MANUAL

Market Manual 6: Participant Technical Reference Manual

Participant Technical Reference Manual

Issue 39.1

The "PTRM" provides the technical details for hardware and software that a participant in the electricity market may need to interface with the IESO

Disclaimer

The posting of documents on this Web site is done for the convenience of *market participants* and other interested visitors to the *IESO* website. Please be advised that, while the *IESO* attempts to have all posted documents conform to the original, changes can result from the original, including changes resulting from the programs used to format the documents for posting on the website as well as from the programs used by the viewer to download and read the documents. The *IESO* makes no representation or warranty, express or implied, that the documents on this website are exact reproductions of the original documents listed. In addition, the documents and information posted on this website are subject to change. The *IESO* may revise, withdraw or make final these materials at any time at its sole discretion without further notice. It is solely your responsibility to ensure that you are using up-to-date documents and information.

This document may contain a summary of a particular *market rule*. Where provided, the summary has been used because of the length of the *market rule* itself. The reader should be aware, however, that where a *market rule* is applicable, the obligation that needs to be met is as stated in the *market rules*. To the extent of any discrepancy or inconsistency between the provisions of a particular *market rule* and the summary, the provision of the *market rule* shall govern.

Document ID	IMO_MAN_0024
Document Name	Participant Technical Reference Manual
Issue	Issue 39.1
Reason for Issue	Issued for Baseline 51.0.
Effective Date	January 5, 2024

Document Change History

For change history prior to Issue 10, see issue 17.0 of the Participant Technical Reference Manual.
For change history prior to Issue 22.0, see issue 29.0 of the Participant Technical Reference Manual.
For change history prior to Issue 30.0, see issue 33.0 of the Participant Technical Reference Manual.

Issue	***Reason for Issue***	**Date**
30.0	Issued for Baseline 35.0 in regard of need for Participants to include use of Windows 7 and IE 11.0, update java policy file and location, update hardware requirements and update of web based applications.	March 2, 2016
31.0	Issued for baseline 36.0 for revisions due to replacement of Reliability Compliance Tool with a functionally equivalent application in the Online IESO system.	September 14, 2016
32.0	Issued for baseline 37.0 for revisions due to refreshment of Market Information Management system.	December 16, 2016
33.0	Issued for baseline 38.1 for revision due to Market Information Management system IDK decommission. Revised Dispatch Information section to add information related to Dispatch Service system.	December 6, 2017
34.0	Issued for Baseline 41.0 regarding the removal of the need for a Java Runtime Environment (JRE) and java policy file for multiple file upload capability for the Portal.	March 6, 2019
35.0	Issued in advance of Baseline 42.1 for revisions made to Online IESO to enable the *transitional capacity auction*.	October 15, 2019
36.0	Issued for Baseline 43.1.	June 3, 2020
37.0	Updated to meet accessibility requirements pursuant to the *Accessibility for Ontarians with Disabilities Act*.	November 2, 2020
38.0	Issued in advance of Baseline 45.0. Updated to include electricity storage participation.	February 26, 2021
39.0	Issued in advance of Baseline 46.0. Updated to remove references and content regarding the IESO Portal and add content regarding the IESO Gateway.	September 15, 2021
39.1	Issued for Baseline 51.0. Updated to fix broken link for the Dispatch Service Client User Guide.	January 5, 2024

Related Documents

Document ID	Document Title
MDP_RUL_0002	Market Rules

Table of Contents

List of Figures

List of Tables

Table of Changes

Reference (Section and Paragraph)	Description of Change
Section 2	Removed all references and content for Portal where applicable and added references and content for IESO Gateway
Section 2	Removed all references and content to Internet Explorer browser where applicable and added references and content for Microsoft Edge browser
Section 5	Removed all reference for Portal where applicable and added references for IESO Gateway. Updated content for Market facing applications

Market Manuals

The *market manuals* consolidate the market procedures and associated forms, standards, and policies that define certain elements relating to the operation of the *IESO-administered markets*. Market procedures provide more detailed descriptions of the requirements for various activities than is specified in the "Market Rules MDP_RUL_0002*"*. Where there is a discrepancy between the requirements in a document within a *market manual* and the "Market Rules", the "Market Rules*"* shall prevail. Standards and policies appended to, or referenced in, these procedures provide a supporting framework.

Conventions

The *market manual* standard conventions are defined in the "Market Manual Overview" document

– End of Section –

1. Overview

1.1 About this Manual

The "Participant Technical Reference Manual" is comprised of the following sections:

Section	Name of Section
1.0	Overview
2.0	Participant Workstation, Network and Security
3.0	Dispatch Information
4.0	Operational Metering Equipment and AGC
5.0	Market Applications

The content of each is described more fully later in this section.

1.2 Purpose

This "Participant Technical Reference Manual" provides the potential and active market participants, program participants and/or service providers (collectively referred to in this document as participants) with the necessary general technical standards to participate in the *IESO*-administered markets. It also provides references to other documents and information sources for detailed technical specifications required for participating in the *IESO*-administered markets. This document is not intended to be used as a stand-alone technical reference manual for all issues within the realm of electricity production, distribution, or consumption.

Written for participants, it provides only information relevant to the participant for communicating with the *IESO* and participating in the electricity market. It provides more detailed information on the requirements stated in the "Market Rules MDP_RUL_0002".

It is intended as a generic guide and the relevance of information in certain sections will depend on the market requirements of the participant. Participants are expected to understand what information they will require for their particular role in the market and apply the required sections accordingly.

1.3 Scope

This document is intended to provide participants with a description of the various facilities and interfaces they require to participate in the *IESO*-administered markets.

This document supplements the *market rules*. It also points to other documents and information sources that provide installation, set-up, and configuration information for the various tools and facilities required for participation in the electricity market as a supplier, *transmitter*, *distributor*, *generator*, *electricity storage participant*, or *consumer*.

The material contained in various sections of the "Participant Technical Reference Manual" is limited to information that is relatively stable and not subject to frequent change. Technical details that are subject to change, on a more frequent basis, are posted on the Technical Interfaces page of *IESO*'s

Web site at the link https://www.ieso.ca. It is therefore important for participants to refer to the specific technical documents on the Technical Interfaces page when reviewing the requirements outlined in the "Participant Technical Reference Manual". Specific document references are included in each of the relevant sections of the "Participant Technical Reference Manual" as well as in the References table at the rear of the document.

1.3.1 Out of Scope

Technical requirements for revenue metering are not contained within the "Participant Technical Reference Manual". Details for *revenue meter* requirements are contained in "Market Manual 3: Metering" which is available on *IESO*'s Web site.

1.4 Limitations

The information in this document is limited to the information available at the time of publication. It is subject to change as the various technical interfaces and/or market requirements evolve.

The information in this document is based on the *market rules* provided to the IESO by the *Minister* of Energy, Science and Technology dated April 15, 1999 and subsequent updates thereof. Future changes in the "Market Rules MDP_RUL_0002" may result in changes in this document. No warranty is provided that any participant's requirements have been completely or correctly interpreted or that all issues have been identified.

The "Participant Technical Reference Manual" is only a technical specification manual and does not provide any procedural information. For procedural details please refer to the relevant user manual and/or guide.

1.5 Who Should Use This Manual

The "Participant Technical Reference Manual" is meant for all those who wish to participate in the *IESO*-administered market. These include, but are not limited to, the *generators*, *distributors*, *wholesale sellers*, *wholesale consumers*, *retailers*, *transmitters*, *electricity storage participants*, and the "financial market" participants.

The "Participant Technical Reference Manual" provides the participants with the technical details and specifications of the hardware and software as well as other security-related information required by participants for interfacing and information exchange with the *IESO*.

1.6 Conventions

The standard conventions followed for *market manuals* are as follows:

- The word 'shall' denotes a mandatory requirement;
- Terms and acronyms used in this *market manual* including all Parts thereto that are italicized have the meanings ascribed thereto in Chapter 11 of the "Market Rules MDP_RUL_0002";
- Double quotation marks are used to indicate titles of legislation, publications, forms and other documents;
- Any procedure-specific convention(s) shall be identified within the procedure document itself.

1.7 How This Manual is Organized

This document is organized by specific areas of interest and not by *market participant* roles. It is the responsibility of participants to know what components are relevant.

The "Participant Technical Reference Manual" is divided into several parts based on specific areas of interest. A brief description and summary of each part is provided below:

- Section 1.0 - Overview: Contains information about the purpose, scope, limitations and structure of the manual.
- Section 2.0 - Participant Workstation, Network and Security: This section contains the minimum technical specifications for the *participant workstation* required by participants making *bids* or *offers* or obtaining information about market activity. The minimum hardware and software specifications for the participant network used for interacting with the *IESO* are also described. This part also provides participants with information and technical specifications for the digital certificates. The participants require the digital certificates or User ID account, identity credentials for purposes of data confidentiality and security.
- Section 3.0 - Dispatch Information: This part contains information about the technical requirement of the *dispatch workstation* and general information about dispatch message exchange. The primary audiences for this part are those participants who will be providing electrical power into or withdrawing electric *energy* from the *IESO-controlled grid* and will receive dispatch instructions from the *IESO*. It includes as well information on the functional aspects of the Dispatch Message Exchange as well as the message structures & actions. Minimum hardware and software specifications for the real time network required for acquiring real time data, dispatch of *automatic generation control* ("*AGC*") and dispatch messaging are also provided besides general information on voice communication specifications and types.
- Section 4.0 - Operational Metering Equipment & AGC: This part details information and technical specifications for the operational metering requirements. It does not contain information on *revenue meter*ing which is provided in the "Market Manual 3: Metering" on the *IESO*'s Web site. It also provides technical specifications for the *AGC* Operational Remote Terminal Units (RTUs).
- Section 5.0 -Market Applications: Provides technical specifications & requirements for the bidding application, *settlement* application, invoicing and application interfaces (MIM API). For viewing templates, validation tables and sample data files please refer to the Technical Interfaces page of *IESO*'s Web site.

The technical specification and requirements contained in the Sections of this Manual are authorized under "Appendix 2.2 of the *market rules*". Specific references, where applicable, will be included at the beginning of each section.

– End of Section –

2. Participant Workstation, Network and Security

(For supporting rule references, please refer to "Appendix 2.2, Section 1.4 of the *market rules*.)

2.1 Participant Workstation

A *participant workstation* is any participant client computer or server that communicates with or conducts transactions with the *IESO* systems. Any data or information exchanged with *IESO* systems is considered a communication. Any communication that is used to submit or retrieve data or information in regards to the wholesale electricity markets for the purpose of conducting business shall be considered a transaction.

2.1.1 Hardware Requirements

Platform

The client software provided by the *IESO* is designed to be platform independent. The IESO has performed extensive testing of this software on the Windows 10 operating systems. Displays may be rendered incorrectly if a Windows Operating System is not used. Other operating systems and hardware may be used as long as the operating system supports the Oracle Java Runtime Environment 7.0 where applicable. At this time there are no known issues with the IESO Gateway and the supported browsers.

For Windows 10 and above it is recommended that the client workstation hardware conform to Microsoft's specifications which can be found by searching the Microsoft Web site for Windows 10 system requirements.

Going forward the *IESO* recommends at least the following:

Processor

The minimum recommended processor is an Intel I5.

Memory

The minimum recommended system requirements are 4 GB of internal RAM.

Disk

The recommended available disk space is a minimum of 15 gigabytes on a typical 128 GB hard drive.

Interface Cards

A minimum of a DSL or Cable connection for high speed internet access is strongly recommended if the participant is interfacing with the *IESO* over the public Internet.

If connecting to the *IESO* through an internal network over the web, then the appropriate participant network equipment will be required.

Monitor

The minimum supported monitor must be XVGA with a resolution capability of 1024 x 768 pixels but using an FHD level monitor of 1920 x 1080 pixels would better serve the needs of the workstation for wholesale market use.

Printer

It is recommended that a printer where required for printing market application output should have resolution of at least 600 dpi and supports multiple fonts.

2.1.2 Software Requirements

Operating System

The recommended operating system is Windows 10 as shown on the *IESO* Supported Client Platform web page at the link http://www.ieso.ca/en/Sector-Participants/Supported-Client-Platforms .

Previous versions of Windows are no longer supported by the *IESO*. The operating system must have support for the TCP/IP protocol.

It should be noted that the participants use Windows 10 as a minimum.

Note: When Windows is used as the operating system, the preferred Short Date format is yyyy/mm/dd. Other Short Date formats may be used provided the year placement is set to yyyy. Go to the Control Panel Regional Settings to make this adjustment. The delivery dates used by the Internet Explorer browser in the submission of *bids* are generated from this date setting and value.

Browser

All *IESO* applications within the MPI are fully tested with the *IESO* supported OS /Browser and JRE combinations where applicable. Only browsers listed on the *IESO* Supported Client Platform should be used.

256-bit encryption or higher is required with the supported browser. Make sure if needed that the browser used is configured for

a. TLS 1.2 or higher as well as the *IESO* secure websites have been configured to work with TLS 1.2 or higher which requires this level of encryption.

The viewing resolution must be 1024 x 788 pixels or higher in view maximized mode.

The supported browsers have been tested with the IESO Gateway and Online *IESO* Systems. It will function as expected with the supported Microsoft OS, and browser combinations

Firewall

It is recommended that each participant ensure that each *participant workstation* is protected by an appropriate firewall for the network and workstations being used. The choice of the technology to be employed is up to the participant.

IESO Confidential Report Site

The production URL for the confidential report repository HTTPS site is available from the Web site link: https://reports.ieso.ca/private/. The sandbox URL for the confidential report repository HTTPS site is available from the Web site link: http://reports-sandbox.ieso.ca/.

The new reports site offers the following access methods:

- New web user interface for browser-based access.
- Secure File Transfer Protocol (SFTP) for machine access.

- RESTful API for machine access.
- Query available reports using a URL request.
- API returns output as XML or JSON.
- No dependency on UI – reliable and direct access to reports.

An explanation of the access interfaces for the new confidential report site can be found in the *IESO* Reports API Guide This can be found at the following location on the IESO corporate website: www.ieso.ca › Files › IESO › api-reports-guide › IESO_Reports_API_Guide

IESO Gateway System for Access to most Market Facing Applications

The *IESO* Gateway is the new Okta based secure web based system used for authentication and access to market applications accessible to participants. This includes:

- EMI – Energy Market Interface for bid and offers
- OCSS – CROW Outage Management System
- Dispatch Service
- Transmission Rights Auction.
- Prudential Manager.
- IESO Workspaces (formerly Watchdox) which will now host all previous Portal Collaboration communities (e.g. as MACD-*TFE* Technical Exceptions, *Emergency* Preparedness, SOE LDC Extranet, Market Surveillance Panel, RT-GCG Cost Recovery Framework, etc., for secure document submission and retrieval etc.)

- The Online IESO system securely hosts a number of market applications. This includes but is not limited to:
    - Registration - for *market participants*, contacts and user accounts.
    - Metering Installation Registration.
    - *Facility*/Equipment Registration.
    - *Meter* Trouble Reporting application.
    - Notice of Disagreement application.
    - Capacity Auction application.
    - *Demand Response* application.
    - Reliability Compliance application
    - Settlements forms

For the supported versions of the browsers to work properly with the IESO Gateway, there are no special configuration settings that need to be made except for the previous Internet Explorer browser.

Where Internet Explorer is still being used, the previous version of this Participant Technical Reference Manual should be referenced for recommended browser settings

Microsoft Edge and Google Chrome, being more mature modern browsers, are configured out of box to be setup for security correctly. The end user can choose to manage some settings but it mostly can be left as is.

If needed, IT administrators can look after any special configuration parameters.

Microsoft Edge –– Security

Very few security configuration settings need to be made for proper functioning of the browser with various *IESO* web sites.

1. Under the Settings menu select Privacy, search and services option See Figure 2-1 (Microsoft Edge / Windows 10 shown).

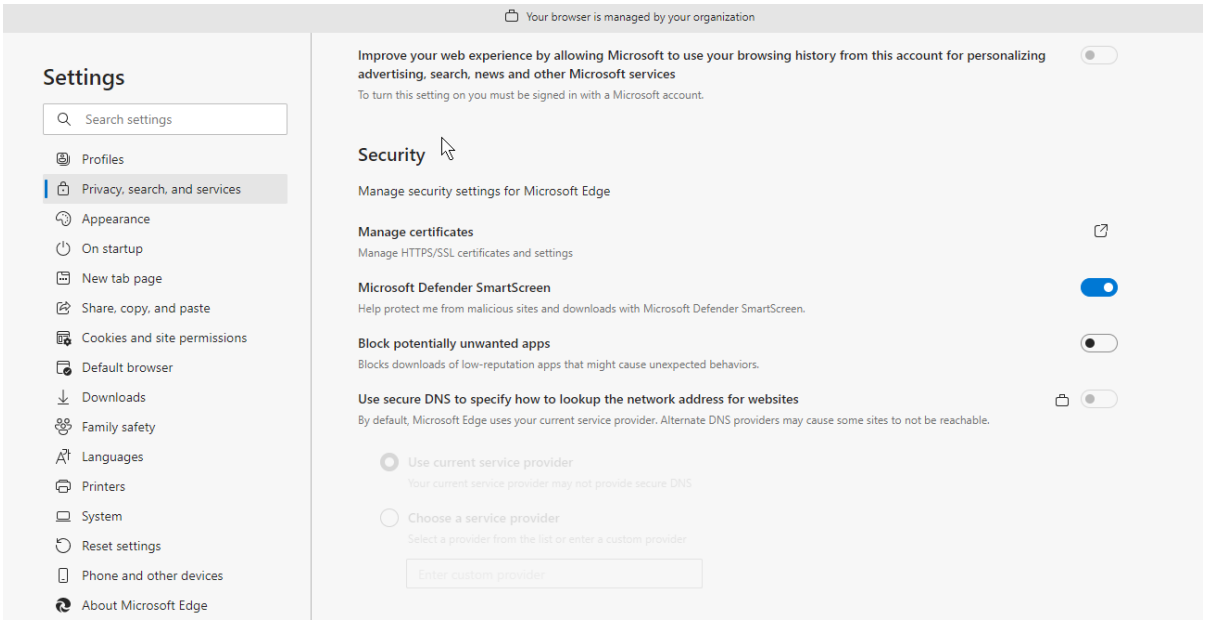

Figure 2-1: Microsoft Edge – Security – Windows 10

2. Modify as required for optimal and secure operation of Microsoft Edge.

Edge Pop-up Blocker

The Microsoft Edge pop-up blocker functionality may have some beneficial and some detrimental effects depending on the needs of the browser user. When enabled with just default settings, the Edge pop-up blocker may impact the functionality of the Energy Market Interface. It is recommended that Edge configuration settings for pop-up blocking be set so that Energy Market Interface functionality is not affected.

The directions included here apply to Windows 10 and Microsoft Edge.

Microsoft Edge Turn Pop-up Blocker On or Off

In order to turn off (or on) the IE pop-up blocker function, do the following:

1. Under the Settings menu selection select the Cookies and site permissions menu option.
2. A submenu list will display. Scroll down to the Pop-ups and redirects selection. Turn off or on the Block function. See Figure 2-9.

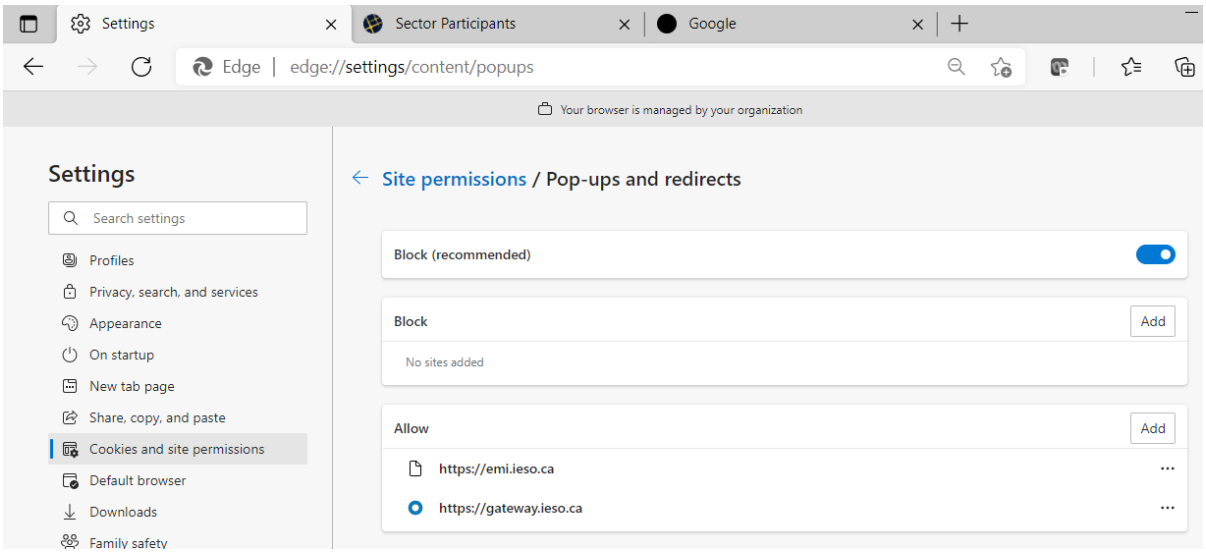

Figure 2-2: Microsoft Edge, Pop-up Blocker

Microsoft Edge Configure Pop-up Blocker Settings

In order to access pop-up blocker settings and set up the pop-up blocker filter parameters to allow the proper functioning of Energy Market Interface and IESO Gateway, the following needs to be done:

1. Under the Settings menu, select the Cookies and site permissions menu option.

A submenu list will display.

2. Scroll down to the Pop-ups and redirects selection. Use the Add button to add the URL for the Energy Market Interface to the Allow list. Enter in the URL addresses of the Sandbox and Production EMI and Gateway sites in the addresses (production example shown in Figure 2-2). This will allow the proper functioning of Energy Market Application.

Secure Connection to IESO Web Sites

When connected to any secure IESO web site, the certificate used by the site can be inspected for validity. Here is the IESO EMI web site example.

1. Use the right mouse button on the “padlock” icon next to the EMI website URL address. A dropdown menu list will display as shown in Figure 2.3.
2. Click on the Connection is Secure option to show the website has a valid certificate as shown in Figure 2.4.
3. Click on the certificate icon at the top to display the Certificate Information popup window to inspect the IESO certificate information and details to validate its certificate as shown in Figure 2.5.

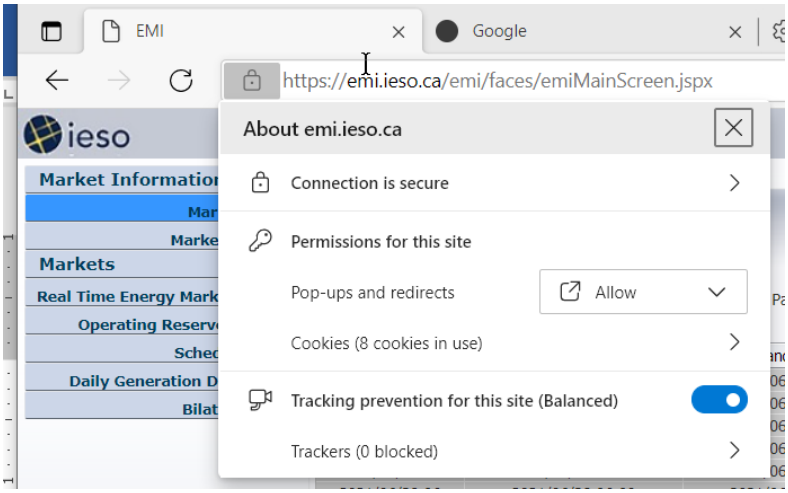

Figure 2-3: Microsoft Edge - Web Site Certificate Inspection 1

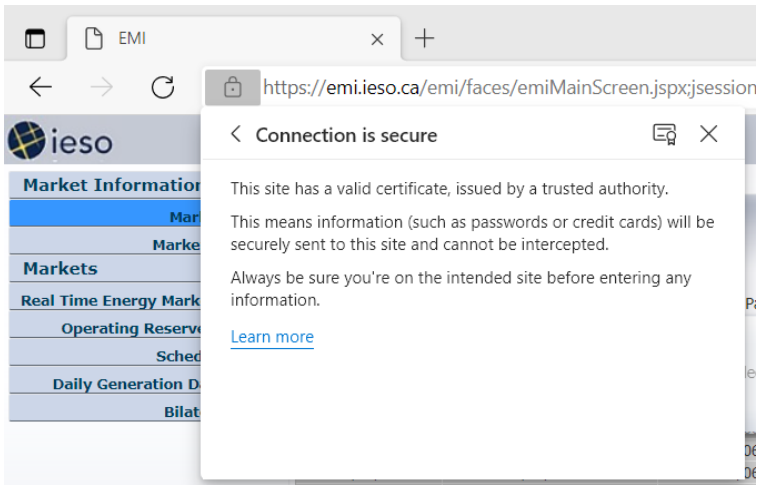

Figure 2-4: Microsoft Edge - Web Site Certificate Inspection 2

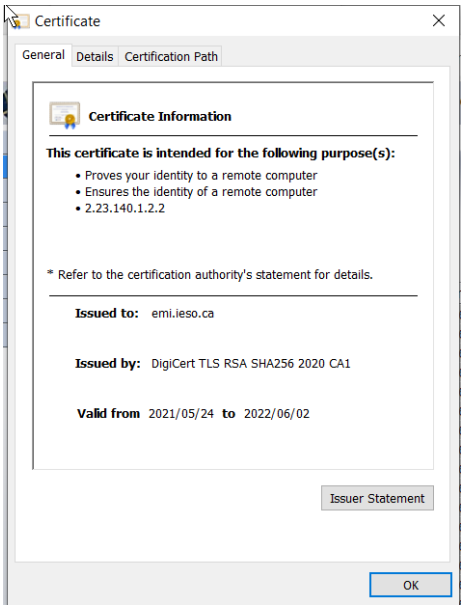

Figure 2-5: Microsoft Edge - Web Site Certificate Inspection 3

Internet Connection

For participants planning to connect to the *IESO* through the public Internet, the participant must have an established Internet connection. This may be in the form of either a high speed link to an ISP (Internet Service Provider) or through an internal Web-gate or proxy server. The speed of this Internet connection will directly affect application performance.

2.2 Participant Network

Participants will submit *bids*/*offers*, access market, *settlements*, and metering information through the use of the *IESO* participant network.

There are three methods for a participant to connect to the *IESO*. These are defined as PUBLIC over the Internet or as PRIVATE through a facility contracted by the participant with a telecommunications service provider.

Regardless of the method chosen, failure of the telecommunications network can occur. Participants should take this into consideration and establish alternate paths or contingency plans, as required.

2.2.1 Internet

The connectivity bandwidth should be at least 1024Kbps but higher speeds are recommended to maintain optimal performance.

Participants will access the *IESO* using *IESO* supplied authentication credentials which are subject to the limitations and conditions defined in the “Market Rules MDP_RUL_0002”. To authenticate to any of the secure IESO Web sites the participant will present an IESO authentication credential (e.g. to the IESO Gateway or IESO Reports site or other secure *IESO* Web site). If the presented IESO authentication credential is valid, the user will be granted access to the site and authorized applications. Participants must register for IESO authentication credentials. Registration will be

performed as specified in the Identity Management Operations Guide via the Online IESO system (see Technical Interfaces page of *IESO*'s Web site).

Secure Sockets Layer (SSL) is used to encrypt the messages between the client system at the participant and a secure Web Server at the *IESO*. SSL uses a combination of asymmetric (public and private keys) and symmetric keys (shared secret) to negotiate the secure session between the participant system and the *IESO* Web Servers. This is a standard technology developed originally by Netscape and used extensively by Internet web servers to establish secure connections between two systems.

2.2.2 Private Network

The Private Network option is recommended to participants concerned about having direct control over the performance of telecommunications with the *IESO* for commercial purposes. As the name implies, the participant privately arranges this service with a commercial telecommunications service provider. The quality of service is subject to the contract between the participant and the service provider. All associated costs will be borne by the participant.

The *IESO* enables this option, by permitting the telecommunications service provider to establish a point of presence at the IESO's main and backup operating centers. The *IESO* also will provide space and a physically and electrically secure environment for the premises equipment.

Participant is expected to terminate its point-of-presence at the *IESO*'s premises with routers, supplied by the participant, located at the *IESO*'s main and backup operating centers. The actual demarcation point is the Ethernet connection to the router. The participant is solely responsible for the management of its telecommunications facilities.

In the interest of manageability, a list of preferred telecommunications service providers has been established. These are listed below. As the list may be revised periodically, it is recommended that the participant check the latest version of this document. Also, the *IESO* is prepared to review on a case-by-case basis if the participant prefers a telecommunications service provider not in the list.

The current list of preferred telecommunications carriers consists of the following:

Bell Canada, Hydro One Telecommunications, Rogers Communications and Zayo.

2.2.3 Shared Network

The Multiprotocol Label Switching (MPLS) network will be maintained through the service provider with *IESO* having responsibility for connectivity up to the router/security device located on the participant site. Static routing will be used across the interfaces between *IESO* and the participant's network

The participant will work the *IESO* to define a satisfactory internal IP or registered external public IP Ethernet address for the Ethernet port that connects to the participant's internal network.

To arrange for a shared network connection, contact the *IESO* (see the *IESO* Web site at www.IESO.ca).

Connecting to the Supplied Ethernet Port

A network connection will need to be established between an Ethernet Port on the router/security device and the participant's Internal Network.

If distance between the Ethernet Port on the router/security device and the participant's Internal Network is an issue, then a recommended solution will be to deploy an Ethernet Repeater or "Ethernet Extender."

Participant Firewall Configuration

Web based network communications will be secured using SSL. Depending on the participant's internal network configuration, changes may have to be made to allow a SSL connection if firewalls are used.

Changes to the participant's firewall configuration will be dependent upon the type of firewall in use. For standard and encrypted web traffic, TCP Ports 80 and, 443 will need to be open.

2.3 Accounts / Identity Credentials

The *Market Rule* amendment (MR-00376) binds all participants in regard to authenticated communication or transactions when using *IESO* accounts and identity credentials.

The *market rules* require that the *IESO* implement access control protocols to protect the unauthorized disclosure of confidential information transmitted by electronic communications. The use of User ID account and strong password identity credentials in combination with SSL encryption allows the *IESO* to fulfill the appropriate market rules governing confidentiality. Additionally, User ID account identity credentials in conjunction with SSL protocols and adaptive authentication software mechanisms can be used to establish authentication, authorization and integrity.

User ID account identity credentials used with the *IESO* Gateway, Confidential Reports site and Online IESO system are authenticated and managed for identity management and Single Sign on by a combination of commercial products from Oracle and Microsoft.

2.3.1 Account Suspension and Auditing

IESO Gateway/Online IESO accounts used for accessing the IESO Gateway, Online IESO and secure Confidential Reports site will be subject to a number of security provisions. These include:

- IESO Gateway/Online IESO Passwords must conform to the construction rules as described in the Identity Management Operations Guide.
- If a user enters an incorrect password a specified number of times in a row on the IESO Gateway, the account will be locked out for a fixed period of time after which the user may attempt login again.
- If a user enters an incorrect password five times in a row on the IESO Report site, the account will be locked out for a fixed period of time after which the user may attempt login again.
- If the user is attempting login to the IESO Gateway from an unrecognized prior location or computer or is attempting login during a time of day that does not match a pattern of recognized use, additional multifactor authentication options or a security question will be presented. The question choice and their corresponding answer shall have been provided by each user at time of account registration and initial IESO Gateway account activation.
- In accordant with *Market Rule* amendment (MR-00376), if the user fails to answer any additional authentication question correctly the account will be immediately locked out for a fixed period of time after which the user may attempt login again.
- All login attempts successful or not will be logged for analysis by the *IESO*.
- All IESO Gateway/Online IESO activity, login, logout and pages visited etc. will be logged for analysis by the *IESO*.

2.3.2 Identity Management

IESO Access Management, with the implementation of the Registration System handle all internal *IESO* management aspects of the Identity Management processes and coordinate their efforts with

both participants and internal staff. Access to the *IESO* secure web servers requires the use of User ID account identity credentials for authentication and authorization except for IESO Workspaces FIT and MicroFIT applications which use email based accounts.

Participant Rights Administrators look after all participant internal management aspects of the Identity Management processes using the Online IESO Registration application to communicate with the *IESO*.

Administration activities for User ID account identity credentials include:

- Registration
- Participant Approval
- User Account Creation and system access privileges assignment
- User Account Revocation and removal of system access privileges
- Change of system access privileges

Individual Subscriber refers to a person at the participant or agent of such. Application Subscriber refers to an application at the participant or agent of such. Either can be referred to as Credential Subscribers. Participant Rights Administrators who request User ID account identity credentials for themselves shall be considered Individual Subscribers when dealing with their own User ID account identity credentials. Under the *IESO* Trust Model each Individual Subscriber, Application Subscriber should be identified using the participant's internal policies and procedures (see "Identity Management Operations Guide" which is available on the Technical Interfaces page of IESO's Web site):

User ID account password reset is handled by email and direct communication with *IESO* Customer Relations.

IESO Access Management is responsible for issuing and maintaining email based account identity credentials for IESO Workspaces.

2.3.3 Energy Market Application

Energy Market Interface (EMI)

All participants must use the EMI via the *IESO* supported browser. The supported browser is listed on the "*IESO* Supported Client Platform" web page located on the *IESO* Corporate web site at: Supported Client Platforms (ieso.ca) .

All participants must register their EMI User account with the *IESO*, and assign applicable MIM contact roles and permissions using the Online IESO tool.

Participants can download the "Identity Management Operations Guide" and the "Submitting, Revising and Cancelling *Bids*/*Offers*/Schedules and Forecasts" (See the Technical Interface Page by clicking on this link Technical Interfaces (ieso.ca) and the Training Page by clicking on this link Training Materials (ieso.ca) on the *IESO*'s Web site) for instructions on EMI interface use.

MIM Programmatic API Application (Application Based Solution

Participants can choose to use the MIM programmatic API solution with a participant custom application.

All participants must register their API accounts with the *IESO*, and assign the applicable MIM system access role and permissions using the Online IESO tool.

In addition to the API account, the participant must register the IP addresses of the systems used to access the *IESO* MOSMIM Web Server with the *IESO* in order for the appropriate firewall rules to be implemented at the *IESO* to permit participant access with the MIM programmatic API.

The API account and IP address registration are required for both MIM production and sandbox environments to enable access to the *bid* site through the *IESO* firewall. Participants must manage their API accounts and IP addresses using the production and sandbox online *IESO* tool respectively.

When a participant uses the MIM programmatic API Application to access the *IESO* Web Server MOSMIM, a SSL (Secure Socket Layer) is session is started. Participants with firewalls must have the SSL port 443 open for communication with the *IESO* Web Server.

The MIM API is XML based Web Services. Its Web Services Client Tool (MWT), WSDL and XSD file can be downloaded from the *IESO* Web site (see the Technical Interfaces Page of IESO's Web site).

The USERID used for authentication with the MIM Web Services is the REGISTRATION User Login Name only.

2.3.4 Gateway/Online IESO/Confidential Reports and Identity Management System

All Gateway/Online IESO/Confidential Reports users log in with a User ID account credential for all Gateway and Online IESO hosted applications and the Confidential Reports site excluding IESO Workspaces and IESO FIT and MicroFIT user who use email based accounts

The IESO Gateway and Online IESO is protected by Okta and Microsoft identity management technologies. These components provide for single-sign-on, authentication, authorization, auditing and in conjunction with SSL protocols, confidentiality and integrity of communications. The Confidential Reports site is protected by the Okta and Microsoft supplied technologies.

All IESO Gateway, Online IESO and Confidential Reports identity management components for User ID account credentials are server based and only a web browser is required by the participant, as specified in this document, to access each system with this type of identity credential.

The "IESO Gateway User Guide" should be referenced for account activation, login and password reset procedures. The "IESO Reports API Guide" should be referenced for secure access to the Confidential Reports site. This can be found at the following location on the IESO corporate website: www.ieso.ca › Files › IESO › api-reports-guide › IESO_Reports_API_Guide.

2.3.5 Requirements for Browser Software Compatibility

Workstation Platform for IESO Gateway and Online IESO Browser Client

The browser client recommended by the IESO Gateway vendor (Okta), Online IESO system vendor (Appian) supported by the IESO is as shown on the "IESO Supported Client Platform" web page.

Recommended by the Gateway vendor but not supported by the *IESO* is:

- Mozilla Firefox - current version
- Safari - current version
- Google Chrome - current version

Any of these will work.

Ports

Port 443 must be open to allow access over SSL (Secure Socket Layer). Participants with firewalls must have this port open for communication with the *IESO* systems.

Other Documentation

The relevant IESO OCSS, Dispatch Workstation and MIM programmatic API manuals should be referred to when appropriate.

2.3.6 Operating Microsoft Edge in Internet Explorer Mode

Microsoft Edge can be operated in Internet Explorer mode to let a user access older web applications that do not work fully in Microsoft Edge.

To do so you must go to settings after starting Edge and under the "Default browser" section; choose to "allow sites to be reloaded in Internet Explorer mode" and add the web site URL to the list of sites for Internet Explorer mode pages. In this case the IESO Portal website is an example

Then restart the Edge browser and navigate to the specified URL. Note the time limit on this in the settings. It is assumed Microsoft does this as a security mitigation.

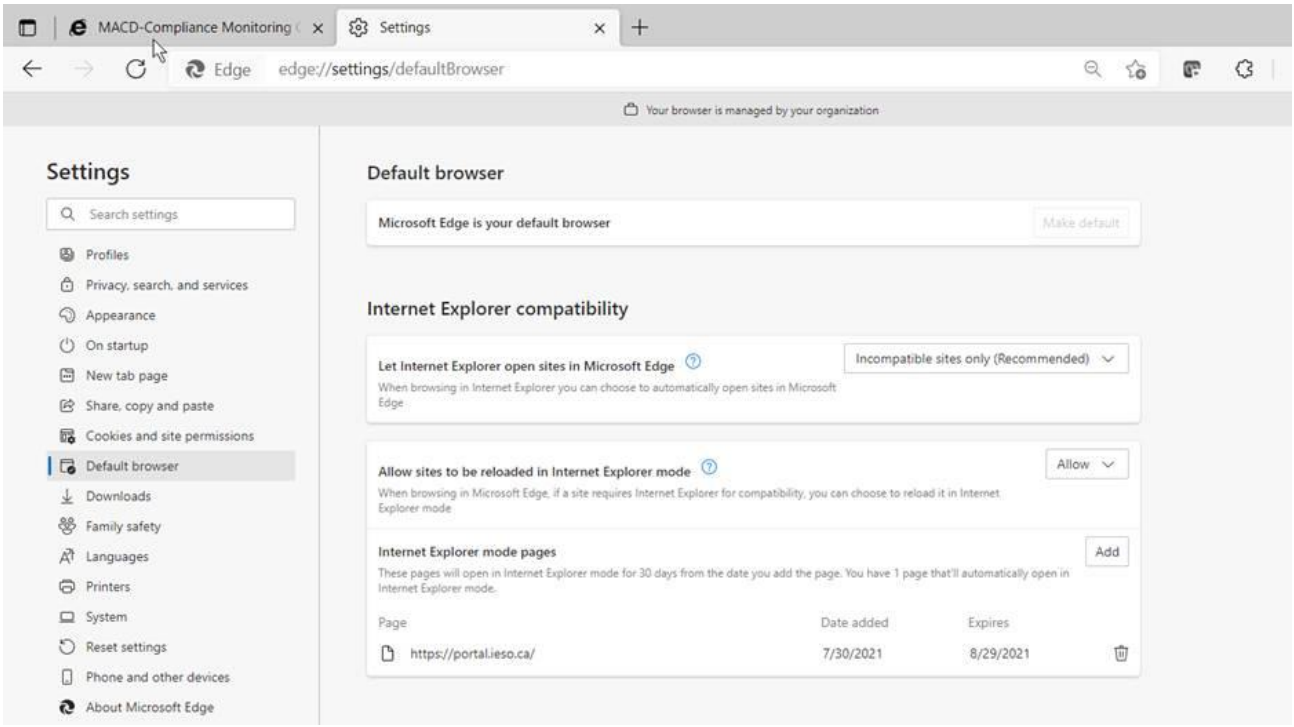

Figure 2-6: Microsoft Edge – Internet Explorer Compatibility Configuration

After navigating to the specified web site the end user must first use the right triple dot menu selection and choose to "Reload in Internet Explorer mode".

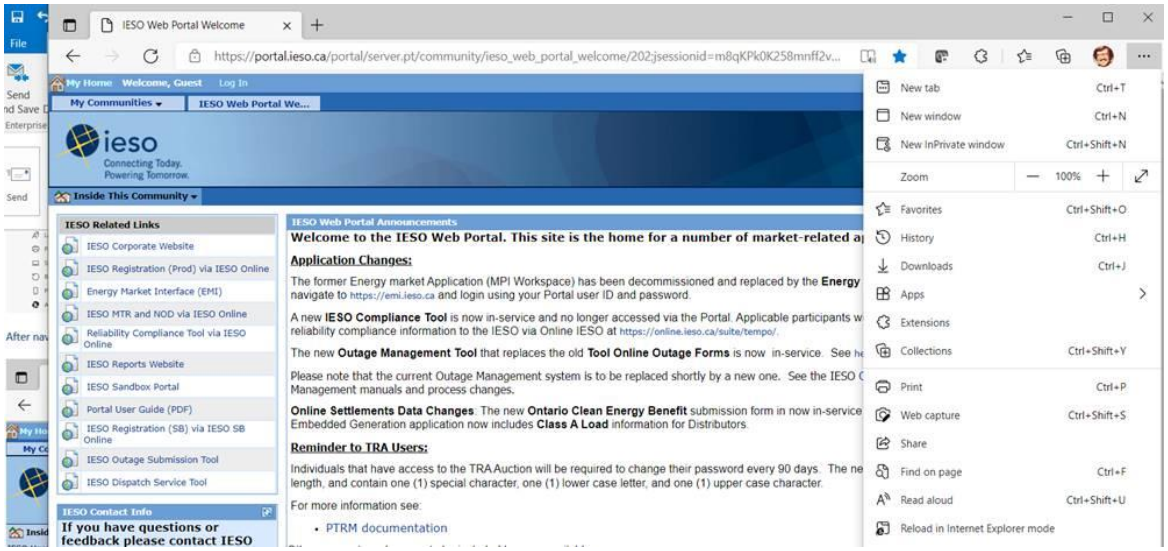

Figure 2-7: Microsoft Edge – Reloading website in Internet Explorer Mode

The browser will then display a popup window as shown below. Turn on the toggle to open the page in Internet Explorer next time and click on “Done”

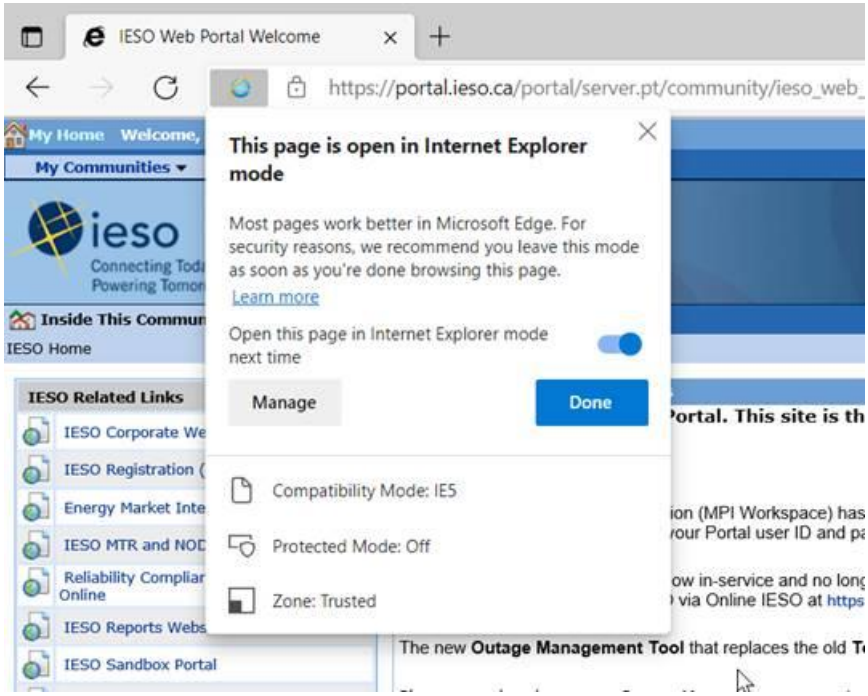

Figure 2-8: Microsoft Edge – Completing Reload of website in Internet Explorer Mode

Then the Edge browser will show at the top you are Internet Explorer mode and you can login. Notice it is still in https mode.

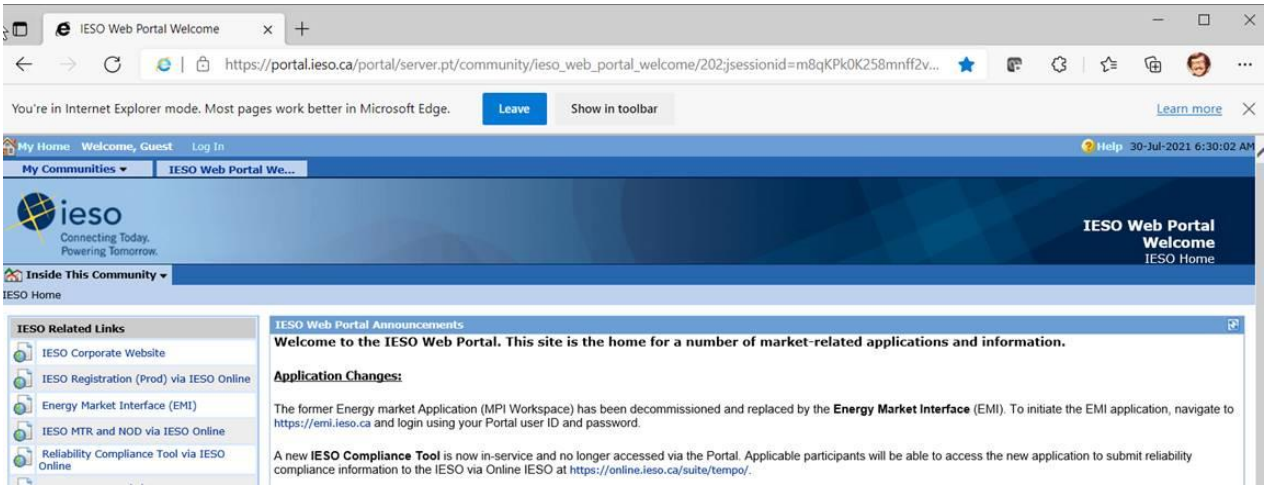

Figure 2-9: Microsoft Edge – Banner Showing Internet Explorer Mode is On

After which the tabs and drop down menus will work in Edge for the specified web site. (e.g. Portal)

– End of Section –

3. Dispatch Information

(For supporting rule references, please refer to "Appendix 2.2, Sections 1.1 & 1.3 of the market rules".)

3.1 Dispatch Service

3.1.1 Overview

Dispatch Service system allows Participants to retrieve and accept/reject *dispatch* instructions as well as easily search current and historical *dispatch* instructions, up to 60 days in the past, with the ability to sort and filter the data based on multiple criteria.

Dispatch Service system uses web/internet based communication (HTTPS protocol).

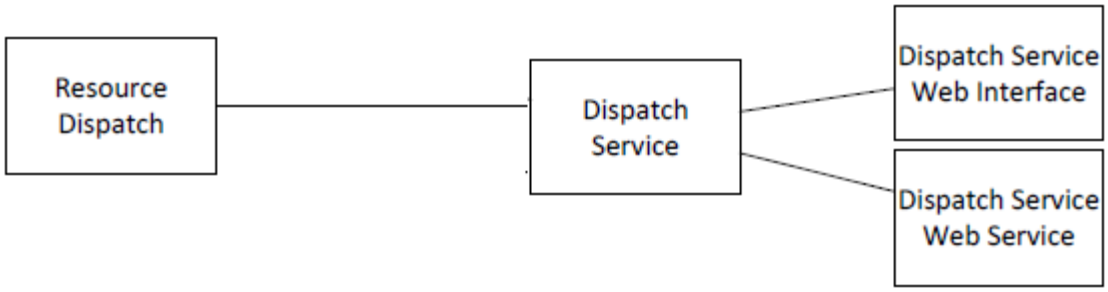

Figure 3-1: Overview of Dispatch Service System

3.1.2 Dispatch Service Web User Interface

Dispatch Service system has a web user interface which allows *Market Participants* to view and accept/reject *dispatch instructions* as well as easily search current and historical dispatch instructions, up to 60 days in the past, with the ability to sort and filter the data based on multiple criteria. "Dispatch Service Client User Guide" available by clicking this link to the *IESO* Web site (https://www.ieso.ca/-/media/Files/IESO/Document-Library/training/web-based-dispatch-service-market-participants-guide.ashx) describes the web user interface in detail.

3.1.3 Hardware and Software Requirement – Web User Interface

Refer to Section 2.1 "Participant Workstation" for hardware and software requirements.

3.1.4 Dispatch Service Web Service

Dispatch Service web service consists of a set of operations through which users retrieve and respond to *dispatch instructions*. *Market Participants* need to integrate the web service into their own systems. The "Dispatch Service Web Service Design Specification", available by clicking this link to the *IESO*

Web site (http://www.ieso.ca/sector-participants/technical-interfaces), contains detailed description of Web Service request, response, and error messages.

3.1.5 Hardware and Software Requirement – Web Service

Refer to Section 2.1 "Participant Workstation" for Hardware and software requirements.

3.1.6 Dispatch Notification Service

In addition to the Dispatch Service web service through which *dispatch workstations* retrieve *dispatch instructions*, *dispatch* messages can be pushed to Participants' server if *Market Participants* host a Dispatch Notification Service. Dispatch notification service is described in "Dispatch Notification Web Service Design Specification" document available through this link to the IESO Technical Interfaces web page (http://www.ieso.ca/sector-participants/technical-interfaces).

3.1.7 Hardware and Software Requirement – Dispatch Notification Service

Refer to Section 2.1 "Participant Workstation" for Hardware and software requirements.

3.2 Voice Communication Specifications

Voice communications are broken into two categories:

1. Normal-priority path participants; and
2. High-priority path participants.

The determination for whether a participant requires a High Priority path is defined in the "Market Rules MDP_RUL_0002, Appendix 2.2". Regardless of the status of the participant, all calls will be 'caller identified' and handled through confidential links between sites. All calls involving *IESO* operations will be recorded by the *IESO* and must be responded to as set out in the *market rules*.

In either category, voice communications between the *IESO* and participants is critical for reliable and secure operations of the high-voltage electrical grid and is required by the "Market Rules MDP_RUL_0002, Chapter 5, Section 12.2".

The *IESO* uses MSAT telephone services. MSAT satellite telephone service is considered to be a High Priority path in that it does not use the Public Switched Telephone Network to complete calls between MSAT callers. It is therefore capable of providing an independent communication function between the *IESO* and new participants. Other satellite telephone services are not considered because they require Public Switched Telephone Network links to either complete a call or to interconnect with *IESO* MSAT communications.

3.2.1 Normal-Priority PATH

A normal priority path will be of a type and capacity that allows unblocked communication with the *IESO*. This will be the primary path used during the normal conduct of business between a participant and the *IESO*. It may consist of a dedicated telephone number on the Public Switched Telephone Network (PSTN) to be used by the IESO only or an extension of a private network or Virtual Private Network (VPN) from either party. This path may involve connection to an IESO approved or administered network. Whatever mode is used this circuit will:

a. provide inherent privacy for the users with the ability to add other parties by invitation only;

b. interface with the *IESO* through the normally available PSTN facilities. Where available, caller identification will be available on this line. Such a *facility* shall be exempt from restriction by Line Load Control and/or have Priority Access for Dialing status; and
c. not be routed by the participant into an answering machine or Voice Mail that impedes or delays an immediate interactive conversation with a live person in attendance at the *facility*.

3.2.2 High-Priority PATH

A High Priority circuit will be of a type that provides backup communication between facilities. It must be 'hardened' against failure due to loss of commercial power at any point (MSAT Synchronous satellite communication facilities may be considered as 'hardened' facilities but are not desired as primary operating facilities due to the delay time involved in conversing over the link). In addition to the normal priority path requirements these facilities will:

a. continue to operate for a minimum of eight hours after the loss of commercial power at any point;
b. be protected against loss of service that may result from overload of the common carrier's public facilities; and
c. be a circuit with physically diverse path from the Normal Priority path to eliminate any common point of failure.

An 'auto-ringdown' circuit and other similar dedicated facilities may be considered as High Priority and 'hardened' depending on location.

Connection to an *IESO* approved, administered, or operated network may also be considered acceptable as a High Priority path. The MSAT network is a presently approved network. Other satellite networks are not approved due to reliance on PSTN connectivity being required to either complete a call or to interconnect with MSAT telephones.

All conversations between a participant and the *IESO* are confidential and will ordinarily connect only the two concerned parties. Other parties may join the conversation by invitation only.

The *IESO* will record all calls involving *IESO* operations. For all other cases, if a participant desires call recording, it is the responsibility of that participant to record the call.

3.2.3 Security

All communications between the *IESO* and the participant are considered confidential and therefore it is recommended that unencrypted radio frequency transmitters, such as cellular phones and other wireless technologies, not be used for communications.

3.2.4 Diverse Path

A diverse path will not use either the same physical path or equipment between sites. This does not include the end user devices.

– End of Section –

4. Operational Metering Equipment and AGC

(For supporting rule references, please refer to "Appendix 2.2, Section 1.2 of the *market rules*")

4.1 Operational Metering Equipment

4.1.1 Introduction

This section covers operational metering requirements. It does not cover specific *revenue meter*ing requirements.

Real-time operational information from participants is required by the *IESO* for the operation of the high voltage electricity system. Participants provide this information by using appropriate monitoring equipment that they supply. The information is sent to the *IESO* over *IESO* provided Real Time Network.

Specifics for the types of monitoring equipment required by the *IESO* are detailed in the "Market Rules MDP_RUL_0002, Chapter 4". The requirements in terms of quantities measured and performance for operational metering are mainly based on the *facility* ratings.

Remote real-time data can be provided to the *IESO* by the participants using two standard data transfer protocols:

a. Distributed Network Protocol (DNP), and/or
b. Inter Control Center Protocol (ICCP).

4.1.2 Qualified Devices

The standard device for collecting real-time information is the Remote Terminal Unit (RTU). Real-time information about the disposition of the participants' *facility* is collected from the participant supplied RTU's and forwarded on a regular basis to the *IESO* Control Center. The Energy Management System (EMS) at the *IESO* Control Center polls the RTUs for information every two to four seconds. Total data latency must not exceed four seconds.

The EMS communicates with the RTUs using the DNP 3.0 protocol. The Binary Input Data are: Object 1, Qualifier 01, Variation 1 (normal) and Variation 2 (not normal). The Analog Input Data are: Object 30, Qualifier 01, Variation 4 (normal) and Variation 2 (not normal) with Application Confirm Request. All data must show Data Quality Flags when not normal, such as Off Line, Restart, Communication Lost, Local/Remote Forced, Over-range. If data are derived from some intermediate devices, these flags must indicate any manual manipulation or failure of these data in these devices. Pseudo data do not require any Data Quality Flags.

DNP (Distributed Network Protocol) is an open, standards-based protocol used in the electric utility industry to address interoperability between substation computers, RTUs, IEDs (Intelligent Electronic Devices) and master stations. This protocol is based on the standards of the International Electrotechnical Commission (IEC). DNP 3.0 is the recommended practice by the IEEE C.2 Task Force for RTU to IED communications.

The document "DNP 3.0 Subset Definitions" is available to DNP User Group members at the DNP User Group Web site (click this link for the DNP web site http://www.dnp.org). This document will help DNP implementers to identify protocol elements that should be implemented.

If the participant wishes to use more than one *meter* at a location for the transmission of real-time data to the *IESO*, the *IESO* requires that the data be combined to one data concentrator such as an RTU so that only one telecommunications connection is required. The data from a failed meter or device must show the Offline and Communication Lost Flags.

If ICCP (Inter Control Center Protocol) is used for real-time data transfer to the *IESO*, the participants will provide their own ICCP server and software or optionally use a third party's ICCP server and software. Co-ordination with the IESO is necessary to establish the communication link between the participant and the IESO Control Centers.

The overall requirements for *reliability* and performance of the monitoring and control equipment are specified in Chapter 4 of the "Market Rules MD_RUL_0002".

4.1.3 Field Instrumentation Standards

The field instrumentation standard focuses on overall accuracy of the measurements being reported to the *IESO*. The accuracy requirement is for an overall end-to-end measurement error no greater than two percent of full scale.

This measurement error is the sum of all the errors in the measurement chain. Typically, the measurement chain is comprised of:

a. primary conversion by potential and/or current transformers;
b. secondary conversion by transducers; and
c. report by the RTU.

Any load *meter* reading must accurately reflect the quantity being measured regardless of load balance across the phases. For generation, a minimum of 2 metering elements is required.

As a guideline to the participants, the anticipated errors in the measurement chain described above are:

a. Primary conversion 0.5% of full scale
b. Secondary conversion (transducers) 0.5% of full scale
c. Report by the RTU, comprising analogue to digital conversion by the RTU and quantification errors 1.0% of full scale

The above accuracy standards are expected to be met by all new installations. However, for existing installations, the existing instrumentation transformers and burdens will be accepted by the *IESO*, for the life of the instrumentation transformers, except where their accuracy is insufficient for monitoring quantities that affect the system limits of the *IESO* controlled electricity network. It is up to the participant to ascertain with the *IESO*, during *facility* registration, whether the accuracy of their instrumentation transformers would have such impact.

4.1.4 Data Specifications

The specific data that needs to be made available to the *IESO* depends not only on the electrical capacity of the participant facility and its participation in the market, but also on other factors that influence the safe operation of the *IESO-controlled grid*. The detailed requirements are available in Chapter 4 and associated Appendices of the "Market Rules MDP_RUL_0002" and through consultation with the *IESO*.

In a generic sense, the data monitored falls into two classes – analogue and status.

Analogue Points

These are continuously varying measurements such as watts, volts and amps. Typically, the measurements are derived from a primary conversion device such as potential or current transformer and a transducer. This measurement chain scales down the actual electrical value that the RTU can report, for example, 0 to 100 MW to an analogue representation of 4 to 20 mA or 0 to 1 mA. Participants may contact the *IESO* for more detailed information.

Status Points

Status points are typically discreet, binary values such as the open or closed status of a switch. This information is presented to the RTU by a contact whose state is representative of the state of the device being monitored. Participants should check the RTU vendors' literature for available options in status monitoring.

4.1.5 Power Supply Specification

As the data received from the RTU is an integral piece to the operation of the electricity grid, the RTU and associated communications equipment requires connection to a secure source of power. Therefore, the RTUs must be powered from an industrial grade uninterruptible Power Supply (UPS) or from continuously charged batteries. In case of a power failure, sufficient battery capacity must be provided to permit ongoing operation of the RTU for a minimum of eight hours.

The RTUs must be operated in an environment of Minus 40 Degrees Celsius to Plus 80 Degrees Celsius and 95% non-condensing relative humidity.

4.1.6 Communications Specification

The RTUs can communicate with the *IESO* using either a serial port (operating in the range of 4.8 to 19.2 kbps) or an Ethernet port (10 Mbps) using IP. Please check with the *IESO* at the time of your installation. Ethernet (IP) connections must comply with the specifications outlined by the DNP Users Group in the document entitled, "Transporting DNP3 over Local and Wide Area Networks." The communications port will be connected to the Real Time Network supplied by the IESO located at the participant's facilities.

For the *IESO* supplied telecommunications equipment, the acceptable environment is Zero Degrees Celsius to Plus 40 Degrees Celsius and 5%to 90% non-condensing relative humidity.

4.1.7 RTU Site Certification

The certification of an RTU site is composed of the following activities:

a. Field Instrumentation Accuracy Audit;
b. Environment Audit;
c. Telecommunications connection; and
d. RTU Check-In Service.

Upon the successful completion of the site certification process by the *IESO*, the RTU Site is certified as acceptable for market use. Each of the above certification activities is described in more detail below.

Field Instrumentation Accuracy Audit, which is the verification of all the errors in the measurement chain, may be required by the *IESO*. The participant should be able to demonstrate that the overall measurement error is no greater than two percent of full scale. An acceptable method would involve a combination of manufacturers' specifications and calibration records.

Environment Audit may be required to verify the physical and electrical environment for the RTU and *IESO* installed telecommunications equipment. The participant may be required to demonstrate that the electrical power supplies meet the requirements. Also, the participant may be required to demonstrate that the environment in which the RTU and telecommunications equipment is installed meets the manufacturer's environmental requirements.

A telecommunication connection must be established between the participant and *IESO*. Participants will grant access to their premises to *IESO* staff or *IESO* designated staff to establish the required telecommunication connection.

The work involved in establishing this connection typically includes:

a. installation of a local loop between the RTU location and a telecommunications service provider;
b. installation of telecommunication equipment at the participant's premises. Typically, this equipment is comprised of two small modules, router/security device and DNP3 communication device; and
c. verifying that the telecommunication connection is working properly.

RTU Check-In Service is the final step in RTU Site Certification. This involves the verification of the accuracy of the RTUs database to ensure a proper correspondence between the actual field device such as a breaker or measurement and the representation in the RTU. The proper operation of the RTU with *IESO*'s Energy Management System (EMS) and the verification of the RTU database being transmitted to the *IESO* will also be verified. Details of the check-in-service process are available from the *IESO*.

4.2 AGC Operational RTU Specifications

Automatic generation control (*AGC*) is a contracted *ancillary service* used by the *IESO* to fine-tune the match between generation and load. Specific details of implementation will be determined during the contracting process.

The actual control of *generators* under *AGC* is accomplished by control signals sent directly by the *IESO* to the plant controller or RTU installed for data gathering and control. **The *IESO* can send either pulse commands to raise or lower generation or it can send MW set-point commands to change the current generation. The type of signal the sent to a specific unit that is providing *AGC* is determined by the *IESO* and is also dependent on the design of the unit's governor system which controls the power input to the *generator*.** A number of associated data inputs, such as generator status, generator output, etc. must also be telemetered by the RTU to the *IESO* Control Center.

The control signals from the plant controller or RTU will issue raise/lower pulses using an output relay. These can be dry or wet contacts depending on the configuration. The pulses typically are one second in length. On receipt of a raise/lower pulse, the generating units under *AGC* control are expected to change their output MW by a pre-determined amount.

Units which do not have remote MW set-point capability in their governors will execute a power change based on the pulse width (time that the pulse is active) of the raise or lower pulse provided by the IESO's *AGC* controller. The pulse width is used to change the position of the unit's power control device – usually a hydraulic gate or a steam turbine governor valve. The resulting power change may not be exactly what was intended by the *AGC* controller. During the next pass of the *AGC* controller (typically every 2 seconds) the error will be detected and a further adjustment made by the *AGC* controller to all the units participating in *AGC*.

Units which have MW controllers with remote MW set-point capability can choose to use either a pulse width to raise or lower the MW set-point value or they can choose to use a direct MW set-point

value provided by the *IESO*'s *AGC* controller. A direct MW set-point value is preferred because it eliminates any error in converting the pulse width into a MW value. This specification applies to those units that have a MW controller with remote MW set-point capability. A typical block diagram of the entire *AGC* control loop is shown in Figure 4-1 below.

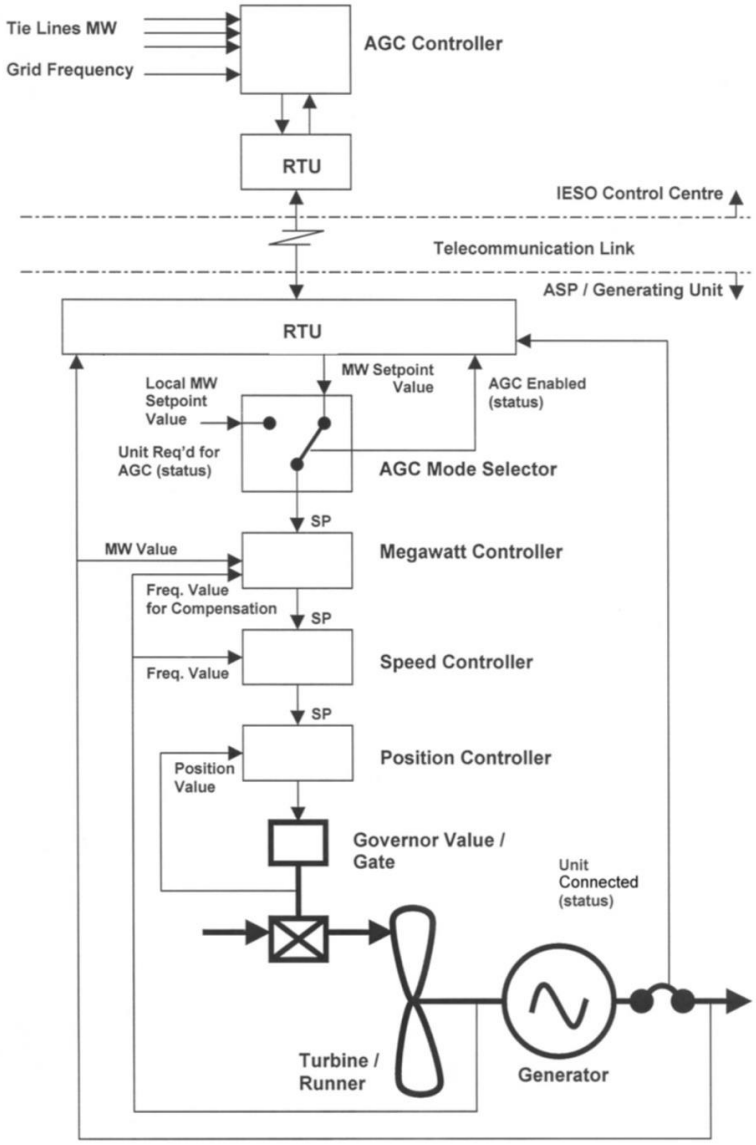

Figure 4-1: Block Diagram of Typical AGC Control Arrangement for Generation units with Remote MW Set-point Control Capability

The information necessary to control the *generation facility* under the terms and conditions of the *AGC* contract will reside and operate in the EMS according to the existing control schemes.

It is the participant's responsibility to protect their equipment from damage due to erroneous pulses or spurious signals that may cause the equipment to operate beyond its designed parameters, regardless of how these signals were generated or transmitted.

– End of Section –

5. Market Applications

5.1 Market Application Systems Information

5.1.1 Overview of Dataflow Systems

The figure below provides an overview of the dataflow from the participants to the *IESO* systems. The following paragraphs also provide technical details of various market applications and application interfaces. It is not intended to provide procedural information, being outside the purview of this document. Procedural information is available in the relevant *market manuals*.

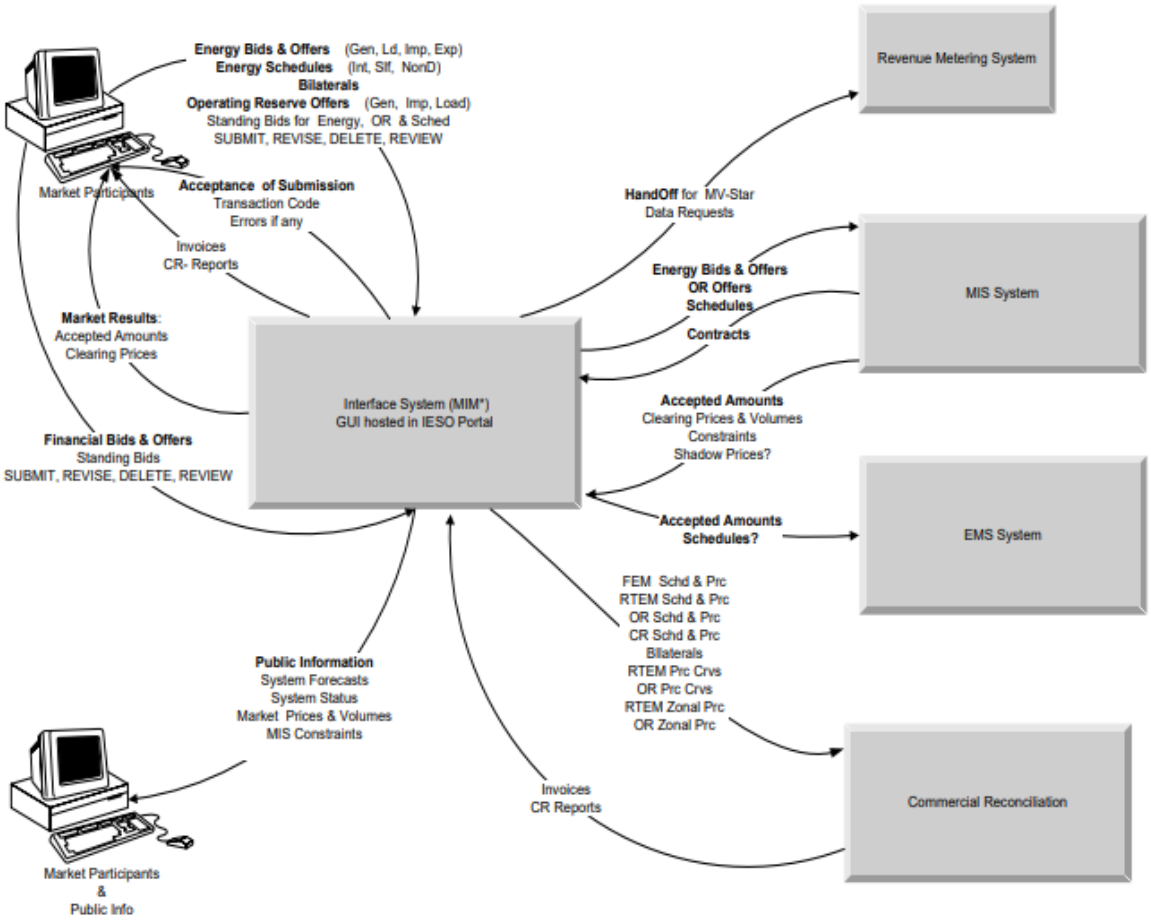

Figure 5-1: Overview of Dataflow from the Market Participant to IESO Systems

5.1.2 Energy Market Application

The Market Information Management (MIM) system at the *IESO* is responsible for receiving participant *bids* and schedules, and then publishing market results. Commercial *settlement* reports and

invoices may be downloaded via the IESO Reports Web Server. The participant may communicate with the system using three mechanisms:

a. Through a *IESO* provided browser-based GUI;
b. Through a programmatic interface via an *IESO* provided API (Web Services).

Bid Data Validation

Submissions are checked for date and all other validations. Submissions for *bids* in the mandatory window must be made not later than 10 minutes before the mandatory hour closing.

Data coming in to the Market Operating System (MOS) is subject to validation. Three types of validation rules are recognized: syntax validation, technical feasibility checks, and commercial acceptability checks. Invalid data will be rejected with the appropriate error messages being posted to the sender.

Bids/*offers* submitted during the mandatory or restricted window will require *IESO* operator approval/rejection. In case of acceptance of a *bid/offer* that is submitted during the mandatory/restricted window and which exceeds the change tolerances, the *IESO* operator will communicate the decision to the participant as a system log message. This *bid/offer* will then also be included in the valid *bid* report. If the *bid* is rejected by the Exchange Coordinator, the decision is communicated to the participant via a system log message.

MIM Web Services

The MIM Web Services Definition Language (WSDL), the XM Schema Definition (XSD) and the Web Services Client Tool (MWT) are provided at the *IESO* Web site under Technical Interfaces (Market Participant Submissions) for viewing or downloading.

The MIM Web Services is a SOAP based web services and participants can use the operations to submit and download dispatch data using XML formatted files.

Participants can download their applicable *Bids/Offers* data using the following query operations:

Table 5-1: Query Operations to download types of Bids and Offers data

Type of Bids/Offers	**Web Services Function**
Real Time *Energy* Market (RTEM)	RTEMBidQueryOperation
Operating Reserve	OperatingReserveBidQueryOperation
Schedule	ScheduleQueryOperation
Bilateral Contract	BilateralBidQueryOperation
Daily Generation Data (DGD)	DGDBidQueryOperation

Participants can create a new *Bid/Offer* or update their existing *Bids/Offers* data using the following upload operations:

Table 5-2: Query Operations to upload types of Bids and Offers data

Type of Bids/Offers	**Web Services Function**
Real Time *Energy* Market (RTEM)	RTEMBidUploadOperation
Operating Reserve	OperatingReserveBidUploadOperation
Schedule	ScheduleUploadOperation

Type of Bids/Offers	Web Services Function
Bilateral Contract	BilateralBidUploadOperation
Daily Generation Data (DGD)	DGDBidUploadOperation

Participants can cancel their existing *Bids/Offers* data using the following cancel operations:

Table 5-3: Query operations to cancel types of existing Bids and Offers data

Type of Bids/Offers	Web Services Function
Real Time *Energy* Market (RTEM)	RTEMBidCancelOperation
Operating Reserve	OperatingReserveBidCancelOperation
Schedule	ScheduleCancelOperation
Bilateral Contract	BilateralBidCancelOperation

Participants can query market statuses by calling the "MarketStatusOperation" function.

Participants can query market messages by calling the 'MarketMessageOperation' function.

Participants can retrieve a list of resources for which the account has permission to submit/download *Bids/Offers* data by calling the 'ResourceOperation' function.

Participants can retrieve a list of participants for which the account has permission to submit/download *Bids/Offers* data by calling the 'ActAsMarketParticipantOperation' function.

5.1.3 Settlements Application

The current Commercial Reconciliation system produces *settlement statements*. The IESO Funds Administration (FA) applications group produces *invoices*. Participants have the ability to review and/or download the invoices through the IESO Reports web server. Settlement statements are similarly available through the secure IESO Reports web server (click on this link to go to the IESO private Reports Site https://reports.ieso.ca/private/)

Detailed information regarding the precise format of *settlement statement* files and supporting data files is detailed on the Technical Interfaces page of *IESO*'s Web site.

Further information regarding *charge type* calculations may be found on the Technical Interfaces page of the *IESO*'s Web site.

Settlement Statement Files

The *settlement statement* files and supporting data files contain *settlement amounts* and the underlying data used in those calculations for a participant. The data included mostly pertains to a particular trading date (the primary trade date), but it may also contain missing charges from prior trading dates. Content, field usage, and format are detailed, in "Format Specification for Settlement Statement Files and Data Files", and may be found on the Technical Interfaces page of the *IESO*'s Web site.

Some general notes about the statement files are listed below:

- Participants will download the files via secure access from the IESO Reports web server.
- The timeline for generating the preliminary and final statements for the financial and *physical market*s is detailed in the "Settlement Manual". In general terms however, their issuance is based on a *business day* timeline rather than on a calendar day timeline and is specifically governed by:

- The *IESO* "Settlement Schedule & Payment Calendar" ("Market Rules MDP_RUL_0002, Ch. 9 Section 6.2, "Market Manual 5: Settlements Part 5.1: Settlement Schedule and Payment Calendars (SSPCs)"); and
- Any *emergency* procedures that may have to be invoked by the *IESO* under the *IESO* "Market Rules, MDP_RUL_0002".

The companion data files are issued following the same timeline as the Statement Files.

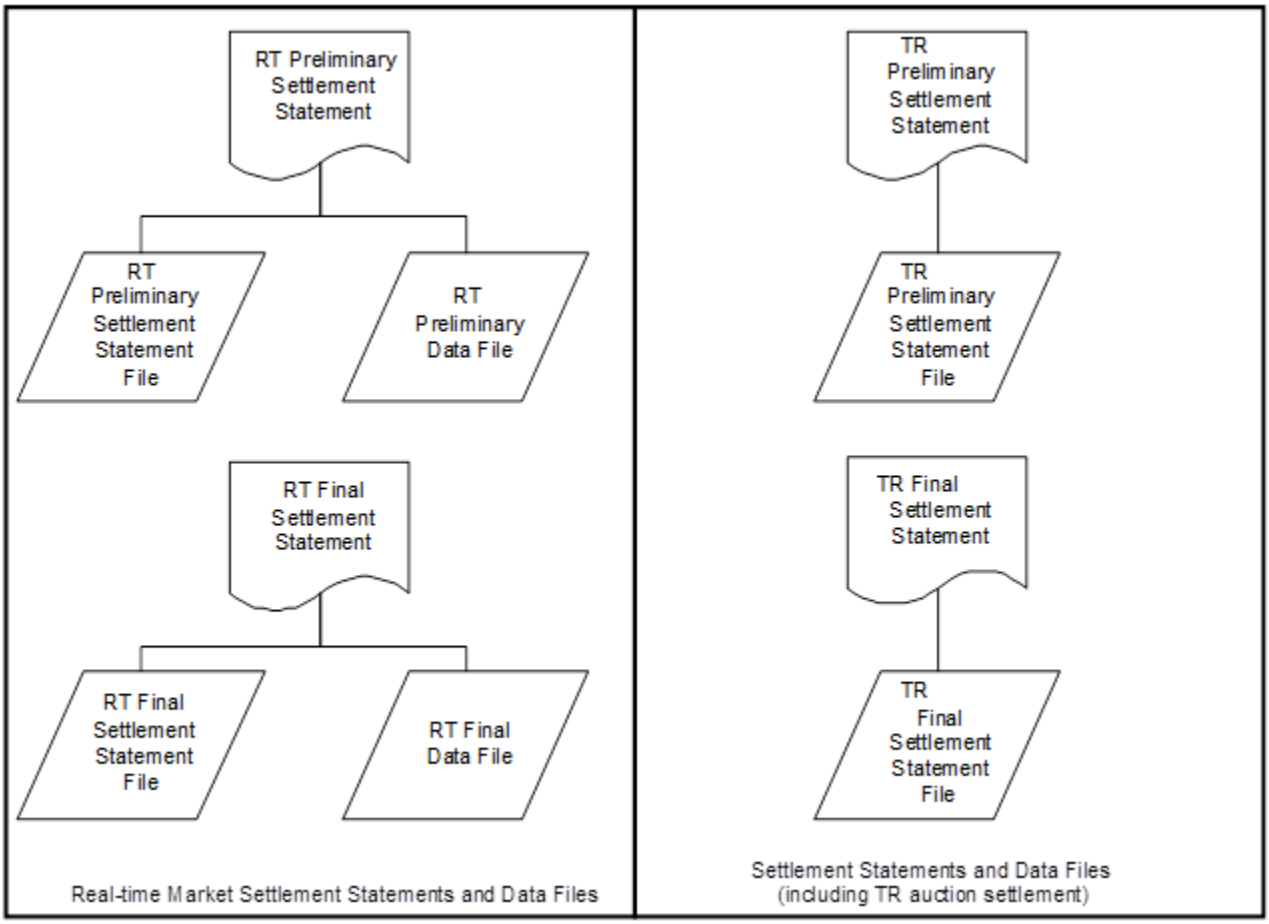

Figure 5-2: Schematic Overview for Settlement Statements and Data Files

The *preliminary settlement statement* provides each participant with an opportunity to review all *settlement* amounts that have been calculated for a particular *trading day* and raise a *notice of disagreement* if necessary. After a predetermined *notice of disagreement* period, a final statement is generated.

Information regarding the format of the *settlement statement* files and supporting data files is provided in, "Format Specification for Settlement Statement Files and Data Files".

Settlement Statement Supporting Data Files

The timeline for issuing the preliminary and final data files for a given trading date are detailed in the "Settlement Manual". In general terms however, their issuance is based on a *business day* timeline rather than on a calendar day timeline and is specifically governed by the following:

- The IESO Settlement Schedule & Payment Calendar ("Market Rules MDP_RUL_0002, Ch. 9 Section 6.2, "Market Manual 5: Settlements Part 5.1: Settlement Schedule and Payment Calendars (SSPCs)"); and
- Any *emergency* procedures that may have to be invoked by the *IESO* under the *IESO* "Market Rules MDP_RIL_0002".
- With each set of *settlement statement* files, each participant will receive a data file. Each data file will correspond to a statement, and will have the same settlement statement ID.
- The data contained in the supporting data file provides each participant supporting data that is used in calculating the preliminary *settlement* for a particular trading date in the *physical market*. The final settlement data file contains the supporting data that is used in calculating the final settlement.

5.1.4 Prudential Manager Application

Accessible via the IESO Gateway, the Prudential Manager Forms application provides functionality to permit participants to understand and manage their prudential requirements. This includes information on estimated net exposure, *margin call* warnings, *margin calls*, *prudential support obligations*, prudential support posted, prudential support reassessments, notification of prepayments and default notices.

5.1.5 Transmission Rights Auction Application

Accessible via the IESO Gateway, the *IESO* Web based TRA application securely allows participating participants to access Transmissions Rights Auctions data by navigating to the TRA application pages:

- The Future Rounds page provides authorized access to upcoming TRA auction information when available.
- The Active Rounds page provides authorized access to TRA Auctions in progress.
- Transmission Rights Auction *Settlement* information can be found in the "Financial Market Settlement Schedule and Payment Calendar".
- TRA users should update their IESO Gateway account password every 90 Days

5.1.6 Online IESO System

The web based Online IESO system allows participants to access it using a IESO Gateway account. A user logged into the IESO Gateway can click on the Online IESO System tile and access it.

The Online IESO System – Manage Participation, Manage Resources, Manage Enrolment Requests, Manage My Information, Manage System Access, Submit Capacity Qualification, Submit Prudential Support Information and Update Organization applications enable the participant to register who they are, and in addition register for enrolment in markets or programs and request system access for *IESO* systems.

Other Online IESO Applications include:

The Online IESO System – Manage Meter Installation application permits management of *metering installations*.

The Online IESO System – Manage Meter Data Report Profile, Request Meter Data Report applications permits management of *meter* data reports.

The Online IESO System – Manage Facilities and Equipment application permits management and registration of equipment and facilities installations.

The Online IESO System – Create a Meter Trouble Report and Schedule a Metering Outage application replaces the old workflow MTR system with equivalent and improved functionality.

The Online IESO System – Create a Notice of Disagreement, View Notice of Disagreement System Variables applications.

The Online IESO – Submit Capacity Qualification, Submit Capacity Auction Offer, Manage Capacity Commitments, Capacity Prudential System, applications permit submissions and reporting for the *capacity auctions*.

The Online IESO – Manage Demand Response Contributor Registry Information and Submit Demand Response Measurement Data permit submissions and reporting for *demand response resources*.

The Online IESO System – Reliability Compliance Tool application enables the IESO to perform comprehensive and thorough reporting procedures and audit controls for ensuring the IESO and participants' compliance to all *reliability* standards and criteria for IESO Reliability Compliance Program.

5.1.7 IESO Confidential Report Site

The web based Confidential Report Site allows participants to access it using an IESO Gateway account even though it is not directly hosted by the IESO Gateway. Participants register their users for access via the normal Online IESO Registration processes. The report site supports XML, HTML, text, zip and EDI report files and now provides additionally for SFTP download.

5.2 Funds Administration

5.2.1 HTML and Text File Invoices

Invoices will be distributed to the participants via XML, HTML or text files hosted on the IESO Confidential Reports web server The participant using any standard web browser over the web can view these XML, HTML or text files. The participant can also download and save the XML, HTML or text file and print the *invoice*.

Descriptions of the XML and text file invoice may be found in the Technical Interface document entitled, "Text File Invoice Format Specification".

5.2.2 E-mail

Emailing of *invoices* and statements is not available as an option.

5.2.3 Fund Transfers

Banks used by the participants must have *electronic funds transfer* capability. *Electronic funds transfer* is a computerized mode for payment and withdrawal used in transferring funds from the participant's bank account to the *IESO* and vice versa.

There are 3 types of electronic funds transfer used by banks including EDI, Wire Transfers, and pay-only electronic funds transfer (Direct Deposit). The amount of information passed to the *IESO* with each of these types of payment is different. The short time frame within which the *IESO* is required

to remit payment to the credit side of the market makes it important to identify the source and relevant invoices associated with payments made to the *IESO* as quickly as possible. The EDI and Wire transfer approaches to *electronic funds transfer* provide the *IESO* with sufficient detail to make identification possible. Pay-only electronic funds transfer (Direct Deposit), however, cannot provide the *IESO* with the needed information. The *IESO* is therefore requesting participants using pay-only electronic funds transfer to send a fax to the *IESO* Finance Department with the details of the payment provided (participant name, *invoice* number(s), amount of payment).

– End of Section –

Appendix A: List of Commonly Used Acronyms

Acronym	Meaning
ANSI	American National Standards Institute
AGC	*Automatic generation control*
API	Application Program Interface
BES	Bulk Electricity System
BOC	Backup Operating Center
Bps	Bits per second
DMI	Desktop Management Interface
DSU	Digital Service Unit
EDI	Electronic Data Interchange
EMS	*Energy* Management System
FIS	Financial Information Systems
GUI	Graphical User Interface
ICCP	Inter Control Center Protocol
ICG	*IESO-Controlled Grid*
IEEE	Institute of Electrical and Electronics Engineers
IESO	*Independent Electricity System Operator*
IP	Internet Protocol
ISO	International Standards Organization
IT	Information Technology
KB	Kilobytes
Kbps	Kilobits per second
LAN	Local Area Network
MB	Megabytes
Mbps	Megabits per second
MIM	Market Information Management
MMP	Metered Market Participant
MSP	*Meter* Service Provider
MW	megawatts
NERC	North American Electric Reliability Council
OS	Operating Systems
PC	Personal Computer (IBM compatible)

Acronym	Meaning
PSTN	Public Switched Telephone Network
PKI	Public Key Infrastructure
PLC	Participant Life Cycle or Registration System
RCT	Reliability Compliance Tool
RTU	Remote Terminal Unit
RTEM	Real-Time Energy Market
SCADA	Supervisor Control and Data Acquisition
TCP	Transmission Control Protocol
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
VAr	Volt-Ampere-Reactive

– End of Section –

References

Document Name	Document ID
DNP 3.0 Subset Definitions	Non-IESO (click on link to DNP web site www.dnp.org)
Market Rules	MDP_RUL_0002
Market Manual 3: Metering; Part 3.0: Metering Overview	MDP_MAN_0003
Market Manual 1: Market Entry, Maintenance & Exit; Part 1.3: Identity Management Operations Guide	IMP_GDE_0088
Format Specifications for Settlement Statement Files and Data Files	IMP_SPEC_0005
Market Manual 5: Settlements Part 5.0: Settlements Overview	MDP_MAN_0005
Market Manual 5: Settlements Part 5.1: Settlement Schedule and Payment Calendars (SSPCs)	MDP_PRO_0031
IESO Reports API Guide	N/A
IESO Gateway User Guide	N/A

– End of Document –