAP)

Prepared by:
Roger D. Colton, JD, MA (economics)
Fisher, Sheehan & Colton
Public Finance and General Economics
Belmont, MA 02478

August 30, 2013

Table of Contents

On behalf of the Legal Services Advocacy Project (LSAP), I respectfully submit these comments in the above-referenced docket. I am a principal in the firm Fisher, Sheehan & Colton, Public Finance and General Economics, of Belmont, Massachusetts. I specialize in law and economics consulting, energy regulation, and consumer economics. Over the course of more than 25 years, I have provided expert testimony, comments, and analysis for public utilities, regulators, nonprofit organizations, and state and local government agencies, in countless utility regulatory proceedings in numerous states and provinces around the United States and Canada.

LSAP is a statewide division of Mid-Minnesota Legal Aid, representing the interests of low-income Minnesotans through legislative and administrative advocacy, research, and community education activities.

The comments below respond to the July 2013 Minnesota Public Utilities Commission ("the Commission" or "PUC") Order in this Docket[1] and are divided into the following Parts:

- Whether Minnesota utilities should prepare and file Privacy Impact Statements (PIAs) and Information Security Plans (ISPs);
- Whether Minnesota utilities should be directed to use alternatives to Social Security Numbers;
- Whether Minnesota should use Fair Information Practices (FIPs) as the touchstone of privacy policy for Minnesota's gas and electric utilities; and
- Whether Minnesota utilities should be barred from the sale, rental or other dissemination and/or distribution of Personally Identifiable Information (other than Customer Energy Usage Data, [CEUD]).

I. THE PREPARATION AND FILING OF PIAS AND ISPS.

LSAP believes that it is reasonable, and urges the Commission, to require Minnesota's natural gas and electric utilities to:

1. Adopt a reasonable PIA, or set of PIAs as appropriate, consistent with the Federal PIA requirements of the E-Government Act of 2002 and resulting regulations [and guidelines], and to file it [them] with the Commission;[2] and

[1] Since that July Order referred back to the June 17, 2013 Order, the two Orders are not distinguished in these comments. References to the "July Order" are intended to incorporate the provisions of the June Order referenced therein.

2. Adopt a reasonable risk-based ISP, or set of ISPs as appropriate, consistent with the Federal ISP requirements of the Federal Information Security Management Act of 2002 (FISMA) and resulting regulations and guidelines, and to file it [them] with the Commission.

A. The Need for Privacy Protection

LSAP will not repeat its discussion of concerns about privacy protection and identity theft presented in its January 2013 comments in this docket.[3] LSAP does, however, supplement those concerns with the following observations about the need for adopting the PIA and ISP requirements articulated above.

Erosion of "reasonable expectations": Protecting the privacy of one's personally identifiable information is a long-term need in addition to being an appropriate response to the short-term need to prevent identity theft. The longer term problem is that the more frequently an intrusion on privacy occurs, the greater an intrusion on privacy is considered to be "reasonable." According to the U.S. Supreme Court,[4] the Fourth Amendment protects only a "reasonable expectation"[5] of privacy. The more common an activity becomes, therefore, the less likely that the courts will hold that a release of data as a result of that activity will constitute an invasion of privacy.[6] Once technology diminishes an expectation of privacy, that expectation no longer exists to be protected.[7]

In applying this principle, the U.S. Supreme Court has now held, for example, that there is no expectation of privacy applicable to copies of personal checks once that data is entered into a computer.[8] This observation directly applies to the concerns that LSAP has previously expressed

---

[2] Not all E-Government Act administrative implementation has been through "regulations." LSAP urges the Commission also to include the term "guidelines" as it does with respect to the Information Security Plan (ISP) provisions of the Federal Information Security Management Act (FISMA) proposal.

[3] By this reference thereto, LSAP incorporates those comments herein as if fully set forth. See also, Swendiman (February 21, 2008). Congressional Research Service Report to Congress, "The Social Security Number: Legal Developments Affecting its Collection, Disclosure and Confidentiality," at CRS-3 ("In recent years, federal agencies have increasingly recognized that SSNs are a key to the perpetuation of identity theft and related fraud.") (hereafter, CRS Report).

[4] Florida v. Riley, 488 U.S. 445, 449 – 452 (1984); Oliver v. U.S., 466 U.S. 170, 177 – 182 (1984).

[5] "Courts define privacy by reference to society's prevailing understanding of what is a reasonable expectation of privacy. Because this conception of privacy tracks societal expectations, what is protected as private will vary in accordance with relevant social changes." Spencer, "Reasonable Expectations and the Erosion of Privacy," 39 San Diego L.Rev. 843, 846 (2002).

[6] Schwartz, "Data Processing and Government Administration: The Failure of the American Legal Response to the Computer," 43 Hastings L.J. 1321, 1345 (1992).

[7] Id., at 1345 - 46.

[8] Id., at 1346.

in this proceeding.[9] The more often personal information is collected and stored in a computer by Minnesota utilities, the less protection is afforded to Minnesota consumers against the loss of other distribution of that information. The pervasive use of SSNs, for example, is argued to "diminish[…] the property right in one's identity that every person has. . ."[10] Accordingly, the personal information that ***has*** been collected by Minnesota utilities should be made subject to a full range of protections through the preparation and filing of PIAs and ISPs.

Protecting and enhancing e-commerce: Quite aside from the personal reasons to protect private information, a "business" reason also exists for the Commission to ensure the appropriate privacy protection of personally-identifiable information through the preparation of PIAs and ISPs. The use of e-services depends on the public's confidence in the protection of the underlying data.[11] In 2002, the federal Information Security and Privacy Advisory Board (ISPAB), a federal advisory committee originally established by the Computer Security Act of 1987, issued a report on government privacy policy-setting and management.

> In its report, the ISPAB raised a number of concerns about advances in technology and its impact on privacy. Specifically, ISPAB observed that "with the migration toward e-government services, greater demands will be placed on the government's privacy policies and systems." ISPAB further observed that the public's willingness to use such services will depend "in large measure on their confidence that the information that they disclose will be safeguarded."
>
> The ISPAB report further stated that, "changes in technology, the privacy management challenges stemming from expanded e-government services, the accelerated interaction of networked information systems within and across critical infrastructure boundaries, and the extended, routine exchange of data among Federal and non-Federal government and non-government systems - all mandate immediate and serious attention to [the] Federal government's data privacy policies and operational controls."[12]

[9] CRS Report, supra, at CRS-9 ("Challenges to SSN collection based on constitutional grounds have not fared well in the courts. Under the current framework for evaluating constitutional privacy rights, which is essentially a 'reasonable expectation of privacy' analysis, courts have been hard-pressed to find a constitutionally protected interested in the SSN because of the broad dissemination of SSNs in public and private records.")

[10] Komouves, "We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers of Personal Identifiers," 16 J. Marshall J. Computer & Info. L. 529, 571 (1998).

[11] Federal Trade Commission (June 21, 2007). Prepared Statement of Federal Trade Commission Before the Subcommittee on Social Security of the House Ways and Means Committee, Protecting the Privacy of Social Security Numbers from Identity Theft, at 2 ("Beyond its direct costs, concerns about identity theft harm our economy by threatening consumers' confidence in the marketplace generally, and in electronic commerce specifically. A Wall Street Journal/Harris Interactive survey, for example, found that, as a result of fears about protecting their identities, 30 percent of consumers polled were limiting their online purchases, and 24 percent were cutting back on their online banking.")

[12] General Accounting Office (May 2008). Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, GAO-08-536, citing Computer System Security and Privacy Advisory Board (which is

The Commission could easily substitute the "Minnesota utility industry" into these ISPAB observations in lieu of references to the federal government and reach identical conclusions about personal information generally and Social Security Numbers (SSNs) in particular.[13] The PUC could (and should) conclude, in a fashion identical to ISPAB, that "expanded e-services, the accelerated interaction of networked information systems within and across critical jurisdictional boundaries, and the extended, routine exchange of data among utility and non-utility systems all mandate immediate and serious attention to utility data privacy policies and operational controls." Further, the PUC could (and should) conclude, in a fashion identical to ISPAB, that "with the migration toward e-commerce services, greater demands will be placed on the utility industry's privacy policies and systems," and that "the public's willingness to use such services will depend in large measure on their confidence that the information that they disclose will be safeguarded."

B. Minnesota Utilities should be Subject to Privacy Protection Requirements, just like other Industries.

While much of LSAP's discussion in these (and prior) comments analogizes recommended privacy controls for the utility industry with the privacy protections required in a governmental setting, privacy controls are obviously not limited to the government (federal or otherwise). Indeed, it is not uncommon, or unreasonable, to place restrictions on the collection and dissemination of personal information by private industry. The Gramm-Leach-Bliley Act, for example, restricts the ability of financial institutions to share their customers' non-public personal information with non-affiliated third parties. The Gramm-Leach-Bliley Act requires financial institutions to provide consumers with an opportunity to "opt-out"[14] of allowing their financial institution to provide such personal information to third-parties.[15] In addition:

---

what ISPAB was named until December 2002), Findings and Recommendations on Government Privacy Policy Setting and Management (September 2002).

[13] CRS Report, at CRS-13 ("Concerns have been expressed regarding the effect of technological advances on the availability and use of the SSN in private sector databases. Organizations that sell personal information, including SSNs, have benefitted greatly from continuing advances in computer technology and the availability of computerized databases.")

[14] According to the FTC: A financial institution must "provide an opt-out notice, with the initial notice or separately, prior to a financial institution sharing nonpublic personal information with nonaffiliated third parties.

- Provide consumers with a "reasonable opportunity" to opt out before disclosing nonpublic personal information about them to nonaffiliated third parties, such as 30 days from the date the notice is mailed.
- If a consumer elects to opt out of all or certain disclosures, a financial institution must honor that opt-out direction as soon as is reasonably practicable after the opt-out is received."

[15] Federal Trade Commission, Bureau of Consumer Protection, Division of Financial Practices, "The Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information," http://www.ftc.gov/privacy/glbact/glboutline.htm (last accessed August 20, 2013).

1. The Video Privacy Protection Act[16] bans any "video tape service provider" from knowingly providing "identifiable information" about a customer to anyone.[17]

2. The Cable Communications Policy Act[18] requires cable companies to give notice of what information they are collecting and how it is being used.[19] This statute also prohibits cable companies from collecting personally identifiable information using the cable system and/or disclosing such information without the prior consent of the customer.[20]

3. The Telecommunications Act protects consumers against the disclosure of individually identifiable subscriber data by a telecommunications carrier without prior approval.[21]

Aside from these specific statutes, the Sarbanes-Oxley Act, though primarily known as reforming corporate governance, requires public companies --which all Minnesota regulated gas and electric utilities subject to this Commission inquiry are-- to maintain adequate "internal controls" on information.[22] This language has been construed to cover the protection of private information by such companies.[23]

The point of this discussion is that it is difficult to conceive of how (or why) one's video rentals, cable watching data, and telephone usage data would be considered to be so private as to merit specific privacy protections, including a ban on disclosure without specific express prior consent (periodically renewed), but that, in applying a "just and reasonable" statutory standard to Minnesota's gas and electric utilities, the personally identifiable information collected by electricity and natural gas utilities could be maintained without adequate internal privacy protections such as are provided through PIAs and ISPs.

C. Ample Substantive Guidance Exists for the Preparation of PIAs and ISPs.

LSAP endorses not simply the general proposal to require the preparation, filing and review of PIAs (para. 3(a)(i)) and ISPs (para. 3(a)(ii)) by Minnesota's public utilities, but also the specific proposals contained in paragraph 3(a)(iii) of the Commission's July 2013 order. In particular, LSAP urges that PIAs and ISPs address, not by way of limitation, each of the following:

[16] 18 USC §2710.
[17] Id., at §2710(b)(1).
[18] 47 U.S.C. §551.
[19] Id., at §551(a)(1).
[20] Id., at §551(b) – (c).
[21] 47 U.S.C. §222(c)(1).
[22] 15 U.S.C. §7262.
[23] Wolf, Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age, §2.8, at 2-82 (1st ed. 2007).

1. Notice to the customer of the data collected and the reasons for it; whether the customer must provide the data as a condition of service;
2. Limitations to assure that only the data that is relevant and necessary is collected;
3. The type and frequency of notice provided to the customer about the utility's privacy policy;
4. The utility's allowable uses of the data, with and without customer consent;
5. Customer access to one's own data;
6. Procedure for the customer to withdraw consent;[24]
7. Procedures for the customer to correct inaccuracies or incomplete information;
8. Limitations on use by the utility;
9. How the data will be retained and secured;
10. How long the data will be retained and the steps taken to purge it;
11. Delineation of authorized and unauthorized use;
12. Protections and limitations in place to prevent unauthorized use, access, destruction, loss, modification, etc.;
13. Procedures in place for documenting authorized use;
14. Notice to the customer of breach;
15. Redress and penalties for unauthorized (intentional or unintentional) disclosure; and
16. Process, including frequency, of review and audits to assure that privacy protections are in place, are followed, and provide adequate protection for the customer with the utility and its contractors.[25]

LSAP points out that there are ample substantive guidelines for implementing the protections articulated by the Commission's paragraphs cited above. The discussion below is intended not to provide a comprehensive discussion of these guidelines, but simply to provide sufficient insights for the Commission (and the state's utilities) to conclude that the scope of requirements set forth by the Commission is not overly burdensome, and certainly not over-reaching.

Before looking at the specifics of OMB and NIST privacy policies and guidelines, however, the PUC should note that OMB reports "it is important to emphasize that a few simple and cost-effective steps may well deliver the greatest benefit, such as: reducing the volume of collected and retained information to the minimum necessary."[26] This same conclusion is also the clear

[24] There should not only be procedures for withdrawing consent, there should also be procedures for periodically renewing consent. In other words, consent, once given, is not to be considered consent in perpetuity.
[25] LSAP urges that there should not only be protections for the "utility and its contractors," but also that "contractors" should be explicitly defined to include downstream out-sourcing (i.e., sub-contractors). Privacy protections should not disappear simply because the "contractor" is one too many steps removed from the utility in privity.
[26] OMB 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.

and consistent message from others who have considered the issue of privacy.[27] The best way to protect the privacy of an individual's information, including Social Security Numbers, is to avoid collecting it in the first instance.[28]

(1) The Federal Office of Management and Budget (OMB) Privacy Guidelines.

According to OMB, federal agencies working to implement the PIA/ISP requirements of federal law should be implementing "four particularly important security requirements":[29]

- Assign an impact level to all information and information systems (high, medium, low);[30]
- Implement minimum security requirements and controls;[31]
- Certify and accredit information systems supporting the operation and assets of the agency, including those provided or managed by another agency, contractor or other source;[32]
- Train employees (including managers) and provide at least annual refresher training.

OMB states that "agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely and complete and reduce them to the minimum necessary for the proper performance of a documented agency function."[33]

---

[27] Presidential Task Force on Identity Theft (2007). Combating Identity Theft: A Strategic Plan, at 24 ("More must be done to eliminate unnecessary uses of SSNs"); GAO (June 2006). Privacy: Preventing and Responding to Improper Disclosures of Personal Information, GAO-06-833T, at 11 ("Limiting the collection of personal information, among other things, serves to limit the opportunity for that information to be compromised. For example, key identifying information –such as Social Security Numbers—may not be needed for many agency applications that have data bases of other personal information.")

[28] "**Minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.** The likelihood of harm caused by a breach involving PII is greatly reduced if an organization minimizes the amount of PII it uses, collects and stores. For example, an organization should only request PII in a new form if the PII is absolutely necessary. Also, an organization should regularly review its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission." NIST Information Technology Laboratory, "Guide to Protecting Personally Identifiable Information," ITL Bulletin (April 2010), citing NIST (April 2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), at Section 4.2.3, NIST (Special Publication) (SP) 800-122.

[29] OMB M-07-16.

[30] Id., citing, Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, National Institute of Standards and Technology.

[31] Id.

[32] Id. This standard supports the PUC's proposal (para. 3(d)) that contractors should be required to register and demonstrate compliance with specified privacy protections.

[33] Id., at A-16.

OMB has provided substantial guidance on how and when to prepare (and/or modify) a PIA. In September 2003, for example, OMB issued guidelines for heads of federal Executive departments and agencies, within the context of the E-Government Act of 2002: (1) specifying when to conduct a PIA;[34] and (2) setting forth the content of a PIA.[35]

Senior management official designation: One element of a PIA that has been recognized by OMB, but that was not explicitly included in the PUC's July 2013 Order in this Docket, which should be, is to "designate an appropriate senior official or officials" for privacy policies.[36] The General Accounting Office, too, has devoted considerable attention to the question of why, and how, a specific senior official should be designated, and then held accountable, for privacy policies.[37] In addition, OMB subsequently specifically addressed the need to designate a particular "senior official" as responsible for, and accountable for, privacy policy.[38] According to OMB:

> The senior agency official shall have a central role in overseeing, coordinating, and facilitating the agency's compliance efforts. This role shall include reviewing the agency's information privacy procedures to ensure that they are comprehensive and up-to-date and, where additional or revised procedures may be called for, working with the relevant agency offices in the consideration, adoption, and implementation of such procedures. . .
>
> In addition to this compliance role, the senior agency official must also have a central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues, including those relating to the agency's collection, use, sharing, and disclosure of personal information. In evaluating these proposals, agencies must consider their potential impact on information privacy and take this impact into account in evaluating alternatives and making decisions. . .[39]

[34] OMB M-03-22, OMB Guidelines for Implementing the Privacy Provisions of the E-Government Act of 2002, at Attachment A, Sec. II.E (September 26, 2003); see also, OMB M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006).
[35] Id., at Section II.F.
[36] Id., at Sec. V.3.
[37] See generally, GAO (May 2008). Privacy: Agencies Should Ensure that Designated Senior Officials have Oversight of Key Functions, GAO-08-603; see also, GAO (May 1998). Executive Guide: Information Security Management: Lessons from Leading Organizations, GAO/AIMD-98-68.
[38] OMB M-05-08. Designation of Senior Agency Officials for Privacy (February 11, 2005).
[39] OMB M-05-08.

A similar obligation should be placed on Minnesota utilities, to designate a senior management official to be responsible for, and accountable for, the promulgation and implementation of privacy protections.

Periodic training: A second element of a PIA/ISP that was not –but should be-- specifically recognized in the Commission's list is the need to periodically train staff and/or personnel "to assure that staff members understand their information security responsibilities and the organization's policies."[40] A standard process through which to build a reasonable training program has been promulgated by the National Institute of Standards and Technology (NIST).[41] LSAP cites the existence of this NIST guidance not to recommend its use as a mandatory process or standard, but rather merely to indicate that Minnesota utilities have significant resources from which to draw to implement such information security training programs. The PUC should explicitly recognize the need for adequate periodic training as part of the PIA/ISP process(es).

(2) The Federal National Institute of Standards and Technology (NIST) Guidelines.

NIST recommends the use of a Risk Management Framework (RMF) for building security controls for information systems.[42] According to the NIST Information Technology Laboratory, the RMF:

> describes a disciplined and structured process that integrates information security and risk management activities into a system development life cycle. The RMF guides agencies through a series of steps, taking into account the risks such as the magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.[43]

While the PUC need not explicitly define the exact content and process of an ISP filed by the state's natural gas and electric utilities, it *is* reasonable for the PUC to indicate that it expects to see evidence of a consideration of each of the six RMF steps:

[40] NIST Information Technology Laboratory, "How to Identify Personnel with Significant Responsibility for Information Security," ITL Bulletin (June 2010); NIST Information Technology Laboratory, "Information Technology, Security Awareness, Training, Education, and Certification," ITL Bulletin (October 2003).
[41] NIST (October 2003). Building an Information Technology Security Awareness and Training Program, NIST SP 800-50.
[42] NIST (June 2010). Guide to Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, NIST SP 800-53A (Rev. 1); NIST (September 2012). Risk Management Guide for Information Technology Systems, NIST SP 800-30; NIST (August 2008). Guide for Mapping Types of Information and Information Systems to Security Categories, NIST SP 800-60 (Rev. 1) (2 volumes: Volume 1: Guide; Volume 2: Appendices).
[43] NIST Information Technology Laboratory, "Assessing the Effectiveness of Security Controls in Federal Information Systems," ITL Bulletin (August 2010).

- **Step 1**. Categorize the information system and the information processed, stored, and transmitted by that system based on an impact analysis.

- **Step 2**. Select an initial set of baseline security controls for the information system based on the security categorization, tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

- **Step 3.** Implement the security controls and describe how the controls are employed within the information system and its environment of operation.

- **Step 4.** Assess the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

- **Step 5.** Authorize information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

- **Step 6.** Monitor the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.[44]

Specific NIST guidelines cover each step of the RMF process.[45] NIST emphasizes that information security and risk management must be considered through the life-cycle of an information system.[46]

D. PIA/ISP Summary and Conclusions

A recent report for the White House noted that:

[44] Id. See generally, NIST (February 2004). Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards (FIPS) Pub. 199; NIST (March 2006). Minimum Security Requirements for Federal Information and Information Systems, FIPS Pub. 200.
[45] See e.g., Step 2: NIST (August 2009). Recommended Security Controls for Federal Information Systems and Organizations, NIST SP 800-53 (Rev. 3); Step 4 and Step 6: NIST SP 800-53A, supra.
[46] NIST (February 2010). Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST SP 800-37 (Rev. 1); NIST (October 2008). Security Considerations in the System Development Life Cycle, NIST SP 800-64 (Rev. 2).

> the Internal Revenue Service and [Department of Homeland Security] pioneered the use of privacy impact assessments (PIAs), which provide for structured assessments of the potential privacy issues arising from new information systems and, under the E-Government Act of 2002, are now required of Federal agencies under some circumstances . . . Since their development within the Federal Government, PIAs have become widely used in the private sector and within the European Union.[47]

Nothing about the proposed PIA/ISP requirement advanced by the PUC is revolutionary. Minnesota utilities should have no more difficulty in complying with these basic planning processes than other entities within the private sector. The PUC's proposal to require gas and electric utilities to prepare and file PIAs and ISPs to protect Minnesota consumers is appropriate and should be adopted.

II. THE NEED TO STOP THE COLLECTION AND RETENTION OF SOCIAL SECURITY NUMBERS (SSNS).

LSAP urges the Commission to conclude, pursuant to its July 2013 Order in this proceeding (para. 3(f)), that Minnesota utilities should move expeditiously to refrain from collecting, storing and using Social Security Numbers as customer identifiers.

Peter Swire is a law professor at Ohio State University. He was the Chief Counselor for Privacy in the Office of Management and Budget for President Bill Clinton's Administration, and is the only person, to date, to have government-wide responsibility for privacy policy. Swire knows what he is talking about. "Social Security Numbers," Swire says, "are an aging technology, and we have to do serious planning for what will come next."[48]

Swire's comment was responding to a study published in the proceedings of the National Academy of Science by researchers at Carnegie Mellon University. That study was able to identify, through a computer statistical analysis, the first five digits of a person's SSN for 44% of persons borne after 1988, and for 7% of those born from 1973 to 1988.[49] The accuracy of the prediction system increased for smaller states and for people born after 1988. While the researchers were able to predict all nine digits of an SSN for 8.5% of those born after 1988 in

[47] The White House (February 2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, at 44.
[48] New York Times, "Weakness in Social Security Numbers is Found," July 6, 2009.
[49] LSAP discussed in its initial filing in this docket how knowing the first five digits of an SSN leads to the discovery of the entire SSN. Due to different truncation protocols, while some entities truncate the first four digits of an SSN, other entities truncate the last four digits, thus allowing partial SSNs to be easily matched.

fewer than 1,000 attempts (testing the data on a half million persons), they needed 10 or fewer tries to predict all nine digits for 1 out of 20 Social Security numbers assigned in Delaware.[50]

William Winkler, an analyst at the U.S. Census Bureau, reports that "Acquisti and Gross demonstrate that it is possible to predict SSNs for a moderately large proportion of the population. This is particularly true for individuals who received SSNs via the Enumeration at Birth (EAB) procedure that began in 1993."[51] Winkler concluded that one of the two major questions posed by the Carnegie Mellon research is: "[W]ill the credit-granting industry and other groups that need to verify identities adopt procedures that somehow significantly reduce the possibility of identity theft for individuals? Because millions of individuals are affected by identity theft annually, the ease with which identity verifying procedures are compromised needs to be reduced."[52]

"Unless mitigating strategies are implemented," the Acquisti and Gross study itself found, "the predictability of SSNs exposes them to risks of identity theft on mass scales."[53] Acquisti and Gross concluded that "[i]ndustry and policy makers may need, instead, to finally reassess our perilous reliance on SSNs for authentication, and on consumers' impossible duty to protect them."[54]

This data shows that the privacy concerns which LSAP has raised about the continuing collection and use of SSNs are not theoretical. The grounds for LSAP's concerns are neither ambiguous nor insignificant. The actions considered by the PUC in this proceeding to reduce, and ultimately eliminate, the State's utility industry's reliance on Social Security Numbers are absolutely essential to the protection of Minnesota's utility consumers in both the short- and long-term.

A. The Need for SSN Collection to Prevent "Fraud" is Over-Stated.

The federal government's policy on SSNs is unambiguous. The federal Office of Management and Budget includes the following in its 2007 policy on implementing privacy protections:

> Reduce the Use of Social Security Numbers.
>
> a. **Eliminate Unnecessary Use**: Agencies must now also review their use of Social Security Numbers in agency systems and programs to identify

[50] Acquisti and Gross (2009). "Predicting Social Security Numbers from Public Data," Proc. Natl Acad. Sci. USA 106:10975-10980.
[51] Winkler (July 2009). "Should Social Security numbers be replaced by modern, more secure identifiers?" Proc. Natl Acad. Sci. USA 106:10877-10878.
[52] Id.
[53] Predicting Social Security Numbers, supra.
[54] Id.

instances in which collection or use of the Social Security Number is superfluous. Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of Social Security Numbers within eighteen months.

b. <u>Explore Alternatives</u>: Agencies must participate in governmentwide efforts to explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.).[55]

It would not be correct to conclude based on this policy that the federal government is any less concerned about fraud prevention than are Minnesota's gas and electric utilities. It would be more correct to realize that the likelihood, magnitude and scope of the harms generated by the unneeded collection, and/or inappropriate disclosure or dissemination, of SSNs is simply not justified by the "fraud-reduction" benefits claimed to be generated by the use of those SSNs. The computer matching which Minnesota's utilities cite as a reason to justify continue collecting SSNs –the rationale being that the matching helps to prevent "fraud"—has been found to be based more on habit and practice than on demonstrated results. Consider one study of the impact of similar "fraud prevention" on the provision of public assistance:

> Data matching has been defined as electronic comparison of two or more sets of personal records. Despite the popularity of this technique, its efficiency is uncertain. In a detailed analysis of matching programs, the Office of Technology Assessment noted that there is no evidence that computer matching is always cost effective. It also concluded that the efficacy of computer matching in detecting fraud is overrated, and that client fraud comprises only a small percentage of the total waste in federal programs. . .
>
> * * *
>
> . . .A study of AFDC, sponsored in part by the Southern Governors' Association and the Southern Legislative Conference, shows that less than a quarter of all denials of assistance can be attributed to excess personal income. The majority of such denials are due, rather, to "Failure to Comply with Procedural Requirements." Thus, the technical complexities of AFDC appear to be more successful at keeping deserving applicants from obtaining welfare than at identifying the undeserving. The bureaucratic structure of the data processing

[55] OMB, M-07-16, at 7.

> system through which social services are currently delivered forms a bar to helping the needy.[56]

Other work has reached similar conclusions, thus giving rise to legitimate questions about whether the mere assertion that the collection of SSNs to protect against "fraud" is, without substantiation, a reason to allow the collection of such personal information by Minnesota's utilities. For years now, the federal government has examined the propriety of matching information from one data source with information from a separate data source and the creation of new information arising from such matching.[57] The costs of engaging in such matching are higher, and the benefits derived from such matching are lower, than is generally assumed in the generalized assertions of fraud-prevention as a rationale for the collection and matching of personal information.[58]

B. Social Security Numbers are Not Good "Authenticators" to Prevent Fraud.

The reason that Minnesota utilities argue that using SSNs is necessary is because those utilities have historically used SSNs as an individual "authenticator." An authenticator is used by the utility as the means by which an individual proves that he or she really is who he or she claims to be.

It has frequently been found, however, that Social Security Numbers are not good "authenticators." It is not merely consumer advocates that have expressed concern. As early as 1995, the newsletter of the Association for Computing Machinery (ACM), reported on the "risks of Social Security Numbers":

> The problem with social security numbers is that some organizations are using these ubiquitous numbers for identification, others are using them for authentication, and still others are using them for both. I call up my bank, tell them my account number and ask them for a balance. Just to make sure that I am really who I claim to be, my bank asks for my SSN—as if this is a number that is some kind of secret that we share.

---

[56] Data Processing and Government Administration, supra, at 1359 – 1360 (internal citations omitted).
[57] See generally, General Accounting Office (GAO) (1986). Computer Matching: Assessing its Costs and Benefits, PEMD-87-2, at 72-79 (survey of seventeen federal agencies shows consideration or assessments of costs and benefits for these matches varied considerably in nature and timing); see also, GAO (1987). Computer Matching: Assessing its Costs and Benefits, GAO/T-FEMP-87-5; GAO (1986). Eligibility Verification and Privacy in Federal Benefit Programs: A Delicate Balance, GAO/HRD-85-22.
[58] Gilman. "The Class Differential in Privacy Law," 77 Brook. L.Rev. 1389, 1407 (2012), citing, Morgan. "Public Assistance for the Price of Privacy: Leaving the Door Open on Welfare Home Searches," 40 McGeorge L.Rev. 227, 251 (2009); see also, Mulzer, "The Doorkeeper and the Grand Inquisitor: The Central Role of Verification Procedures in Means-Tested Welfare Programs," 36 Colum. Hum. Rights L.Rev. 663, 664 – 65 (2005).

> But my SSN isn't secret—and there is no way to make it that way in today's increasingly cross-indexed society. That's because for every organization that thinks your SSN should be kept secret, there's another that is using it as some kind of account number, leaving it open for all of the world to see.[59]

There are three ways for a person to authenticate who they are: (1) by something they *know* (like a PIN or password); (2) by something they *have* (like a physical device or token); or (3) by something they *are* (like a physical characteristic such as a fingerprint, or an age and birthdate). Authenticators should not be widely known, perhaps even should be secret. The problem is that SSNs are *widely* known,[60] and even if not known, can be accurately predicted by computer statistical analysis as shown by the Carnegie Mellon research discussed immediately above. The historic use of SSNs as an authenticator by Minnesota's natural gas and electric utilities is not a sufficient reason for the Commission to approve the continued collection and use of SSNs.

C. *Reasonable Alternatives Exist to the Use of SSNs for Identification and Authentication.*

The Commission inquired in its July 2013 Order in this proceeding whether it would be appropriate for utilities to "collect and maintain customer social security numbers, and if so the purpose for doing so, and specifying whether the utility could use the information solely to create a unique account identifier and then to purge the number from its records." (para. 3(f)). LSAP believes that the thinking behind the Commission's query is appropriate, but that the specifics of the question can be improved. With some modification, the fundamental elements of the Commission's proposal can be retained while addressing the continuing problems that would exist in the absence of modification.

The alternative recommended by LSAP is a process through which Minnesota utilities would create a unique, long-term identifier to use in matching customers intra-jurisdictionally (i.e., between service addresses) and over time. LSAP's recommended process is to use a computer algorithm to digitize a person's full name, date of birth, parent's name, place of birth and/or other permanent personal characteristic.[61] Such a digitized personal identifier cannot be copied.

---

[59] Garfinkel (October 1995). "Risks of Social Security Numbers," Vol. 38, No. 10, Communications of the ACM.

[60] See e.g., Given (December 2007). "Uses of Social Security Numbers in the Private Sector: Why SSNs are not Appropriate for Authentication," Privacy Rights Clearinghouse presentation to the Federal Trade Commission Workshop "Security in Numbers: SSNs and ID Theft."

[61] Consider, for example, MIB, Inc. (formerly known as the Medical Information Bureau), a nonprofit cooperative insurance association, which uses a similar methodology. MIB reports: ". . .MIB's records cannot be used to actually perpetrate identity theft. MIB is unique compared to other consumer reporting agencies (i.e., credit agencies) because the consumer information stored by MIB, by its nature, cannot be used in the furtherance of identity theft. MIB uses an applicant's name, date of birth and place of birth (if known) as the primary identifiers used to locate a record in the database. MIB does not collect contact information such as address or telephone number, nor does it require its members to report the applicant's SSN or policy number. In the event that a Member reports a consumer's SSN, MIB "hashes" the SSN (i.e., uses a one-way irreversible "hash," which is an encryption

Moreover, according to one national privacy expert, such a digitized personal identifier has the added advantage that a search file will return the closest match, thus allowing recognition of a positive match even if not all of the elements are "right."[62] According to the Privacy Journal:

> Proprietary forms of this methodology include SOUNDEX, Alpha Search, and SearchSoftwareAmerica. Federal Express, the National Insurance Crime Bureau, VISA and Wasau Insurance use variations of these techniques. The state of Maryland keeps track of millions of motor-vehicle files with these methodologies.[63]

The Privacy Journal reports that "[l]imiting collection of SSNs will not be disruptive. With today's database technology, the SSN and other personal identifiers make using SSNs or any numerical identifier unnecessary."[64]

D. SSN Summary and Conclusions

SSNs are an "aging technology" and Minnesota gas and electric utilities have to do serious planning on what will come next, according to one privacy expert. Other researchers, publishing in the proceedings of the National Academy of Science, conclude that industry and policy makers need to "reassess our perilous reliance" on SSNs. The federal government has told all federal Executive Agencies to "eliminate the unnecessary collection and use" of SSNs. The Presidential Task Force on Identity Theft concludes that "more must be done to eliminate the unnecessary use of SSNs."

Reasonable alternatives exist to the continued collection and use of SSNs by Minnesota's gas and electric utilities. No reason exists for the Commission to lag behind in eliminating or minimizing the use of SSNs. At the state and federal level, as well as at the regulatory level for businesses other than public utilities (e.g., educational institutions, financial institutions), there is a distinct move to find alternatives to the use of SSNs to help reduce the threat of identity theft. The Commission should join in those efforts.

III. THE ADOPTION AND USE OF FAIR INFORMATION PRACTICES (FIPS).

The Commission inquired in its July 2013 order in this proceeding whether it would be appropriate for it to "adopt the Fair Information Practices (FIPs) as the guiding set of privacy

---

algorithm) at the edge of its network and never stores the actual number in its systems. MIB also does not collect bank or credit card account numbers (with or without associated PINs)." MIB (2013). New Breed of Identity Crime: Medical Identity Theft, http://www.mib.com/medical_identity.html, last accessed August 23, 2013.

[62] Smith (2012). Social Security Number: Uses and Abuses, A Special Report for the American Free Press from the Privacy Journal, Providence (RI).

[63] Id., at 19.

[64] Id.

principles and as the standard benchmark against which utility privacy actions will be assessed." (para. 3(b)). For all the reasons stated in its previous comments in this proceeding, LSAP urges the PUC to adopt the FIPs for such purposes.

There is, however, no ***single*** set of FIPs for the PUC to adopt simply by reference to "the FIPs." For the reasons stated in its previous comments, LSAP urges the Commission to adopt the FIPs promulgated by the Organisation for Economic Co-operation and Development (OECD) as cited and quoted in LSAP's previous comments.

Appendix A to these comments sets out a comparison of the FIPS as set forth in the Obama Administration's proposed "consumer privacy bill of rights," the OECD privacy guidelines (excerpts), the Asia-Pacific Economic Cooperation (APEC) principles, and the Department of Homeland Security (DHS) privacy policy.[65] Appendix B to these comments sets forth a similar comparison published by the National Institute of Standards and Technology.[66]

IV. THE SALE AND SHARING OF CUSTOMER INFORMATION.

The Commission inquired in its June 17, 2013 Order in this docket whether there are circumstances in which Minnesota utilities should be allowed to sell personally identifiable information (para. 3(e)) or to share such information with unregulated affiliates (para. 3(g)). LSAP urges that both the sale and sharing of PII be prohibited.[67]

Three separate, but related, reasons exist to ban the sale and/or sharing of personal information with third parties, including unregulated affiliates.

First, the sale and/or sharing of information gives rise not merely to the possibility, but also to the probability, that the utility-supplied personal information of customers of Minnesota's gas and electric utilities will be combined with the non-utility-supplied personal information of those customers to create new, unintended, and non-consensual information products on those customers,[68] often known as "digital dossiers." In other words, it is not merely the utility data that is provided by the sale or sharing of the personal information, it is the combinations of data and the resulting new insights into customers' lives arising from financial transactions, purchasing patterns, travel patterns, residential locations, voting (and other civic engagements,

[65] The White House (February 2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, at Appendix B.
[66] NIST (April 2010). Guide to Protecting the Confidentiality of Personally Identifiable Information, supra, at Appendix D.
[67] As noted in the PUC's order, and LSAP recognizes, the treatment of CEUD is considered in a separate process and these comments do not relate to CEUD. LSAP's comments on the sale and/or sharing of CEUD were presented in its Initial Comments in this Docket.
[68] GAO (April 2006). Agency and Reseller Adherence to Key Privacy Principles, GAO-06-421, at 67 (aggregation of information from multiple sources creates new information products).

such as drivers licenses), criminal histories, and an ongoing list of other data and history stored in matched data bases.

This creation of ***new*** information products/digital dossiers is in sharp conflict with many (if not most) of the Fair Information Practices discussed earlier in these comments, including without limitation:

- Use limitation principle: information is to be used only for the purposes for which it was collected;

- Individual participation principle: consumers have the right to review and correct erroneous information;

- Accountability principle: a specific individual is accountable for the implementation of FIPs;

- Collection limitation principle: entities should obtain only the minimum amount of personal data needed to process a transaction, and maintain only such information about an individual as is necessary; and

- Data quality principle: an entity should ensure the accuracy of data maintained.

The sale or sharing of personal information --including to unregulated affiliated entities, along with the creation of new information products/digital dossiers about Minnesota utility customers-- through the matching of multiple data bases simply cannot be reconciled with these FIPs.

Second, the sale and/or sharing of personal information precludes the ability of Minnesota utility consumers to access, review, and correct (where appropriate) erroneous information that is used "downstream." When personal information is sold or shared, the consumer no longer is in privity with the entity holding and using his or her personal information. If that information is subsequently used to his or her detriment, no mechanism exists to allow the consumer to access that information, let alone to review (and correct if appropriate).

To the extent that the personal information has been combined with other information to create a new information product/digital dossier, it is impossible for the consumer to make corrections. Any modification would exist only until the information-combiner obtains a new set of (incorrect) information to incorporate into the information product/digital dossier.[69] Even if a

[69] Adherence to Key Privacy Principles, supra, at 48 ("resellers stated that making corrections to their databases could be ineffective because the data are continually refreshed with updated data from the source, and thus any correction is likely to be changed back to its original state the next time the data are updated.") While this GAO report references "information resellers," the conclusions are applicable to any information combiners.

correction in the new information product/digital dossier could be made, in other words, the correction exists only until it is subsequently overwritten by the next new set of external data from which the new information product/digital dossier was compiled with which to begin. Indeed, the frequent response by information-combiners is that consumers can only make corrections by going to the original source of information.[70]

Third, the sale or sharing of personal information by Minnesota utilities creates an ever-expanding universe of "downstream" entities through which the personal data might be released. Data breaches are generally not intentional, but rather are a result of a performance lapse. In the financial industry, data breaches are "typically due to lapses in data security by [a] third-party entity (such as a contractor or sub-contractor) and not the financial institution itself."[71] Similarly, two of five information breaches at federal agencies actually involved vendors or contractors rather than the agency itself.[72] As one commentator appropriately notes:

> The advent of the Internet and the proliferation of outsourcing have only magnified the speed and extent of dispersal of the social security number. Just as the weakest link will make a chain give way, the institution with the most lax security procedures or least honest employees may be the only thing standing between a thief and the contents of an individual's bank account and private records.[73]

This concern is not theoretical. A GAO report noted that businesses use contractors for a wide variety of reasons, such as financial statement processing, maintenance services, information technology management, bill collection, and the like.[74] According to the GAO, 90% of private companies outsource some activity.[75] The monitoring and enforcement of privacy protections for downstream outsourcing is extraordinarily difficult.[76]

---

[70] Id., at 48. When information is combined into a new information product/digital dossier, however, the "original source" is not necessarily known to the consumer. See generally, GAO (June 2006). Personal Information: Key Federal Privacy Laws do not Require Information Resellers to Safeguard All Sensitive Data, GAO-06-674.
[71] GAO (June 2007). Data Breaches are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, GAO-07-737, at 15, n.26.
[72] Id., at 22.
[73] Darrow and Lichtenstein, "'Do you Really Need my Social Security Number?' Data Collection Practices in the Digital Age," 10 No. Car. J. L. and Tech. 1, 2 (2008).
[74] GAO (January 2006). Social Security Numbers: Stronger Protections Needed when Contractors have Access to SSNs, GAO-06-238, at 10 – 11.
[75] GAO (March 2006). Social Security Numbers: More could be Done to Protect SSNs, GAO-06-586T, at 3 – 4; see also, GAO (June 2007). Social Security Numbers: Use is Widespread and Protection could be Improved, GAO-07-1023T, at 9.
[76] GAO (September 2006). Privacy: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid and TRICARE, GAO-06-676; see also, Robbins and Walleghem, "Technology Outsourcing: A Community Bank Perspective," Financial Industry Perspectives, Federal Reserve Bank of Kansas City, at 32 (4th Qtr 2004) ("The inherent risks of technology applications in financial institutions have always required rigorous controls to address risks related to the security, availability and integrity of technology systems and resources, and customer

Given the problems documented above, LSAP presents the conclusions of one commentator as offering the best recommendation for the Commission regarding the sale or sharing of personal information with third parties, including unregulated affiliates:

> Banning the sale and rental of private information is not a perfect solution, but it provides the best balance between privacy and business innovation. Allowing companies virtually unfettered use of the data they collect allows them to continue to innovate. Banning the dissemination of that data, however, keeps it contained. This containment has several benefits. First, it allows the customer or web surfer to know that her data will be available only to companies that she does business with or visits. This presumably will give those concerned about the spread of their private information the reassurance that--at the very least--it will be available only to those they trust enough to give it to in the first place. Second, if such a ban were coupled with more stringent data security laws, it would create some assurance that the collector of that data is responsible for keeping it safe and is unable to share it with another person or entity that might not be as careful. Third, a ban makes it less likely that separate strands of data will be pieced together to discover personal information about a person that she had no intention of sharing. . .This reduces the danger to personal privacy posed by "digital dossiers," because they would be much harder to assemble.[77]

LSAP agrees with the above conclusion and urges the PUC to ban the sale or sharing of personal information with third parties, including affiliates.[78]

V. SUMMARY AND RECOMMENDATIONS

Based on the data and analysis presented above, along with the comments LSAP previously presented in this docket, LSAP recommends as follows:

- The Commission should require Minnesota gas and electric utilities to prepare and file PIAs and ISPs substantially in conformance with the requirements imposed on federal agencies by FISMA and the E-Government Act of 2002, and implementing regulations, standards and guidelines, including specifically OMB and NIST guidelines.

---

privacy. Outsourcing complicates management and control of these risks because the bank is separated from the day-to-day management and physical control over the processes.")

[77] Roethlisberger, "Someone is Watching: The Need for Enhanced Data Protection," 62 Hastings L.J. 1793, 1831 (2011).

[78] These same arguments might apply to the collection and distribution of CEUD, as well. The scope of LSAP's comments here, however, is limited to the need for protection of other personally identifiable information, whether related to credit and collection data, SSNs, and otherwise, through the proposed PIA and ISP process.

- The Commission should immediately prohibit Minnesota utilities from henceforth collecting individual Social Security Numbers from residential customers;[79] prohibit Minnesota utilities from publishing, transmitting, or otherwise communicating SSNs they currently hold to any entity other than the utility, including affiliates and out-sourcing contractors; and prepare and deliver to the Commission within a timeframe deemed to be reasonable by the Commission (e.g., six months) a report containing recommendations on alternatives to the collection and use of SSNs in the future.

- The Commission should adopt the Fair Information Practices (FIPs) promulgated by the Organization for (OECD) as the guiding set of privacy principles, and as the standard benchmark against which Minnesota privacy actions will be assessed;

- The Commission should ban the sale, rental or other distribution or dissemination of personally identifiable information, other than CEUD.[80]

[79] Clearly, even if the Commission "immediately prohibited" Minnesota utilities from collecting individual SSNs, there would need to be a transition period to an SSN alternative. The need for such a transition period, however, does not detract from the need for the PUC to issue the immediate prohibition. No additional "study" period by Minnesota utilities would generate new information on the threats posed by the collection of SSNs, the harms created by the use of SSNs, or the availability of alternatives to the use of SSNs.

[80] CEUD is excepted from this recommendation for the exclusive reason that the PUC is considering the treatment of CEUD in a separate proceeding. This exception should not be read to indicate any "position" on the treatment of CEUD to be determined in that proceeding and accompanying work group process.

Appendix A

CONSUMER DATA PRIVACY IN A NETWORKED WORLD:

A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY

FEBRUARY 2012

Appendix A: The Consumer Privacy Bill of Rights

CONSUMER PRIVACY BILL OF RIGHTS

The Consumer Privacy Bill of Rights applies to *personal data*, which means any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device. The Administration supports Federal legislation that adopts the principles of the Consumer Privacy Bill of Rights. Even without legislation, the Administration will convene multistakeholder processes that use these rights as a template for codes of conduct that are enforceable by the Federal Trade Commission. These elements—the Consumer Privacy Bill of Rights, codes of conduct, and strong enforcement—will increase interoperability between the U.S. consumer data privacy framework and those of our international partners.

1. **INDIVIDUAL CONTROL: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.** Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place.

2. **TRANSPARENCY: Consumers have a right to easily understandable and accessible information about privacy and security practices.** At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.

3. **RESPECT FOR CONTEXT: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.** Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Control by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If,

subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults.

4. **SECURITY: Consumers have a right to secure and responsible handling of personal data.** Companies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.

5. **ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.** Companies should use reasonable measures to ensure they maintain accurate personal data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures they may use to maintain accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm.

6. **FOCUSED COLLECTION: Consumers have a right to reasonable limits on the personal data that companies collect and retain.** Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise.

7. **ACCOUNTABILITY: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.** Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for adhering to these principles. To achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise.

Appendix B: Comparison of the Consumer Privacy Bill of Rights to Other Statements of the Fair Information Practice Principles (FIPPs)

Consumer Privacy Bill of Rights	OECD Privacy Guidelines (excerpts)	DHS Privacy Policy (generalized)	APEC Principles (excerpts)
Individual Control. Consumers have a right to exercise control over what personal data that companies collect from them and how they use it.	**Use Limitation Principle.** Personal data should not be disclosed . . . except "with the consent of the data subject or by the authority of law."	**Individual Participation.** Organizations should involve the individual in the process of using PII [personally identifiable information] and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII.	**Choice.** Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.
Transparency. Consumers have a right to easily understandable information about privacy and security practices.	**Openness Principle.** There should be a general policy of openness about developments, practices and policies with respect to personal data.	**Transparency.** Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of PII.	**Notice.** Personal information controllers should provide clear and easily accessible statements about their practices and policies . . . .

Consumer Privacy Bill of Rights	OECD Privacy Guidelines (excerpts)	DHS Privacy Policy (generalized)	APEC Principles (excerpts)
Respect for Context. Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.	**Purpose Specification Principle.** 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.	**Purpose Specification.** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.	**Notice.** All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.
	Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [purpose specification] except . . . (a) with the consent of the data subject; or (b) by the authority of law.	**Use Limitation.** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.	**Uses of Personal Information.** Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.
Security. Consumers have a right to secure and responsible handling of personal data.	**Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.	**Security.** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.	**Security Safeguards.** Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses.

Consumer Privacy Bill of Rights	OECD Privacy Guidelines (excerpts)	DHS Privacy Policy (generalized)	APEC Principles (excerpts)
Access and Accuracy. Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.	**Individual Participation Principle.** 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; d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.	**Data Quality and Integrity.** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.	**Access and Correction.** Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is generally understandable; and, c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.
	Data Quality Principle. 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.		**Integrity of Personal Information.** Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
			Preventing Harm. Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information.

Consumer Privacy Bill of Rights	OECD Privacy Guidelines (excerpts)	DHS Privacy Policy (generalized)	APEC Principles (excerpts)
Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.	**Collection Limitation Principle.** 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 Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).	**Collection Limitation.** The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.
Accountability. Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.	**Accountability Principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.	**Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.	**Accountability.** A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

Appendix B

NIST Special Publication 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2010

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Director

Appendix D—Fair Information Practices

The Fair Information Practices, also known as Privacy Principles, are the framework for most modern privacy laws around the world. Several versions of the Fair Information Practices have been developed through government studies, Federal agencies, and international organizations. These different versions share common elements, but the elements are divided and expressed differently. The most commonly used versions are discussed in this appendix.[92]

In 1973, the U.S. Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services) issued a report entitled *Records, Computers, and the Rights of Citizens* (commonly referred to as the *HEW Report*). The report was the culmination of an extensive study into data processing in the public and private sectors. The HEW Report recommended that Congress enact legislation adopting a "Code of Fair Information Practices" for automated personal data systems. The recommended Fair Information Practices became the foundation for the Privacy Act of 1974. The HEW Report Fair Information Practices included the following:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information is in his or her file and how the information is being used.
- There must be a way for an individual to correct information in his or her records.
- Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse.
- There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

In 1980, the Organisation for Economic Co-operation and Development (OECD)[93] adopted *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which provide a framework for privacy that has been referenced in U.S. Federal guidance and internationally. The OECD Guidelines, along with the Council of Europe Convention,[94] became the foundation for the European Union's Data Protection Directive.[95] The OECD Guidelines include the following Privacy Principles:

- **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.

---

92 Portions of this appendix were contributed to and published in the Executive Office of the President, National Science and Technology Council's *Identity Management Task Force Report 2008*, see http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf.

93 The U.S. is an OECD member country and participated in the development of the OECD Privacy Guidelines, see http://www.ftc.gov/speeches/thompson/thomtacdremarks.shtm.

94 In 1981, the Council of Europe enacted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, which also recognized the Fair Information Practices.

95 In 1995, the European Union enacted the *Data Protection Directive*, Directive 95/46/EC, which required member states to harmonize their national legislation with the terms of the Directive, including the Fair Information Practices. For additional information, see Jody R. Westby, *International Guide to Privacy*, American Bar Association Publishing, 2004.

- **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.

In 2004, the Federal CIO Council published the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP).[96] It included a set of privacy control families based on Fair Information Practices. The privacy control families were intended to provide guidance for integrating privacy requirements into the Federal Enterprise Architecture. In 2009, the CIO Council drafted a revised set of privacy control families.[97] The revised set contains the following privacy control families:

- **Transparency**—Providing notice to the individual regarding the collection, use, dissemination, and maintenance of PII.

- **Individual Participation and Redress**—Involving the individual in the process of using PII and seeking individual consent for the collection, use, dissemination, and maintenance of PII. Providing mechanisms for appropriate access, correction, and redress regarding the use of PII.

- **Purpose Specification**— Specifically articulating the authority that permits the collection of PII and specifically articulating the purpose or purposes for which the PII is intended to be used.

- **Data Minimization and Retention**—Only collecting PII that is directly relevant and necessary to accomplish the specified purpose(s). Only retaining PII for as long as is necessary to fulfill the specified purpose(s) and in accordance with the National Archives and Records Administration (NARA) approved record retention schedule.

---

[96] FEA-SPP, Version 2, http://cio.gov/documents/Security_and_Privacy_Profile_v2.pdf.

[97] This set of privacy control families is based on the working draft of Version 3 of FEA-SPP, August 28, 2009. It is expected to be finalized and published in 2010.

- **Use Limitation**—Using PII solely for the purpose(s) specified in the public notice. Sharing information should be for a purpose compatible with the purpose for which the information was collected.
- **Data Quality and Integrity**—Ensuring, to the greatest extent possible, that PII is accurate, relevant, timely, and complete for the purposes for which it is to be used, as identified in the public notice.
- **Security**—Protecting PII (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing**—Providing accountability for compliance with all applicable privacy protection requirements, including all identified authorities and established policies and procedures that govern the collection, use, dissemination, and maintenance of PII. Auditing for the actual use of PII to demonstrate compliance with established privacy controls.

In 2004, the Asia-Pacific Economic Cooperation (APEC) ministers officially endorsed the Privacy Framework[98] developed within one of its committees. The APEC Privacy Framework was based on the OECD Privacy Guidelines and was developed to encourage electronic commerce among the member states and to build trust with the international community. The Privacy Framework includes the following Privacy Principles:

- **Preventing Harm—**Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.
- **Notice—**Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information.
- **Collection Limitation—**The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.
- **Uses of Personal Information—**Personal information collected should be used only to fulfill the purposes of the collection and other compatible related purposes, except with the consent of the individual, when necessary to provide a product or service requested by the individual, or by authority of law.
- **Choice—**Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.
- **Integrity of Personal Information—**Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
- **Security Safeguards—**Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other

[98] http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held, and they should be subject to periodic review and reassessment.

- **Access and Correction—**Individuals should be able to obtain from the personal information controller confirmation of whether the personal information controller holds personal information about them, have the information provided to them at a reasonable charge and within a reasonable time, and challenge the accuracy of the information, as well as have the information corrected or deleted. Exceptions include situations where the burden would be disproportionate to the risks to the individual's privacy, the information should not be disclosed due to legal or security concerns, and the privacy of other persons would be violated.
- **Accountability—**A personal information controller should be accountable for complying with measures that give effect to the Principles stated above.

CERTIFICATE OF SERVICE
DOCKET NO. E,G-999/CI-12-1344

I, Roger Colton, hereby certify that I have this day served copies of the foregoing document on the attached list of persons.

xxx	by depositing a true and correct copy thereof, properly enveloped with postage paid in the United States Mail in Belmont, MA
xxx	electronic filing

Dated this 30th day of August 2013

/s/

_____

Roger D. Colton
34 Warwick Road
Belmont, MA 02478

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	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
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
Cesar	Caballero	Cesar.Caballero@windstream.com	McLeodUSA Telecommunications Services, LLC	4001 Rodney Parham Little Rock, AR 72212	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
James R	Denniston	james.r.denniston@xcelenergy.com	Xcel Energy	414 Nicollet Mall 5th Floor Minneapolis, MN 55401	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Ian	Dobson	ian.dobson@ag.state.mn.us	Office of the Attorney General-RUD	1400 Bremer Tower 445 Minnesota Street St. Paul, MN 55101	Electronic 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
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
Jim	Hawley	jhawley@technet.org	Technology Network (TechNet)	1215 K Street, Suite 1900 Sacramento, California 95818	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
Nikki	Kupser	nkupser@greatermngas.com	Greater Minnesota Gas, Inc.	202 South Main Street P.O. Box 68 Le Sueur, MN 56058	Paper 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
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
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	apm@mcmlaw.com	Mackall, Crounse and Moore	1400 AT&T Tower 901 Marquette Ave Minneapolis, MN 55402	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
Richard	Savelkoul	rsavelkoul@martinsquires.com	Martin & Squires, P.A.	444 Cedar St Ste 2050 St. Paul, MN 55101	Electronic Service	No	SPL_SL_12-1344_Interested Parties
Kevin	Saville	KSaville@czn.com	Citizens Telecommunications Company of MN,LLC	2378 Wilshire Blvd Mound, MN 55364	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

First Name	Last Name	Email	Company Name	Address	Delivery Method	View Trade Secret	Service List Name
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	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	Paper Service	No	SPL_SL_12-1344_Interested Parties

Revised CERTIFICATE OF SERVICE
DOCKET NO. E,G-999/CI-12-1344

I, Roger Colton, hereby certify that I have this day served copies of the foregoing document on the attached list of persons.

Xxx	by depositing a true and correct copy thereof, properly enveloped with postage paid in the United States Mail in Belmont, MA
Xxx	electronic filing

Dated this 30th day of August 2013

/s/

_____

Roger D. Colton
34 Warwick Road
Belmont, MA 02478

Last Name	First Name	Email	Company Name	Delivery Method	View Trade Secret
Aberle	Tamie A.	tamie.aberle@mdu.com	Great Plains Natural Gas Co.	Electronic Service	No
Ahern	Michael	ahern.michael@dorsey.com	Dorsey & Whitney, LLP	Electronic Service	No
Anderson	Kristine	kanderson@greatermngas.com	Greater Minnesota Gas, Inc.	Electronic Service	No
Anderson	Julia	Julia.Anderson@ag.state.mn.us	Office of the Attorney General-DOC	Electronic Service	Yes
BeVier	Martin S.	bevi0022@umn.edu	N/A	Electronic Service	No
Berndt	Emma	emma.berndt@opower.com	Opower	Electronic Service	No
Bohler	Scott	scott.bohler@ftr.com	Frontier Communications Corporation	Electronic Service	No
Christensen	Brent	bchristensen@mnta.org	Minnesota Telecom Alliance	Electronic Service	No
Colton	Roger	roger@fsconline.com	N/A	Electronic Service	No
Dobson	Ian	ian.dobson@ag.state.mn.us	Office of the Attorney General-RUD	Electronic Service	No
Downer	Steve	sdowner@mmua.org	MMUA	Electronic Service	No
Elwood	Ron	relwood@mnlsap.org	Legal Services Advocacy Project	Electronic Service	No
Ferguson	Sharon	sharon.ferguson@state.mn.us	Department of Commerce	Electronic Service	No
Haar	Burl W.	burl.haar@state.mn.us	Public Utilities Commission	Electronic Service	Yes
Hoyum	Lori	lhoyum@mnpower.com	Minnesota Power	Electronic Service	No
Kismohr	Steve	skismohr@mwalliance.org	Midwest Energy Efficiency Alliance	Electronic Service	No
Kupser	Nicolle	nkupser@greatermngas.com	Greater Minnesota Gas, Inc.	Electronic Service	No
Larson	Douglas	dlarson@dakotaelectric.com	Dakota Electric Association	Electronic Service	No
Lindell	John	agorud.ecf@ag.state.mn.us	Office of the Attorney General-RUD	Electronic Service	Yes
Moeller	David	dmoeller@allete.com	Minnesota Power	Electronic Service	No
Moratzka	Andrew	apmoratzka@stoel.com	Stoel Rives LLP	Electronic Service	No
Norris	Samantha	samanthanorris@alliantenergy.com	Alliant Energy	Electronic Service	No
Palmer	Greg	gpalmer@greatermngas.com	Greater Minnesota Gas, Inc.	Electronic Service	No
Pyles	Adam	adam.pyles@centerpointenergy.com	CenterPoint Energy	Electronic Service	No
Ragsdale	Kent	kentragsdale@alliantenergy.com	Alliant Energy-Interstate Power and Light Company	Electronic Service	No
Savelkoul	Richard	rsavelkoul@martinsquires.com	Martin & Squires, P.A.	Electronic Service	No
Saville	Kevin	kevin.saville@ftr.com	Citizens/Frontier Communications	Electronic Service	No
Slotterback	Brendon	brendon.slotterback@minneapolismn.gov	City of Minneapolis	Electronic Service	No
Sorum	Peggy	peggy.sorum@centerpointenergy.com	CenterPoint Energy	Electronic Service	No
Spangler, Jr.	Ron	rlspangler@otpco.com	Otter Tail Power Company	Electronic Service	No
Thompson	SaGonna	Regulatory.Records@xcelenergy.com	Xcel Energy	Electronic Service	No
Topp	Jason	jason.topp@centurylink.com	CenturyLink	Electronic Service	No
Walters	Gregory	gjwalters@minnesotaenergyresources.com	Minnesota Energy Resources Corporation	Electronic Service	No
Woeste	Robyn	robynwoeste@alliantenergy.com	Interstate Power and Light Company	Electronic Service	No

Last Name	First Name	Company Name	Address	Delivery Method	View Trade Secret
Anderson	Arnie	Minnesota Community Action Partnership	MCIT Building, 100 Empire Drive, Suite 202, St. Paul, MN - 55103	Paper Service	No
Blauvelt	Katherine	Sen. Al Franken Saint Paul Office	60 East Plato Blvd Suite 220, Saint Paul, MN - 55107	Paper Service	No
Braman	Jon	Bright Power, Inc.	11 Hanover Square, 21st floor, New York, NY - 10005	Paper Service	No
Brezinka	Sheri	USGBC-Minnesota Chapter	5353 Wayzata Blvd Suite 350, Minneapolis, MN - 55416	Paper Service	No
Brown	Peter	Minnesota Tenants Union	2121 Nicollet Ave Ste 203, Minneapolis, MN - 55404	Paper Service	No
Bull	Michael J.	Center for Energy and Environment	212 Third Avenue North, Suite 560, Minneapolis, MN - 55401	Paper Service	No
Caballero	Cesar	McLeodUSA Telecommunications Services, LLC	4001 Rodney Parham, Little Rock, AR - 72212	Paper Service	No
Carter	Richard	N/A	371 Water Street, Excelsior, MN - 55331	Paper Service	No
Clearwater	Andrew	Future of Privacy Forum	919 18th Street N.W. Suite 901, Washington, DC - 20006	Paper Service	No
Flisrand	Janne	MN Green Communities	c/o Flisrand Consulting, 2112 Dupont Ave. S, Minneapolis, MN - 55405	Paper Service	No
Hawley	Jim	Technology Network (TechNet)	1215 K Street, Suite 1900, Sacramento, California - 95818	Paper Service	No
Horton	Caroline	Aeon	901 N. 3rd St. Suite 150, Minneapolis, MN - 55401	Paper Service	No

Last Name	First Name	Company Name	Address	Delivery Method	View Trade Secret
Johnson	Joel	Minnesota Rural Electric Association	11640 73rd Avenue N, Maple Grove, MN - 55369	Paper Service	No
Johnson	Craig	League of Minnesota Cities	145 University Ave. W., Saint Paul, MN - 55103-2044	Paper Service	No
Krukowski	Andrea	Institute for Market Transformation	1707 L Street NW Ste 1050, Washington, DC - 20036	Paper Service	No
Lewis	Kevin	Greater Minneapolis BOMA	Suite 610, 121 South 8th Street, Minneapolis, MN - 55402	Paper Service	No
Liljenquist	Todd	Minnesota Multi Housing Association (MHA)	1600 West 82nd Street, Suite 110, Minneapolis, MN - 55431	Paper Service	No
Lindburg	Alison	Fresh Energy	408 Saint Peter St. Ste 220, Saint Paul, MN - 55102	Paper Service	No
Matthews	J.B.	Cushman & Wakefield/NorthMarq	3500 American Blvd W - #200, Minneapolis, MN - 55431	Paper Service	No
McDonough	Amy	AARP	30 E 7th Street, Suite 1200, St. Paul, MN - 55101	Paper Service	No
Stephenson	Gary	Otter Tail Power Company	215 South Cascade Street, Fergus Falls, MN - 56537	Paper Service	No
Whitney	Patricia	St. Paul Assn of Responsible Landlords	2197 Silver Lake Road NW, New Brighton, MN - 55112	Paper Service	No
Wilson	Elizabeth	Humphrey School of Public Affairs	130 Humphrey School, 301 19th Ave. S, Minneapolis, MN - 55455	Paper Service	No

Last Name	First Name	Company Name	Address	Delivery Method	View Trade Secret
Winters	Josh	MPIRG	2722 University Ave SE, Minneapolis, MN - 55414	Paper Service	No