Seattle IT

AMI PRIVACY CONSIDERATIONS

Purpose

The AMI Program has completed two activities to identify potential privacy risks:

- An independent review by the law firm of Orrick, Herrington & Sutcliffe (Orrick), which reviewed the City's AMI Program through the lens of the City's Privacy Principles and identified potential risks that should be considered.
- Completion of the City's privacy review process, including a Privacy Impact Assessment (PIA). The PIA identified potential privacy risks and areas where the AMI Program could be strengthened to mitigate these risks and build public trust.

Below are the considerations raised by Orrick and the PIA, and suggested actions to mitigate potential privacy risk. The AMI Program should review the considerations and complete the column "Action Taken" to note how the consideration will be addressed by the program.

PIA Considerations

PIA Section	Statement	Suggested Action	Action Taken
8. Does the project/program follow the City records retention standard for the information it collects? Departments are responsible for ensuring information collected is only retained for the period required by law. City departments are further responsible for reviewing and auditing their compliance with this process. For more information, please see the internal retention schedule, here, and records retention ordinance, here.	Raw meter data and CEUD is maintained in compliance with applicable laws and regulations with respect to the collection, retention, and destruction. SCL's retention policy for CEUD information is compliant with FERC requirements. FERC requires CEUD be maintained six (6) years. Disposition practices and an audit process will be defined as part of project implementation.	Define and document practices for disposing of raw meter data and CEUD older than six years. Define and document practices for disposing of CEUD not needed for billing purposes, such as raw meter data.	Task is added to project plan and will be completed by June 30, 2017.

PIA Section	Statement	Suggested Action	Action Taken
9. Are there other departments or agencies with assigned roles and responsibilities regarding the information that is collected? Identify and list the name(s) of any departments or agencies with which the information is shared and how ownership and management of the data will be handled.	… Standard contractual language for service provider use of raw meter data and CEUD will be developed and memorandums of agreement will be implemented between City Light, SPU, and Seattle IT governing data use.	Develop contractual language limiting the use of raw meter data and CEUD - across the systems in which the data resides (e.g. HES, MDM, CCB). Include this language in MOAs with SPU and Seattle IT, and in contracts with third party service providers.	Will develop standard language and amend any existing MOA's/contracts that do not already specifically address the limited provision use by June 30, 2017.
14. How is data accuracy ensured? Explain how the project/program checks the accuracy of the information. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. If the project/program does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project/program.	… End-to-end automated data integrity checks will be configured and implemented.	Include end-to-end data quality and accuracy testing as part of the AMI Program project plan.	This is included in the project plan.
17. Is the system compliant with all appropriate City of Seattle and other appropriate regulations and requirements? Please provide details about reviews and other means of ensuring systems and project/program compliance.	The AMI Program will work with SCL Internal Audit and Seattle IT throughout the project design, implementation, and operation to better ensure effective and appropriate security and privacy provisions are in place.	Add to the AMI Program Project plan specific actions to support this statement, including: • Documenting roles and responsibilities of the teams involved in compliance related activities. • Developing of a privacy statement specific to raw meter data and CEUD. • Developing data handling procedures for raw meter data and CEUD. • Developing a policy and plan for the periodic review of energy data use. • Assessing the security of raw meter data and CEUD at rest and as it flows through the meter to cash process. • Validating that meters only collect and transmit the data elements necessary for relevant City processes – and match what is documented in the PIA.	This will be documented in two separate areas. The AMI Program has developed a charter establishing the AMI operations center whose responsibility will be to document the policies, processes and procedures for handling raw data and identify roles and responsibilities. Any policies, processes and procedures for CEUD will be amended and included in the MOA between SCL, SPU and ITD. This work will be completed by June 30, 2017.

PIA Section	Statement	Suggested Action	Action Taken
18. Has a system security plan been completed for the information system(s) supporting the project/program? Please provide details about how the information and system are secured against unauthorized access.	Landis+Gyr provided the City with a report on controls implemented to maintain the operating effectiveness of its systems. Entitled, "Report on Landis+Gyr Technology, Inc.'s Description of its Managed Services Operations System and on the Suitability of the Design and Operating Effectiveness of Its Controls", the report includes the opinion of an independent auditor that found controls were designed and implemented sufficiently to achieve the desired outcomes specified by L&G. City Light's contract with L&G requires the company to provide this report on a regular basis. The scope of the report is limited to the provider, and the scoping statement provided by the independent services auditor notes "certain control objectives specified in the [control's] description can be achieved only if complementary user entity controls contemplated in the design of Landis+Gyr Technology, Inc.'s controls are suitably designed and operating effectively, along with related controls at the service organization." As part of the AMI implementation program, City Light will implement requisite controls. A system security plan has not been developed for the systems that comprise City Light's AMI Program.	Develop a system security plan for the operation of the AMI Program systems, including HES, MDM, and CCB. Implement user entity controls implemented to complement the controls referenced in L&G's "Report on Landis+Gyr Technology, Inc.'s Description of its Managed Services Operations System and on the Suitability and Design and Operating Effectiveness of Its Controls."	Will document security protocols in place for the front end of HES, MDM and CCB as defined by the utilities risk and control group by June 30, 2017. Will document the backend security per internal standards established by ITD by June 30, 2017.
21. Have access controls been implemented and are audit logs regularly reviewed to ensure appropriate sharing outside of the department? Is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies? Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.	Refer to question 9 for information on agreements implemented with other departments and third parties for information sharing.	Develop and document a policy and procedure for reviewing and auditing use of systems that handle CEUD, including MDM and CCB.	Complete documentation by June 30, 2017

PIA Section	Statement	Suggested Action	Action Taken
22. How does the project/program ensure that the information is used in accordance with stated practices of the project/program? What auditing measures are in place to safeguard the information and policies that pertain to them? Explain whether the project/program conducts self-audits, third party audits or reviews.?	City Light Internal Audit periodically reviews the design and operating effectiveness of controls implemented to facilitate system use in accordance with security, privacy, legal, and regulatory commitments. As part of the AMI Program, the methodology for these reviews will be updated to include a review of controls intended to maintain proper use of raw meter data and CEUD.	Refer to PIA #17 and #21	Refer to PIA #17 and #21
23. Describe what privacy training is provided to users either generally or specifically relevant to the project/program. City of Seattle offers privacy and security training. Each project/program may offer training specific to the project/program, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to personal information are trained to handle it appropriately. Explain what controls are in place to ensure that users of the system have completed training relevant to the project/program.	Employees with access to systems containing raw meter data CEUD, including HES, MDM, and CCB are trained about appropriate use and handling of the data before receiving access to the systems. In addition, City of Seattle employees, including City Light, SPU, and Seattle IT employees complete annual privacy awareness training, which reinforces that data may only be used for the purpose stated in the notice and consent provided to customers at the time of data collection, if provided, and in accordance with the City's privacy statement and privacy principles.	Validate trainings address the proper handling of raw meter data and CEUD and considering developing a training specific to raw meter data and CEUD.	City Light Privacy Champion will develop and provide training on proper handling of raw meter data and CEUD by June 30, 2017.

Privacy Principles Considerations

Note: Orrick's assessment refers to two external references, the Department of Energy's Voluntary Code of Conduct for Data Privacy and the Smart Grid (VCC), and the National Institute of Standards and Technology Guidelines for Smart Grid Cybersecurity, Volume 2 (NIST Guidelines). Both the VCC and NIST Guidelines are non-binding sets of recommendations and best practices, but as they are specific to smart grid issues, they may be useful in informing how the City can meet its privacy principles in the AMI project.

Privacy Principle	Statement	Suggested Action	Action Taken
Principle #1: We value your privacy	**Determine what information is personal information.** For the information that will be collected and used in connection with the AMI metering project, consider which data elements should be considered personal information. In general, personal information includes any information that directly identifies an individual, or that relates to a specific individual. The VCC goes further and identifies two types of information that should be viewed as akin to personal information in the smart meter context. First, the VCC refers to "account data", which includes the following items, when identified to a specific customer: names, geographic subdivisions smaller than a state (e.g., address, city, zip code, or equivalent geo-codes), dates of service provided to a customer or information specific to identifying an individual's utility service, phone/fax numbers, e-mail addresses, utility account numbers, and device identifiers and serial numbers (including for meters). Second, it refers to "customer energy usage data" which is non-identifying information that reflects a customer's energy usage. Together, account data and customer energy usage data ("CEUD") are "customer data", which the VCC indicates should be viewed as private.	The City should consider treating account data as personal information, if it does not already. Further, per the VCC and RCW 42.56.330(2), the City should consider treating CEUD as personal information.	CEUD meets the definition of personal information used by the City's Privacy Program.
Principle #1: We value your privacy	**Verify data aggregation and anonymization is effective.** Whenever data is intended to be aggregated or anonymized, it is important to design the aggregation and anonymization processes in a way that is reasonably designed to prevent the information from being used to re-identify people. Upon implementation, data collected from meters and shared with Landis+Gyr is supposed to be anonymized data. We have not seen, and the City may not have been provided, with information on how the data is aggregated and/or anonymized. Privacy Benchmark: The VCC includes specific guidance for data aggregation, and for data anonymization.	Consider evaluating VCC guidelines to verify that the data collected from the meters and shared with Landis+Gyr is anonymized in a manner that meets the VCC recommendations. Other anonymized or aggregated data should be measured against the recommendations. Finally, consider such validation periodically to confirm that the manner of aggregating and anonymizing is still effective in light of technological developments that make it easier to re-identify forms of aggregated or anonymized information.	Will document as part of work being done establishing the AMI operations center.
Principle #1: We value your privacy	**Adopt employee training and designate responsibility.** Training and appointment of a responsible employee (e.g., a privacy champion) are necessary to fulfill the City's first privacy principle of protecting individual privacy. The NIST Guidelines call for employee training on privacy and security practices to protect CEUD. They also recommend appointing a person who will be responsible for verifying that appropriate privacy policies and practices are established and followed with respect to smart meter data.	Consider developing appropriate training to help City employees understand the privacy and security practices that are designed for the privacy and security of CEUD and other customer data. Also consider appointing an employee at City Light to have privacy practice oversight responsibilities.	Refer to PIA #23 for training plans. City Light has appointed a privacy champion who is responsible for the privacy related activities in in the department.

Privacy Principle	Statement	Suggested Action	Action Taken
Principle #1: We value your privacy	**Conduct periodic privacy assessments.** The NIST Guidelines call for privacy risks to be re-examined via periodic risk assessments, especially when there are significant changes in operations or practices with respect to the collection or use of data from an AMI system.	Consider creating a process to verify that changes in practices lead to privacy re-assessments.	Refer to PIA #17 and #21
Principle #2 – We collect and keep only what we need	**Limit data collected from the meters.** Privacy concerns arise not only from the information that particular data elements in isolation may reveal, but also from understanding what they reveal in combination with the other data elements that are at issue. Together, multiple data elements can be combined to identify particular individuals, even if the elements by themselves do not do so. Consideration should be given to determining whether City Light need all of the information that will be transmitted from the meters, and for any data elements that are not needed to deliver utility services, further consideration given to excluding from collection such elements. NIST Guidelines note that the risk of re-identification increases with technological innovation. Accordingly, in assessing what data elements are necessary to collect to provide service to customers, do not assume that an element that is not necessary can be safely collected anyway because it does not, by itself, identify particular individuals.	Minimize collection of elements that are not necessary/critical to provision of services.	Refer to PIA #8
Principle #2 – We collect and keep only what we need	**Limit retention of the data.** To fulfill the second Seattle privacy principle, data that is no longer needed for the purpose it was collected (e.g., to provide and bill for energy services) should be securely deleted. The VCC recommends retaining customer information and information collected from meters only as long as it is needed to fulfill the purpose for which it was collected.	If some of the data collected from particular meters needs to be retained for a longer period than all of the data that was collected, evaluate whether it will be feasible to delete the data elements that are no longer needed, or to de-identify or anonymize the data. For example, if energy consumption data needs to be maintained and shared with City Light teams that are not involved in directly servicing particular meters or delivering services to particular residences or buildings, consider whether it is feasible to maintain and share that data in a de-identified or aggregated format (including, for example, without items that could identify or relate to particular meters or locations, such as the Premise ID, ESIID, Meter ID, or any other equipment or location identifiers).	Policy and procedure will be developed as part of the work effort developing the AMI operations center, and will be completed by June 30, 3017.

Privacy Principle	Statement	Suggested Action	Action Taken
Principle #2 – We collect and keep only what we need	**Consider frequency of data collection.** The more frequently data is collected, the more it can reveal about what is happening inside a home—such as when people are awake, when they are asleep, and when they are out of the house. The NIST Guidelines call attention to this concern, and note that equipment electricity signatures and time patterns that reveal when particular devices are used are detectible when data is collected more frequently. Accordingly, the NIST Guidelines recommend using larger time intervals for collecting AMI data to help prevent against recognition of such signatures and patterns.	Balance should be struck between the frequency of transmitting data and the need for granular data to provide utility services. The City should keep these considerations in mind when determining how frequently energy usage data is collected, and strive to transmit data only as frequently as need to deliver the relevant services.	Refer to PIA #8
Principle #2 – We collect and keep only what we need	**Validate data collection from meters.** Collection of additional data elements can raise additional privacy risks. The NIST Guidelines recommend collecting only the data that is needed to fulfill the purpose for which data is collected	To help fulfill the City's second privacy principle, consider conducing a validation assessment of the meters to verify that they are only collecting and transmitting only the data elements that the City intends to obtain. Also, consider verifying that the meters do not collect or transmit information that identifies particular devices, such as by transmitting serial numbers, MAC addresses, or other device-identifying information when individuals charge smart appliances/vehicles at their home, or when they use home area networks. If the configuration of the meters to set what data they transmit is a responsibility of Landis+Gyr , the agreement with Landis+Gyr should specify that obligation.	Refer to PIA #17

Privacy Principle	Statement	Suggested Action	Action Taken
Principle #3 - How we use your information	**Give notice of privacy practices:** Evaluate how the City will notify individuals of the types of information that will be collected, and how it will be used. Transparency to customers is the first core principle in the VCC, which declares that understandable notices about privacy-related policies and practices should be provided at the start of service, on a reoccurring basis thereafter (e.g., annually), and at the customer's request. The VCC also states that notice should be given whenever there is a substantial change in practices or procedures that might impact customer data. The VCC recommends that notice of privacy practices should: • Detail the types of information that are being collected, and include a commitment to collect only the information needed to provide the service; • Explain how customer data is used, including (i) how account data is collected; (ii) how CEUD is collected (e.g., via meters); (iii) an overview of the purposes for which it is collected; (iv) how individual customer data will be used; and (v) whether aggregate or anonymized data will be created, and if so, how it will be used or shared; • Disclose how the customer can access, identify inaccuracies, and request correction of, customer data; • Explain when customer data will be shared without prior consent, including describing the types of third parties/service providers used to provide energy services and the other supporting services/legally-mandated third parties information must be shared with, and disclosing the purpose of the sharing; • Describe how consent will be requested, and how it can be revoked, before customer data is shared with a third party for a purpose other than providing service to the customer; • Describe how the customer data will be protected; • Indicate that customer data will be retained and disposed of pursuant to applicable law and policy; • Include an effective date, contact information, and a summary of changes from prior versions along with instructions for how to obtain prior versions; and • Include any customer-specific obligations and expectations (e.g., giving accurate data, notifying of changes in account data, etc.). The items above parallel typical concepts that are included in privacy policies, though they are specific to the smart meter context. The City should consider including those items in a privacy notice for the AMI meter program, and should evaluate how the privacy notice will be made available to citizens.	Perform the action recommended in the statement.	Refer to PIA #17

Privacy Principle	Statement	Suggested Action	Action Taken
Principle #3 - How we use your information	**Obtain consent for new uses:** Provide privacy notices and obtain consent. The VCC recommends that when customer data will be used for purposes other than to provide a customer with customer-initiated service or other reasonably expected uses, customer consent should be obtained first. The VCC includes detailed guidance about when and how these consent options should be provided to the customer, and the information that they should include. The VCC also recommends that consent be freely revocable.	If the City plans any uses of customer data—or will share customer with third parties who will make uses of customer data—other than as necessary to provide energy services to customers, the City should consider whether consents should be (re)obtained, and what disclosures should be provided.	Refer to PIA #12

Privacy Principle	Statement	Suggested Action	Action Taken
Principle #4 - We are accountable	**Evaluate security of meters and AMI system.** The security of AMI meter information in its collection, transmission, and storage, should be examined. The PWC report on Landis+Gyr 's managed services operations controls in 2015 sheds some light on the information security practices at Landis+Gyr , but that report also indicates that Landis+Gyr 's customers must implement particular security controls for the Landis+Gyr controls to operate properly. The report also indicates that controls that are specific to individual Landis+Gyr customers were not reviewed. The City may want to review the complimentary user entity controls on pages 35-36 of the PWC report (especially Control Objectives 4, 5, 8-10) and verify that the City will address them. Consider conducting an initial and periodic assessment—either internally (if the city has the appropriate expertise and resources) or through use of a third party—of both the meters and the metering system infrastructure to verify that appropriate security controls are in place and that there are no security gaps. **Review security of data transmissions.** In addition to the aspects of the AMI system that Landis+Gyr will be responsible for, the City should consider conducting an assessment of the security controls for the other system aspects that will involve collection, transmission, or storage of data from the AMI meters. For example, the NIST Guidelines note that wireless transmission of smart meter raises additional privacy and security risks, and it calls for controls to protect the data transmissions from inappropriate use. The City mentioned that the data transmitted wirelessly by the wireless carrier network will be encrypted, but it may want to assess whether the manner and level of encrypting the data is sufficient and effective. **Assess cybersecurity program.** The fourth principle in the VCC addresses integrity and security of customer data. It calls for a cybersecurity risk management program that: (i) identifies, analyzes, and mitigates cybersecurity risks for customer data; (ii) implements and maintains security controls to protect against unauthorized access, use, or disclosure; (iii) includes a comprehensive cybersecurity incident response program; and (iv) timely provides notice to customers when customer data is compromised in a cybersecurity incident. The NIST Guidelines also call for periodic audits, ideally conducted by independent third parties, of the security and privacy practices that an AMI system involves. To better meet the fourth City privacy principle, the City may want to review and revise its existing cybersecurity program to verify that the data that it is appropriate for the data that the AMI system will collect and process, and to include periodic audits of practices to verify that the privacy and security controls are working properly.	Perform the action recommended in the statement.	Refer to PIA #17 and #18

Privacy Principle	Statement	Suggested Action	Action Taken
Principle #5 - How we share your information	**Contract for privacy protections.** The City may want to require Landis+Gyr to comply with the City's privacy principles, or with requirements that are equivalent to the City's privacy principles, in the contract with Landis+Gyr. In addition, if any other third party vendor or service provider will obtain meter information or personal information, agreements with those third parties should also be reviewed for compliance with the privacy principles. **Limit third party collection of personal information.** While the City's fifth privacy principle does not expressly require it, it may be a good idea to verify what information Landis+Gyr (or any other service provider involved in the AMI solution) will receive. For example, in our discussion it was noted that Landis+Gyr would receive meter identifiers and latitude and longitude coordinates. If the location data is not essential for Landis+Gyr to provide the services, consider withholding that information from Landis+Gyr. **Obtain consent for sharing with third parties.** The NIST Guidelines recommend obtaining customer authorization before sharing CEUD with third parties. If the City plans to share meter information or customer information such as CEUD with third parties for purposes other than assisting with providing energy service to customers, the City should consider obtaining customer consent before doing so.	Perform the action recommended in the statement.	Refer to PIA #9, 10, 11, and 12
Principle #6 - Accuracy is important	**Provide customer data access.** The VCC and NIST Guidelines both call for customers to have access to their own customer data, and for customers to have the ability to participate in how the data is maintained. The VCC indicates that access should be convenient, timely and cost-effective, and should also allow the customer to identify potential inaccuracies and request correction of them. The City may want to consider how it will verify that data in the AMI system is accurate and up to date. In addition, it should consider whether allowing individual access to the data would be feasible and helpful in building trust and helping to meet the City's sixth privacy principle.	Perform the action recommended in the statement.	Refer to PIA #15