Foundation Working Group
Draft Framework for Third Party Access

The purpose of this document is to facilitate the development of a framework that would support providing access to electricity data to third parties (the "Framework"). This Framework may be used to support future projects to implement such access rights and to provide guidance to the IESO or other entities that might be interested in providing data to third parties. This Framework assumes that all data is handled in accordance with relevant privacy legislation.

There is a spectrum of potential types of 3rd party access to data. For the purpose of this Framework, we have identified four scenarios:

1. Standard reports downloadable from a public website by any 3rd party (public)
2. Access requests for de-identified electricity consumption data, alone or matched with other data sets, that are fulfilled by the holder of the electricity data (the "Data Custodian") and available to authorized 3rd parties
3. Access requests for personal electricity consumption data, alone or matched with other data sets, that are fulfilled by the Data Custodian and available to authorized 3rd parties
4. Access requests fulfilled by the Data Custodian through an access portal or interface for use by authorized 3rd parties.

1. Downloadable Standard Reports from a Public Web-site

Standard reports derived from the MDMR could be created and made available on the IESO's website for download by any 3rd party. These reports would contain only de-identified data. This would be similar in concept to the electricity system data currently available on the IESO website: http://reports.ieso.ca/public/RealtimeMktPrice/PUB_RealtimeMktPrice.xml

The terms and conditions of use governing 3rd party access to this type of data may be similar to those already contained on the IESO website: http://www.ieso.ca/Pages/Terms-of-Use.aspx

Questions:
- What, if any, standard reports from the MDMR might be of interest to 3rd parties?
- Should there be any additional limits on access to de-identified standard reports (other than those contained in the website terms of use)?

2. De-Identified Data Requests That Are Fulfilled By The Data Custodian

This category would be for custom requests for de-identified electricity data, either on its own or paired with other data sets, and fulfilled by the Data Custodian. The results would be delivered to the requesting party via an agreed upon delivery channel. This could include the requester providing the Data Custodian with additional data sets to match with the electricity data and de-identify. The requestor will not have direct access to the source system of the data nor would they have access to personally identifiable information. The terms and conditions of use governing 3rd party access to this type of data could include provisions governing some of the same situations contemplated by the website terms of use noted above. However, these situations contemplate a customer agreement containing their own terms and conditions, as well as basic rules of access including:

1) Requestor goes through a registration process authorizing them to submit requests. If seeking data matching, the requestor and request must comply with data access rules for the other data sets.
2) Submitted requests must provide the following information:
   a) Specific data being requested
   b) Intended use of the information
   c) Other data sets the requested data is to be matched with and at what level of granularity the data is to be matched
   d) Analysis required to be performed by the Data Custodian.

3) A request fulfillment assessment process would consider the following constraints and prioritization criteria:
   a) Current volume of requests to be serviced
   b) Complexity and amount of requested information
   c) Availability of resources (systems and personnel) and associated costs
   d) Use of the information
   e) Deadlines, directives, regulations involved
   f) Organization requesting information.

4) Requesting organization must demonstrate and/or agree to certain terms and conditions, which may include the following:
   a) Cost structure for services
   b) Payment terms for services
   c) Ability for the Data Custodian to require the requestor to be subjected to an independent audit and provide evidence to the Data Custodian to demonstrate the design and operating effectiveness of their security and privacy controls
   d) Requestor has in place effective controls to protect the security and privacy of data that meet or exceed the control requirements of Data Custodian.

5) Data must be de-identified following an appropriate de-identification process (see presentation material entitled: Principles and high level Process Requirements for De-

Identification) prior to being delivered to the requestor.

Questions:
- Can any 3rd party request de-identified data? If there are to be restrictions, what are the criteria for determining eligibility to receive the data?
- What priority criteria should be used in a fulfillment assessment process?
- What, if any, cost structures might be considered?

Personal Information Requests that are Fulfilled by the Data Custodian

This category focuses on access to personally identifiable electricity information, on its own or paired with another data set. Electricity consumption data that is connected with an address is considered personally identifiable electricity information. The access framework may be similar to that noted for de-identified data, however, additional criteria would be expected regarding who can access the data, for what purpose, as well as control requirements over the security and privacy of data.

Questions:
- What use cases involve the use of personal information?
- What organizations, if any, should have access to personal information? For what purposes?
- Are there protections, beyond those noted above, that need to be in place when dealing with personal information?

Data Access Requests fulfilled using a Portal or Interface for use by Authorized 3rd Parties

The broadest data access to 3rd parties would be allowing them to retrieve or access data from the Data Custodian using a portal or interface. In addition to all the terms and conditions of use contained in the above types of access, we would also need to consider the following processes, rules and requirements:

- Submit an application to be qualified to directly connect to the portal or interface.
- Comply with the registration, connectivity and authentication processes and tests for direct access to the portal or interface by each qualified organization and its individual users.
- Agree to the timely notification and removal of individual users' access privileges to the portal or interfaces in accordance with the established processes and procedures of the Data Custodian.

Questions:

- Should personal information be provided through such a portal/interface? If so, what additional precautions, if any, need to be put in place?
- What organizations, if any, should have access to the portal or interface? For what purposes (use)?