MAINE PUBLIC UTILITIES COMMISSION

REPORT ON CYBER-SECURITY AND PRIVACY ISSUES RELATING TO SMART METERS

SUBMITTED TO THE JOINT STANDING COMMITTEE ON ENERGY, UTILITIES AND TECHNOLOGY

January 15, 2012

TABLE OF CONTENTS

I. INTRODUCTION

A. Legislative Resolve

During the 2011 session, the Legislature enacted Resolve, To Examine Cyber Security and Privacy Issues Relating to Smart Meters.[1] The Resolve directs the Commission to open an inquiry for comments, examine cyber security and privacy issues regarding smart meters and provide a report to the Legislature. Specifically, the Resolve states:

> **Sec. 1. Examination of cyber security and privacy issues relating to smart meters. Resolved:** That the Public Utilities Commission shall examine current cyber security and privacy requirements that exist under federal and state law, rules and utility policies and practices that apply to transmission and distribution utilities and identify potential regulatory gaps that may exist by examining the extent to which existing federal requirements may or may not apply to cyber security and privacy issues regarding smart meters and related systems. To the extent regulatory gaps exist, the commission shall develop recommendations to address them. As part of this examination, the commission also shall consider issues related to access to customer data and the disclosure of transmission and distribution utility residential electric energy consumption and cost information pursuant to the Maine Revised Statutes, Title 14, section 6045; and be it further
>
> **Sec. 2. Monitor federal cyber security initiative. Resolved:** That the Public Utilities Commission shall actively monitor the efforts by the United States Department of Energy to launch a cyber security initiative to enhance cyber security on the electric grid with input from the Federal Energy Regulatory Commission, the United States Department of Homeland Security and publicly and privately owned utilities.

The Resolve specifies that the Commission report the results of its study, including the progress of the federal cyber security initiative as it applies to smart meters and related systems, to the Joint Standing Committee on Energy, Utilities, and Technology by January 15, 2012.

B. Inquiry Process

To obtain information, viewpoints and recommendations from interested persons on the issues identified in the Resolve, on August 17, 2011, the Commission initiated an Inquiry.[2] The Notice of Investigation (NOI) was sent to interested persons, including individuals who testified or commented on LD 756 (the bill that led to the enactment of

[1] Resolves, 2011, ch. 82 (See Appendix A).

[2] *Inquiry into Cyber Security and Privacy Issues Regarding Smart Meters and Related Systems,* Docket No. 2011-274 (August 17, 2011).

Resolves 2011, ch. 82), all transmission and distribution utilities, all competitive electricity providers (CEPs), the service list in Docket No. 2010-345 (smart meter opt-out investigation), Efficiency Maine Trust, Industrial Energy Consumers Group, Office of Energy Independence and Security, and Office of the Public Advocate (OPA). The following entities and individuals responded to the NOI: Central Maine Power (CMP), Bangor Hydro Electric Company (BHE), the Retail Energy Supply Association[3], Richard McKenney, Robin Noyes, Jeanne M. Sonia, and the Public Advocate. Comments and reply comments were received in September.[4]

The Commission issued a draft report for comment from interested persons on December 22, 2011 and requested comments by January 5, 2012. The Commission received comments from the OPA, Dianne Wilkins, Ed Friedman, and Suzanne Foley-Ferguson.

II. MAINE UTILITY SMART METER PROGRAMS

Two of Maine's investor-owned transmission and distribution (T&D) utilities either have installed smart meters[5] or are currently in the process of installing them. Both are in the process of designing dynamic pricing options.

On February 25, 2010, the Commission issued an order approving installation by CMP of advanced metering infrastructure (AMI), finding that the benefits in terms of savings and utility operational cost savings are likely to exceed the costs of the investment.[6] On October 27, 2009, the Department of Energy (DOE) notified CMP that it had received approximately $90 million (representing 50% of the cost of CMP's AMI project) in funding under the DOE's Smart Grid Investment Grant Program. AMI includes smart meters and related systems that allow for automated and remote meter reading, detailed customer usage measurement and data storage, and communications to and from customer meters. CMP's AMI system communicates and transmits data using a wireless "mesh" network made up of

[3] RESA is a nonprofit organization and trade association and its members include providers of competitive electric supply products to customer in the five restructured New England states. RESA's members include: Champion Energy Services, LLC; ConEdison *Solutions*; Constellation NewEnergy Company; GDF SUEZ Energy Resources NA, Incl; Green Mountain Energy Company; Hess Corporation; Integrys Energy Services, Inc.; Just Energy; Liberty Power; MC Squared Energy Services, LLC; Mint Energy, LLC; MXenergy; NextEra Energy Services; Noble Americas Energy Solutions LLC/ PPL EnergyPlus, LLC; Reliant and TriEagle Energy, L.P..

[4] Filings in Docket No. 2011-274 may be accessed from the Commission's Virtual Case file at http://mpuc.informe.org/easyfile/easyweb.php?func=easyweb_splashpage..

[5] A smart meter is a meter capable of recording electricity consumption in short intervals, such as an hour or less. This allows customers to utilize "time-of-use" pricing, in which the cost they pay for electricity varies with the time that the electricity is used. Time-of-use pricing is also referred to as "dynamic pricing."

[6] *Order Approving Installation of AMI Technology*, Docket No. 2007-215(II) (Feb. 25, 2010).

individual customer meters, repeaters and other devices that are being installed throughout CMP's service territory. On December 20, 2007, the Commission approved BHE's plan to install AMI for all of its customers.[7] While CMP uses wireless smart meters, BHE's smart meters are hard-wired.[8]

The CMP and BHE AMI programs provide both utility operations savings (e.g., lower storm restoration) and a platform for programs that allow customers to lower their energy costs and use energy more efficiently through more accurate and timely information and pricing programs that better reflect the hourly and seasonal differences in electricity costs (e.g., time-of-use (TOU) rates). Such time-differentiated rates could include: optional TOU standard offer rates for residential and smaller commercial customers (whereby customers see the same cost differentials incurred by suppliers in the market); optional dynamic pricing programs whereby customers can lower their bills by reducing usage during the peak hours of the year; and programs that allow suppliers (or the utility on their behalf) to directly control customer loads. Programs may also include systems that would allow customers to view their account information and any relevant system information through the internet, as well as systems that provide market or meter information via AMI equipment back to the customer or the customer's appliances. This could occur by sending a signal from the meter to in-home display units, or by sending a signal directly to particular appliances equipped with receiving units. TOU pricing programs are currently being developed for CMP and BHE in Docket Nos. 2010-132 and 2010-14.[9]

III. CYBER-SECURITY ISSUES

Section 1 of the Resolve requires that the Commission examine current cyber security requirements that exist under federal and state law and utility policies and practices that relate to smart meters. In examining current cyber security laws, the Commission is to determine whether any regulatory gaps exist, and to the extent such regulatory gaps do exist, develop recommendations to address them.

A. Federal Laws and Guidelines Regarding Cyber Security

Through the Commission's NOI, the Commission received information from BHE and CMP on the cyber security laws and guidelines that govern or guide each utility in developing its AMI programs. While various federal laws provide rules for cyber security in general, they do not explicitly address all the cyber security concerns of smart meters. Various organizations are currently in the process of developing guidelines that address the unique aspects of the smart grid. In particular, the National Institute of Standards and Technology's

[7] *Order Approving Stipulation*, Docket No. 2006-661 (Dec. 20, 2007).

[8] BHE's smart meters transmit information over the electric wires to the sub-station. From the sub-station, the information is transmitted over the public switched telephone network.

[9] Filings in these dockets may be accessed from the Commission's Virtual Case File at http://mpuc.informe.org/easyfile/easyweb.php?func=easyweb_splashpage.

(NIST) Smart Grid Interoperability Panel (SGIP) and DOE's Cyber Security Initiative are developing guidelines that will have particular relevance to smart grid cyber security. Additionally, the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) standards may also be seen as guidelines for smart grid cyber security. These efforts are described below.

1. NIST's Smart Grid Interoperability Panel

The Energy Independence and Security Act of 2007[10] ("EISA") made it the policy of the United States to implement smart grid technologies to modernize the country's aging electricity grid. EISA assigned to NIST "primary responsibility to coordinate the development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems."[11] NIST is a measurement standards laboratory and is a non-regulatory agency of the United States Department of Commerce. NIST is to seek input and cooperation from various entities, including the Federal Energy Regulatory Commission (FERC) and DOE's Office of Electricity Delivery and Energy Reliability, along with private entities interested in protocols and standards. Once NIST's work has led to sufficient consensus, as determined by FERC, EISA directs FERC to institute a rulemaking proceeding in order to adopt developed standards and protocols.[12] EISA does not authorize FERC to require compliance with the final standards but FERC may consider requiring compliance under its Federal Power Act authorities.

NIST established the SGIP, which is made up of more than 600 organizations and charged with identifying gaps in smart grid cyber security regulations and developing standards to address those gaps. In August 2009, NIST launched a three-phase plan:

I. Identify gaps in currently available standards and establish applicable standards through a participatory public process;

II. Establish the SGIP to continue to develop standards; and

III. Develop a framework for conformity testing and certification.

In January 2010, NIST published a framework and roadmap that identified standards applicable to the smart grid.[13] In October 2010, NIST released a suite of five

[10] Public Law 110-140 (EISA).

[11] Id. Title XIII, Section 1305.

[12] Id. Title XIII, Section 1305(d).

[13] *Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*, NIST Special Publication 1108, January 2010, available at http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

standards for consideration by FERC.[14] However, on July 19, 2011, FERC issued an order on the proposed five standards and found insufficient consensus to institute a rulemaking.[15] While sufficient consensus has not yet been reached, FERC continues to encourage stakeholders to participate in the NIST interoperability process and to continue to work toward developing sufficient standards. Since FERC's July Order, NIST has continued to make progress and in October 2011 released a new report on the development of these standards.[16]

2. Department of Energy's Cyber Security Initiative

In February 2011, the DOE launched an initiative to enhance cyber security on the electric grid. The initiative is led by the DOE's Office of Electricity Delivery and Energy Reliability, NIST and NERC. This is a separate initiative from the NIST's Smart Grid Interoperability Panel, but involves many of the same organizations. The initiative is an open collaboration and is developing cyber security risk management guidelines. The Risk Management Process (RMP) guideline was released for comment in September 2011. It is expected that the document will be a useful tool for developing and improving electricity sector organizations' cyber security programs. Comments on the RMP were due on October 28, 2011.[17]

3. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards

The Energy Policy Act of 2005 (Energy Policy Act) gave FERC authority to impose mandatory reliability standards on the bulk transmission system.[18] Compliance with

[14] *Summaries of Use, Application, Cybersecurity, and Functionality of Smart Grid Interoperability Standards Identified by NIST, Release 1.0*, October 6, 2010, available at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTStandardsSummaries.

[15] *Order, Smart Grid Interoperability Standards*, FERC Docket No. RM11-2-000, July 19, 2011, available at FERC's elibrary, http://elibrary.ferc.gov/IDMWS/search/fercgensearch.asp.

[16] In October, 2011, NIST released *Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0*, which documents many developments related to smart grid cyber security since the release of the framework NIST published in January 2010. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/IKBFramework/Draft_NIST_Framework_Release_2-0_10-17-2011.pdf.

[17] *Electricity Cybersecurity Risk Management Process Guideline, Draft for Public Comment*, Department of Energy, September 2011, https://public.commentworks.com/CW_DOE_WF/InitiativeDocFiles/46/RMP_Guideline_Draft_for_Public_Comment_08312011-1.pdf.

[18] NERC defines the bulk electric system as the "electric power generation facilities combined with the high-voltage transmission, which together create and transport electricity around the continent." *NERC FAQ*, http://www.nerc.com/page.php?cid=1|7|114. It does not include facilities used in the local distribution of electricity, and thus is not directly applicable to smart meters.

these standards is mandatory and NERC is certified as the nation's Electric Reliability Organization.

The NERC standards cover various aspects of the bulk power system, including Critical Infrastructure Protection (CIP). The CIP standards require certain users, owners and operators of the bulk power system to comply with security requirements to safeguard critical cyber assets. Examples of CIP standards include Security Management Controls (requiring that entities have minimum security management controls in place),[19] Personnel and Training (requiring that personnel have authorized cyber or authorized unescorted physical access to Critical Cyber Assets),[20] and Recovery Plans for Critical Cyber Assets (ensuring that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices).[21]

B. CMP and BHE's Cyber Security Practices

As a recipient of a DOE Smart Grid Implementation Grant, CMP was required to create a Cyber Security Plan (CSP). The CSP was approved by DOE and as part of this plan, CMP has developed policies and procedures to protect its Smart Grid system. The policies and policy directives encompass the following areas:

1. Cyber Security Policy
2. Governance Policy
3. Risk Assessment Policy Directive
4. Certification and Authorization Policy Directive
5. Planning Policy Directive
6. System and Service Acquisition Directive
7. Access, Authentication, and Authorization Policy Directive
8. Audit and Accountability Policy Directive
9. System and Communication Protection Policy Directive
10. Awareness and Training Policy Directive
11. Configuration Management Policy Directive
12. Contingency Planning Policy Directive
13. Incident Response Policy Directive
14. Maintenance Policy Directive
15. Media Protection Policy Directive
16. Physical and Environmental Protection Policy Directive
17. Personnel Security Policy Directive
18. System and Information Integrity Policy Directive
19. Compliance Program Management

[19] Standards CIP-003-3 and CIP-003-4.

[20] Standards CIP-004-3 and CIP-004-4.

[21] Standards CIP-009-3 and CIP-009-4.

The DOE works in partnership with all utilities that have received Smart Grid Implementation Grants. The DOE conducts annual site visits in order to review progress with budgets and milestones, along with ensuring implementation of each project's Cyber Security Plan.[22]

Additionally, in its response to the NOI, CMP noted that it had adopted Best Practice Standards based on the Consensus Audit Guidelines (CAG). The CAG findings were based on the collaborative efforts of both government and private sector organizations to create information technology security controls and are based on specific experiences in dealing with particular attacks directed at government and the defense industry's information systems. CMP has adopted Best Practice Standards based on the CAG findings, including:

- Retain data only for a reasonable period of time related to the purpose for which they were collected.
- Adopt privacy and security policies for internal and external access to and use of personally identifiable information that satisfy both legal requirements and fair information privacy principles.
- Define the data collection and use rights of customers, vendors, etc. in clear contractual language with strong privacy and security commitments and accountability for breach.
- Avoid resistance by permitting consumers to turn off or limit detailed data collection, especially during early research phases. Make "Off" the default mode for data transmissions.
- Design security into every collection, access, and transfer point. Create separate pathways for personally identifiable information. Use single hop networks to reduce transmission and storage vulnerabilities.
- Train all utility and third party employees who have access to AMI data or controls.
- Employ internal and external audits.
- Establish incident response and breach notification procedures.
- Establish Board of Directors and senior management oversight of data privacy and security practices.

While BHE follows general federal guidelines in order to ensure smart grid cyber security, it is not a recipient of a Smart Grid Implementation Grant like CMP, and therefore does not have a comparable Cyber Security Plan that has been approved by the DOE. It appears that the NERC CIP standards are the most relevant standards guiding BHE's smart grid security system, and in response to the NOI, BHE noted that it believes its network security goes beyond the requirements of the NERC CIP standards. Some of BHE's network security practices include conducting annual vulnerability assessments along with internal and external audits to validate security practices and employing a third-party security company to monitor its firewalls and alert BHE of potential security risks.

[22] *Recovery Act Smart Grid Programs, Cyber Security*, http://www.smartgrid.gov/recovery_act/overview/standards_interoperability_and_cyber_security/cyber_security.

C. Regulatory Scope for Cyber Security

It appears that current standards (NERC CIP standards) and the evolving standards under development by NIST's Smart Grid Interoperability Panel and DOE's Cyber Security Initiative do not or may not apply to distribution-level smart grid facilities. The NERC CIP standards are only mandatory at the bulk power system level, and while the NIST SGIP standards may eventually result in a rulemaking proceeding by FERC, it is unclear whether such standards could be enforced at any level other than the bulk transmission system. EISA, the Act requiring that FERC institute a rulemaking proceeding once consensus has been reached on NIST SGIP standards, does not allow FERC to require mandatory compliance. While FERC may consider requiring compliance under its Federal Power Act authority, its Federal Power Act jurisdiction is at the bulk power system level and would not be applicable to the smart grid equipment installed on distributed facilities. It is also unclear whether DOE's Cyber Security Initiative will apply beyond the bulk power system.

IV. PRIVACY ISSUES

Section 1 of the Resolve requires that the Commission examine current privacy requirements that exist under federal and state law and utility practices and policies that relate to smart meters. In examining current privacy requirements, the Commission is to determine whether any regulatory gaps exist, and to the extent such regulatory gaps exist, to develop recommendations to address them.

AMI and other smart grid technologies have the potential to improve the reliability of electric service, reduce utility operating expenses and help customers make informed choices that could reduce or lower the cost of their electricity consumption. While utilities already possess detailed information about their customers' electric use, some concerns have been raised that smart meters may generate more detailed or granular data related to the nature and frequency of energy consumption than what was possible with a traditional monthly meter, and that such detailed data could have privacy implications. This more detailed data may make it easier to identify usage and occupancy patterns at a given location – (e.g., when and what appliances are being used and the number of people in a given residence which could reveal when that residence may be empty). Some have argued that there is a need for privacy rules that address the different ways customer information made available with smart meters may be shared with utilities and third parties: 1) from the utility owned smart meter to the utility, 2) from the smart meter to the utility and then from the utility to third-party providers that deliver services to the utility (as its agent) for billing, website support and other functions, 3) data that may also flow from the smart meter to the utility and then from the utility to third-party providers selected by the customers and 4) finally, data the customer may provide from consumer-owned devices within the home to other third-party providers directly.

A. Commission Rule Protecting Customer Information

1. Chapter 815 and Utility Procedures to Comply

Chapter 815, Consumer Protection Standards for Electric and Gas Transmission and Distribution Utilities, of the Commission's rules contain requirements that

utilities must comply with regarding the privacy of customer information. Section 4 of the rule sets the standards for the utility's use of customer data and states:

> **4. CUSTOMER PRIVACY**
>
> A utility shall not disclose, sell or transfer, other than for debt collection, credit reporting, or usage reporting pursuant to state and federal law or to law enforcement agencies pursuant to lawful process, or as otherwise authorized by law, Commission rule or Order, individual customer information, including, but not limited to, a customer's name, address, telephone number, electricity or gas usage, or payment history, to a third party without the consent of a customer. Utilities may accept oral certification from a social service agency that they have received authorization from the customer to discuss that customer's account information. For a consumer-owned utility where its customers are members of the utility's corporation, the utility may share customer information with its corporation members only to the extent necessary to allow for the election of officers and for the utility to perform other functions necessary for the operation of the utility. A utility may also share customer information with State, County, tribal, and local emergency management agency personnel when the customer information is requested at the time of that agency's response to an emergency situation.

In accordance with the Commission's privacy rules, CMP has developed a Policy Regarding the Release of Customer Information (Policy) which provides that except as required by law, regulation or order of authority with jurisdiction over CMP, CMP will not release customer specific information to third parties (except agents of CMP who agree to maintain the confidentiality of such information, such as third-party credit and collection agencies) without consent of the customer.[23] CMP employees who have access to customer specific information are trained on its Policy and the requirements of Section 4 of Chapter 815. The Policy is posted on the Policies section of its intranet site for CMP employees.

BHE's customer service representatives are similarly instructed in new employee and refresher training to guard the privacy of individual customer data in compliance with Chapter 815, Section 4. Should a third party request individual customer information,

[23] Examples of where CMP does release customer-specific information without customer consent are in information responses to the Commission, in response to subpoenas issued by courts or law enforcement (such as the Federal Bureau of Investigation or the Drug Enforcement Agency), to competitive electricity providers (CEPs) pursuant to 35-A M.R.S.A. § 3203(16-A) (which provides that a T&D utility may not release any customer-specific information to a licensed CEP unless the provider produces sufficient evidence, as defined by the Commission by rule, that the provider has obtained the customer's authorization), and to current or prospective customers pursuant to 14 M.R.S.A. § 6045 (which deals with the disclosure of T&D utility residential electric energy consumption and cost information to current and prospective customers, tenants or property owners).

BHE refers them to the Commission to obtain an Order directing BHE to disclose the information. Currently, BHE customers may access their own daily and monthly usage information online by entering their account number (it cannot be accessed by customer name or address). As web tools are enhanced to provide more detailed information, such as hourly consumption and cost information, BHE states that additional security measures will be added, including requiring customers to establish and enter a username and password to access information online.

2. Adequacy of Chapter 815 to Protect Customer Information and Address Privacy Concerns Associated With Smart Meters

The Commission sought comments through the NOI on whether Chapter 815 adequately addresses privacy concerns associated with smart meters and if not, what specific modifications should be made to the rule. The Commission also sought comment on whether any new state laws are necessary to address privacy concerns regarding smart meters and smart meter related equipment.

BHE and CMP believe Chapter 815 adequately addresses privacy concerns regarding smart meters. Both noted that the rule protects customers from utility disclosure of individual customer information, including electricity usage information to a third party without consent of the customer or Commission Order, and that this protection covers monthly, daily, hourly and sub-hourly usage information. BHE noted that time-of-use consumption data has been recorded and stored by utilities and used for billing since 1988 in Maine and that the same security standards exist for all consumption data that BHE collects from its customers. BHE has internal controls in place with regard to utility employee access to individual customer data. Authorized users such as customer service representatives only use the hourly or TOU information to assist customers with billing or usage inquiries, or to address individual customer power quality issues (e.g., blinking lights or voltage issues). Internally, BHE may also look at individual customer usage patterns to investigate potential diversion or theft of services.

The OPA stated that Chapter 815 should be reviewed and expanded to ensure adequate privacy protection, assuming new products and services are offered by new third party market participants. The OPA also raised concerns about the potential for smart metering technologies to provide detailed records of activities within private residences. The OPA pointed to recommendations in NIST's Privacy and the Smart Grid Report[24] as a starting point for discussions on smart meter customer privacy issues in Maine. The more important aspects of the NIST recommendations, in the OPA's view, include issues related to prior customer consent for releasing customer information, with exemptions for short-term emergencies and regulatory requirements; restricting information that is released to only that which is required to complete a specific task and stating the length of time the information may be retained; and adoption of strong security measures, including employee training, to ensure protection of customer information.

[24] NISTIR 7268, *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid* (August 2010) (*NIST Privacy and the Smart Grid Report*).

In the Commission's view, Chapter 815 and utility practices, at this point, sufficiently address the privacy concerns raised by the deployment of smart meters. Chapter 815 currently requires customer consent before releasing customer information, including usage information, to third parties and provides exemptions for emergency situations and regulatory requirements. Both BHE and CMP train their employees who have access to customer information to guard the privacy of individual customer data in compliance with Chapter 815 and have security measures in place to protect this information.

As noted earlier, CMP has also adopted Best Practice Standards, based on the Consensus Audit Guidelines (CAG) agreed to by federal and private industry cyber security officials, which include a number of practices to protect the privacy of customer information. These include retaining data only for a reasonable period of time related to the purpose for which it was collected; designing security into every collection, access, and transfer point; employing internal and external audits; establishing incident response and breach notification procedures; and establishing Board of Directors and senior management oversight of data privacy and security practices.

In addition, the CAG Best Practice Standards include adopting privacy and security policies for internal and external access to and use of personally identifiable information that satisfy both legal requirements and fair information privacy principles;[25] defining the data collection and use rights of customers, vendors, etc, in clear contractual language with strong privacy and security commitments and accountability for breach. CMP has also adopted procedures to comply with Federal Trade Commission Red Flag Rules, which require creditors to implement a written Identity Theft Prevention Program designed to detect the warning signs – or "red flags" – of identify theft in their day-to-day operations.

Finally, BHE suggested that a state law prohibiting hacking and or tampering with utility meters and communications systems could aid in the protection of information and power theft.[26]

With respect to concerns about smart meter information that could reveal occupancy patterns and information about specific appliance usage, BHE stated that its meters do not record small enough intervals to determine what appliances are being used. The smart meters currently in use can only provide the total usage within a specific interval, not individual appliance or circuit usage within a customer's home or business**.** However, BHE does note that in the future, a Home-Area-Network (HAN)[27] that receives real time readings from the

[25] These principles, developed by the Federal Trade Commission, represent widely-accepted concepts concerning fair information practice in an electronic marketplace.

[26] The Commission notes that there is a theft of services statute in Maine (17 M.R.S.A. § 357) which makes theft of electricity and other public utility services a crime. The Commission sought comment in the draft report on whether 17 M.R.S.A. § 357 or other laws sufficiently address BHE's concern. The Commission received no comments on this issue.

[27] A Home Area Network is a residential local area network used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. See DOE Data Access and Privacy Issues Related to Smart Grid Technologies Report (Oct. 5, 2010).

meter likely could determine what appliances are being used but this information would only be accessible in the home and would not be transmitted back to BHE.[28]

CMP similarly stated that for the majority of customers, including residential and small business customers, specific interval data is the only usage type information that is collected from their smart meters. For larger commercial and industrial customers, additional information, such as demand and reactive power data, would be provided by the meters but CMP states this is consistent with information already provided from its meters today.

3. Third Party Information Access

Information that a third party may seek to provide supply services or operate energy management and conservation services for customers could include current and historical usage to support energy usage analysis and rate information to support savings calculations. Other potential third parties who might want access to customer information could include appliance manufacturers, marketers, or vendors creating applications and services for smart appliances, smart meters or other products and services.[29]

In response to the NOI, the Retail Energy Supply Association (RESA) commented that the ability to access real-time customer data in a standardized and cost efficient manner enables suppliers to offer consumers price responsive demand products as well as other new and innovative products that encourage customers to adopt new solutions to meet their energy needs, including making demand response and energy efficiency modifications to better manage their electricity consumption and costs. RESA asserts that a competitive retail providers' ability to offer these products to its customers is directly affected by its ability to have quick, standardized and inexpensive access to customer data and that in many cases the current approach to customer data is an impediment to the advancement of these types of products.

For example, RESA stated that the current method of data dissemination from the T&D utilities varies widely and can encompass anything from a manual process to various forms of Electronic Data Interchange (EDI) and that each T&D implements the method of access and data format differently which requires CEPs to incur costs to ensure compatibility with the different systems. RESA recommends that to ensure that innovative solutions can be created for customers, an EDI policy that defines a standard internet protocol (IP) based access in a common language or data standard would provide the most efficient and cost-effective solution. RESA also commented that T&Ds often charge CEPs a significant amount per account (e.g., $15.00 - $25.00) for access to customer data due, in part, to the manual processes employed for gathering and/or disseminating this information but argues that with the installation of smart meters and the use of EDI, the costs incurred by T&Ds can

---

[28] BHE states that this capability is not currently available, but is being developed by a Smart Grid vendor.

[29] *NIST Privacy and the Smart Grid Report* at 14. NIST intends to address third party access issues in more depth in future reports. *Id*. at p. 12, n. 23.

be reduced significantly and those cost reductions should be passed onto CEPs. RESA also notes that with the installation of smart meters, T&Ds will have more robust information available to them in electronic form (e.g., customer's voltage level) and that this information should also be made available to CEPs with appropriate authorization from the customer.

Chapter 322 of the Commission's rules establishes terms and standards governing metering, billing and collections by T&D utilities and by CEPs. Section 9(A)(5)(a) of the rule provides that before issuing a request to receive customer-specific information, a CEP must obtain customer authorization which may be in writing, provided electronically[30] or occur through a notification in the CEP's terms of service document issued pursuant to Chapter 305 of the Commission's rules.[31] Section 9(A)(5)(b) requires that before providing customer-specific information to the CEP, the T&D utility must obtain written evidence that the provider has complied with the customer authorization requirement.[32]

RESA commented that this latter requirement increases the administrative burden and cost to both the T&Ds and CEPs and unnecessarily makes it more difficult for customers to authorize the release of their data. RESA stated that customers should be free to choose the method by which they authorize the release of their information, such as by third-party verified verbal consent or electronic means including text messaging, and that CEPs, not the T&Ds, should be responsible for maintaining records of those authorizations subject to audit by the Commission.[33] RESA asserts that with the deployment of smart meters, T&Ds will be in a position to collect more valuable and detailed information about consumer usage patterns and that as this information becomes available, the Commission should adopt

[30] The rule also requires that if customer authorization is provided electronically, the CEP must maintain a security system sufficient to confirm the identity of the customer.

[31] Section 9(A)(5)(a) further provides that the notification shall specify that by becoming a customer of the CEP, the customer authorizes the T&D utility to provide customer-specific information to the CEP and that the notification must be conspicuous and precisely identify the information that may be provided. Chapter 305 establishes licensing requirements for CEPs.

[32] The rule further provides that this requirement is satisfied by a contractual provision or a written certification that obligates the CEP to seek customer-specific information from the utility only after complying with the customer authorization requirements contained in Commission rules.

[33] In their submitted Comments on the draft report, the OPA and Dianne Wilkins disagreed with RESA's statement that the rule should be changed to allow for verbal consent. The OPA stated that the current rules requiring written authorization provide essential protection in their current form and should not be changed.

standards that allow for efficient and cost-effective access to this data by competitive providers.[34]

B. Disclosure of T&D Utility Residential Electric Energy Consumption and Cost Information

Finally, the Resolve directed the Commission to consider issues related to access to customer data and the disclosure of transmission and distribution utility residential electric energy consumption and cost information pursuant to 14 M.R.S.A. § 6045 which provides that a T&D utility shall provide, residential electric energy consumption and cost information for a dwelling unit for the prior 12-month period, free of charge, to current or prospective customers, tenants or property owners. Specifically, the statute states:

> **§ 6045. Disclosure of transmission and distribution utility costs**
>
> Upon request, a transmission and distribution utility, as defined in Title 35-A, section 102, shall provide free of charge to current or prospective customers, tenants or property owners residential electric energy consumption and cost information for a dwelling unit for the prior 12-month period or figures reflecting the highest and lowest electric energy consumption and cost for the previous 12 months. The cost must include and separately identify the cost of the transmission and distribution utility's services and the cost of electricity. If a unit has been occupied for a period of less than 12 months or for any other reasons the utility does not have information regarding electricity consumption or costs for a period of 12 months, the utility shall estimate the unit's annual kilowatt-hour consumption or cost. The estimated cost must be based on the applicable standard-offer service price or default service price established by the Public Utilities Commission. Provision of this information is neither a breach of customer confidentiality nor a guarantee or contract by the utility as to future consumption levels for or the cost of the provision of electricity to that unit. For purposes of this section, "dwelling unit" includes mobile homes, apartments, buildings or other structures used for human habitation.

In the NOI, the Commission sought comment on whether this statute needs to be modified to address privacy concerns related to smart meters and smart meter related

[34] In its reply comments, CMP stated that RESA's comments are beyond the scope of the issues the Legislature directed the Commission to review in this report which were limited to privacy and cyber security issues. The Commission agrees that the comments regarding data dissemination are beyond the scope of this report but notes that these issues may be addressed as part of the dynamic pricing proceedings or future rulemakings. RESA's comments about Chapter 322 of the Commission's rules, and whether customers should be able to authorize the release of their information by, for example, third party verified verbal consent or text messaging, are within the scope of the privacy issues examined in this report. These issues will also likely be explored in the dynamic pricing proceedings and any subsequent rulemaking proceedings.

equipment and specifically whether it should be modified to specify that the utility shall only provide monthly data and not time-of-use hourly data.

BHE commented that the statute should be modified in this way assuming the purpose of disclosing this information is to provide current or prospective customers, tenants or property owners with 12 month of electricity usage and cost trends at a specific location in order to assist them with planning and decision making related to electricity usage at this property. BHE also noted that sharing time-of-use hourly data would not be necessary to achieve this aim. CMP also supported the proposed statutory change noting that it has implemented the statute this way and believes this strikes the proper balance between the goals of providing usage information to current and prospective tenants and property owners and protecting against the disclosure of customer specific information.

C. Regulatory or Statutory Gaps Regarding Privacy Protection

Based on its review, the Commission does not find substantial regulatory gaps with respect to protecting customer information made available with smart meters. The current rule prohibits utilities from giving customer information, including usage information, to third parties without customer consent and BHE and CMP have internal processes for rule compliance. While the OPA raised concerns about privacy as it relates to third parties that may want access to customer information, it is premature to propose changes in this area until more is known about the type of dynamic pricing programs that will be offered to BHE and CMP customers and the specific information that would be useful to third party providers. Similarly, consideration of the issues RESA raised regarding efficient and cost-effective access to usage data and methods for customers' consent to the release of their information would also be premature. The Commission will consider these issues as the dynamic pricing options for utility customers becomes more defined through the current BHE and CMP dynamic pricing program proceedings and will initiate any rulemaking proceedings required to make changes to the Commission's rules based on the result of those proceedings.

The statute which governs disclosure of T&D utility residential electric energy consumption and cost information to current or prospective customers, tenants or property owners, 14 M.R.S.A. § 6045, was enacted prior to the development of smart meter technologies in Maine. As a result, the current statute could allow for utility disclosure of hourly or sub-hourly consumption data which may have privacy implications. The current absence of limitations on the type of usage data that may be provided pursuant to 14 M.R.S.A. § 6045 represents a statutory gap that may be considered by the Legislature.

V. RECOMMENDATIONS

While a number of efforts to improve cyber security protections are currently taking place at the federal level, the NERC Critical Infrastructure Protection standards and the standards being developed by NIST's Smart Grid Interoperability Panel and DOE's Cyber Security Initiative do not or may not apply to distribution level smart grid facilities. The Legislature may wish to consider legislation that would require Maine's T&D utilities to adopt NERC CIP standards applicable to the bulk transmission system for their smart meter and associated systems. If the NIST's Smart Grid Interoperability Panel and the DOE's Cyber

Security Initiative do result in mandated standards, these too could apply to smart meter and related systems.

The Commission suggests legislative consideration to amend 14 M.R.S.A. § 6045, which governs disclosure of T&D utility residential electric energy consumption and cost information to current or prospective customers, tenants or property owners, to require that the information provided is monthly, not hourly or sub-hourly. The Commission has attached draft legislation for the Legislature's consideration (See Appendix B).

Finally, the Commission recommends that issues related to customer information made available as part of CMP and BHE's smart meter-enabled dynamic pricing programs, including how third parties may seek access to customer information and for what purposes, data dissemination and customer consent methods, be explored further during the Commission's dynamic pricing proceedings and future rulemaking proceedings. The Commission will continue to evaluate what, if any, additional privacy protections or security measures may be necessary to protect the privacy of customer information as CMP and BHE's smart meter-enable dynamic pricing programs are developed.

Appendix A

RESOLVE Chapter 82, LD 756, 125th Maine State Legislature
Resolve, To Examine Cyber Security and Privacy Issues Relating to Smart Meters

Resolve, To Examine Cyber Security and Privacy Issues Relating to Smart Meters

Sec. 1 Examination of cyber security and privacy issues relating to smart meters. Resolved: That the Public Utilities Commission shall examine current cyber security and privacy requirements that exist under federal and state law, rules and utility policies and practices that apply to transmission and distribution utilities and identify potential regulatory gaps that may exist by examining the extent to which existing federal requirements may or may not apply to cyber security and privacy issues regarding smart meters and related systems. To the extent regulatory gaps exist, the commission shall develop recommendations to address them. As part of this examination, the commission also shall consider issues related to access to customer data and the disclosure of transmission and distribution utility residential electric energy consumption and cost information pursuant to the Maine Revised Statutes, Title 14, section 6045; and be it further

Sec. 2 Monitor federal cyber security initiative. Resolved: That the Public Utilities Commission shall actively monitor the efforts by the United States Department of Energy to launch a cyber security initiative to enhance cyber security on the electric grid with input from the Federal Energy Regulatory Commission, the United States Department of Homeland Security and publicly and privately owned utilities; and be it further

Sec. 3 Report. Resolved: That the Public Utilities Commission shall report the results of its examination and recommendations required pursuant to section 1 and the progress of the federal cyber security initiative as it applies to smart meters and related systems under section 2 to the Joint Standing Committee on Energy, Utilities and Technology by January 15, 2012. The Joint Standing Committee on Energy, Utilities and Technology may submit a bill to the Second Regular Session of the 125th Legislature based on the report.

HP0563, Signed on 2011-06-15 00:00:00.0 - First Regular Session - 125th Maine Legislature, page 19

Appendix B

An Act To Clarify Requirements Regarding Disclosure of Transmission and Distribution Consumption Information

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 14 M.R.S.A. § 6045, as amended by PL 2009, c. 657 § 6, is further amended to read:

Disclosure of transmission and distribution utility consumption and cost information

Upon request, a transmission and distribution utility, as defined in Title 35-A, section 102, shall provide free of charge to current or prospective customers, tenants or property owners residential electric energy consumption and cost information for a dwelling unit for the prior 12-month period or figures reflecting the highest and lowest electric energy consumption and cost for the previous 12 months. A transmission and distribution utility shall only provide monthly electric energy consumption data and shall not provide time-of-use or hourly or sub-hourly electric consumption data. The cost must include and separately identify the cost of the transmission and distribution utility's services and the cost of electricity. If a unit has been occupied for a period of less than 12 months or for any other reasons the utility does not have information regarding electricity consumption or costs for a period of 12 months, the utility shall estimate the unit's annual kilowatt-hour consumption or cost. The estimated cost must be based on the applicable standard-offer service price or default service price established by the Public Utilities Commission. Provision of this information is neither a breach of customer confidentiality nor a guarantee or contract by the utility as to future consumption levels for or the cost of the provision of electricity to that unit. For purposes of this section, "dwelling unit" includes mobile homes, apartments, buildings or other structures used for human habitation.