MANUAL

Connecting Today.
Powering Tomorrow.

Market Manual 6: Participant Technical Reference Manual

Participant Technical Reference Manual

Issue 37.0

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 37.0
Reason for Issue	Updated to meet accessibility requirements pursuant to the *Accessibility for Ontarians with Disabilities Act.*
Effective Date	November 9, 2020

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

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
Throughout document	Updated to meet accessibility requirements pursuant to the *Accessibility for Ontarians with Disabilities Act*.

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*, 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* 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 Portal 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 note that Windows 7 is no longer supported by Microsoft and the *IESO* encourages 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. However, it is recommended that participants use IE 11.0 due to end of Microsoft support for earlier browser versions.

128-bit encryption is required with the Internet Explorer browser. To make sure that Internet Explorer uses 128-bit or more of cipher strength, please use following steps:

a. Click Tools while Internet Explorer is open.
b. Click Internet Options and then click advanced.
c. Under Security section, check mark Enable TLS 1.0, TLS 1.1 and TLS 1.2, Enable SSL 3.0 and Disable Enhance Protected Mode.
d. Save the changes by clicking Apply and OK.

The *IESO* secure websites have been configured to work with SSL 3.0 or higher which requires this level of encryption.

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

Internet Explorer has been tested with the Online *IESO* System. It will function as expected with the supported Microsoft OS, Internet Explorer combinations

The *IESO* Portal is accessible with Internet Explorer 11.0. This specification is provided by the *IESO*'s Portal vendor Oracle. The vendor has also stated that browser support is no longer based on OS but strictly tied to the browser themselves, no matter which OS they are installed on except where noted. However, going forward the *IESO* no longer supports Internet Explorer versions prior to 11.0.

Prudential Manager Browser Configuration

The Prudential Manager applications have the following requirements:

- Screen resolution of 1024 X 768 or higher.
- Internet Explorer version 11.0 with Compatibility View setting updated to include ieso.ca to the Web site list. IE 8.0 and 9.0 will work but are not supported.
- Internet Explorer native XMLHTTP enabled.
- Internet Explorer pop-up blocker configured to allow pop-ups from *IESO* secure sites.

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 *IESO* has implemented a new 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 at this link to the *IESO* Reports API Guide:
http://www.ieso.ca/Documents/ti/API_Guide/IESO_Reports_API_Guide.pdf.

Microsoft Internet Explorer Configuration for Portal and Online IESO

The *IESO* Portal is the secure web based system used for hosting market applications accessible to participants. This includes:

- Transmission Rights Auction.
- On-line Settlement Forms.
- Prudential Manager.
- Various Collaboration initiatives such 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.
- Access to the new Online IESO system for Registration, *Meter* Trouble Reporting, Notice of Disagreement, Meter Installation registration, *Facility* and Equipment Registration, Prudential, Capacity Auction, and *Demand Response* applications.

The Online IESO system securely hosts a number of market applications. This includes:

- 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.

For the supported versions of Microsoft Internet Explorer to work properly with the Portal and Online IESO there are a number of configuration settings that need to be made. This includes configuration items in both the Advanced and Security tabs under Internet Options menu selection in Internet Explorer. It is important to note that the settings are unique to each user profile for IE on a workstation. Therefore, if multiple users with separate logins share a workstation, settings will need to be checked and altered as required for each user.

Under Windows 10, Internet Explorer 11.0 use the Protected Mode capability for the various security zones as described at this link to the Microsoft Web site: http://msdn2.microsoft.com/en-us/library/bb250462.aspx. The recommendation is to put the Portal and *IESO* corporate Web site URLs into the 'Trusted sites' zone when using Windows 10 and turn off Protected Mode for this zone only. Windows 10 enforces the opening of a new browser window every time the security zone changes

Internet Options – Advanced

A number of parameters may need to be set for Advanced Internet Options. To do this:

1. Under the IE Tools menu select Internet Options.
2. Select the Advanced tab. See Figure 2-1. (IE / Windows 10 is shown).

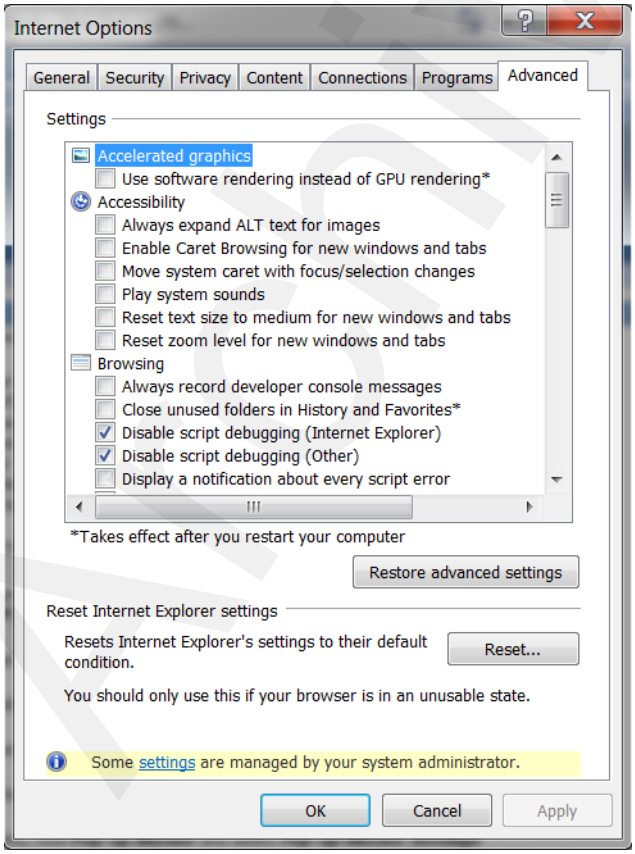


Figure 2-1: Internet Explorer, Internet Options - Advanced

Choose the following settings as shown in Table 2-1 for the appropriate Windows / IE combination and then click on the 'Apply' button. Depending on the user's workstation software environment, specific options may need to be altered from the settings recommended here for proper function of Internet Explorer under all circumstances with other non-*IESO* applications.

Table 2-1: Table 2-1: Internet Explorer Advanced Internet Options with Windows 10

Advanced Internet Option Parameter	**IE 11.0, Windows 10 Selection**
Accelerated Graphics Options	
User software rendering instead of GPU rendering	No stipulation
Accessibility Parameters – All Options	
Always expand ALT text for images	Not applicable
Move system caret with focus/selection changes	Not applicable
Play system sounds	No stipulation
Reset text size to medium for new windows and tabs	Not applicable
Reset text size to medium while zooming	Not applicable
Reset Zoom level for new windows and tabs	Not applicable
Browsing Parameters	
Always record developer console messages	Not applicable
Close unused folders in History and Favorites	Not applicable
Disable script debugging (Internet Explorer)	Not applicable
Disable script debugging (Other)	Not applicable
Display a notification about every script error	Not applicable
Enable automatic crash recovery * (requires restart)	Not applicable
Enable FTP folder view (outside of Internet Explorer)	Not applicable
Enable Suggested Sites	Not applicable
Enable page transitions	Not applicable
Enable Personalized Favorites menu	Not applicable
Enable third-party browser extensions * (requires restart)	Not applicable
Enable visual styles on buttons and controls in web pages	Not applicable
Go to an intranet site for a single word entry in the address bar	No stipulation
Load sites and content in the background to optimize performance	Not applicable
Notify when downloads complete	Not applicable

Advanced Internet Option Parameter	**IE 11.0, Windows 10 Selection**
Reuse windows when launching shortcuts	Not applicable
Show friendly HTTP error messages	Not applicable
Underline links	Not applicable
Use inline AutoComplete in File Explorer and Run Dialog	No stipulation
Use inline AutoComplete in the Internet Explorer Address bar and Open Dialog	Not applicable
Use most recent order when switching tabs with Ctrl+Tab	Not applicable
Use Passive FTP (for firewall and DSL modem compatibility)	Not applicable
Use smooth scrolling	Not applicable
HTTP 1.1 Settings	
Use HTTP 1.1	Not applicable
Use HTTP 1.1 through proxy connections	Not applicable
International	
Always show encoded addresses	Not applicable
Send IDN Server Names for Intranet addresses	Not applicable
Send IDN server names for non-Intranet addresses	Not applicable
Send URL path as UTF-8	Not applicable
Send UTF-8 query strings for Intranet URLs	No stipulation
Send UTF-8 query strings for non-Intranet URLs	No stipulation
Show Information Bar for encoded addresses	Not applicable
Use UTF-8 for mailto links	Not applicable
Microsoft VM	
Java Console enabled	Not applicable
Java logging enabled	Not applicable
JIT compiler for virtual machine enabled	Not applicable
Multimedia	

Advanced Internet Option Parameter	**IE 11.0, Windows 10 Selection**
Enable alternative codecs in HTML5 media elements * (requires restart)	Not applicable
Enable automatic image resizing	Not applicable
Play animations in web pages * (requires restart)	Not applicable
Play sounds in web pages	Not applicable
Play videos in web pages	Not applicable
Show image download placeholders	Not applicable
Show pictures	Not applicable
Show image dithering	Not applicable
Printing	
Print backgrounds colors and images	Not applicable
Search from the Address bar	Not applicable
Security	
Allow active content from CD to run on My Computer * (requires restart)	Not applicable
Allow active content to run in files on My Computer	Not applicable
Allow software to run or install even if the signature is invalid	Not applicable
Block unsecured images with other mixed content	No stipulation
Check for Publishers certificate revocation	Not applicable
Check for server certificate revocation * (requires restart)	Not applicable
Check for signatures on downloaded programs	Not applicable
Do not save encrypted pages to disk	Not applicable
Empty Temporary Internet Files folder when browser is closed	Not applicable
Enable DOM storage	Not applicable
Enable Enhanced Protected Mode * (requires restart)	Not applicable
Enable Integrated Windows Authentication * (requires restart)	Not applicable
Enable memory protection to help mitigate online attacks	Not applicable

Advanced Internet Option Parameter	IE 11.0, Windows 10 Selection
Enable native XMLHTTP support	Not applicable
Phishing Filter	Not applicable
Enable SmartScreen filter	Not applicable
Enable Strict P3P Validation * (requires restart)	Not applicable
Send do not track requests to sites you visit in Internet Explorer * (requires restart)	Not applicable
Use SSL 2.0	Not applicable
Use SSL 3.0	Not applicable
Use TLS 1.0	Not applicable
Use TLS 1.1	Not applicable
Use TLS 1.2	Not applicable
Warn about invalid site certificates	Not applicable
Warn about certificate address match * (requires restart)	Not applicable
Warn if changing between secure and not secure mode	Not applicable
Warn if Post submittal is redirected to a zone that does not permit posts	Not applicable

Internet Explorer – Internet Options – Security

A number of security configuration settings need to be made in order for proper functioning of the browser with various *IESO* web sites. The participant can choose to define and place the Portal and Online *IESO* URLs for the Production and Sandbox environments into the Trusted Sites zone under IE Security If the URLs are left in the Internet zone by default then it is recommended that the Security settings for that zone be configured as defaulted (medium security level) except where noted. However, for Windows 10 is important that the URLs be placed in the ‘Trusted sites’ zone as well as the IESO corporate site as discussed previously.

When the URL’s are included in the 'Trusted Sites' zone it is recommended that the Security settings default of medium be left as is.

However, the participant’s IT security people should be involved in deciding the appropriate settings and implement based on their own rules and policies, which may take precedence over the settings recommended here. The choice is in the end, up to each participant.

Internet Zone Security Settings

When leaving the *IESO* Portal URLs by default in the IE 'Internet' zone for Windows 10 it is recommended the following settings be made:

1. Under the Tools menu select Internet Options.
2. Select the Security tab. See Figure 2-2 (IE 11 / Windows 10 shown). For Windows 10 some additional security has been added in the form of Protected Mode as mentioned above. This can be turned on or off for each security zone. It is required under Windows 10 for the Portal Energy Market GUI web site that Protected Mode is turned off. This can be done in the

Security tab via the check box at the bottom of the Internet Options window as shown in Figure 2-2 as follows.

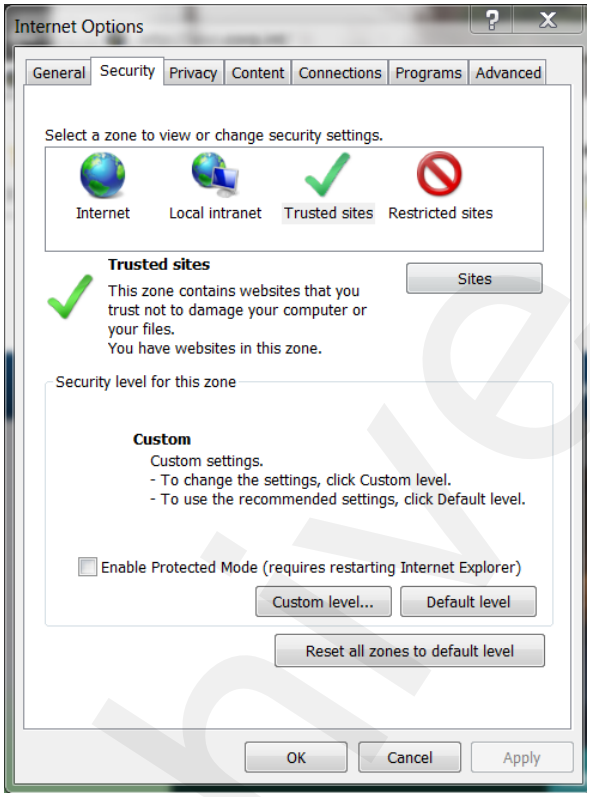


Figure 2-2: Internet Explorer 11.0, Internet Options – Security – Windows 10

3. In the security tab, click on the Internet zone icon to specify its security settings. The default level for the Internet zone in IE is 'Medium'. Most of the settings should be left as is unless security policies for the participant require something else.
4. Click on the 'Custom Level' button to activate the Security Settings configuration window. See Figure 2-3 below. (IE 11 / Windows 10 shown)
5. Verify default settings are as per Table 2-2 and Table 2-3 when *IESO* Portal URLs are by default in the Internet zone. If conflicts occur for other IE operations with other Web sites modify as required for optimal and secure operation of Internet Explorer.
6. Click on the "OK" button to accept all changes.

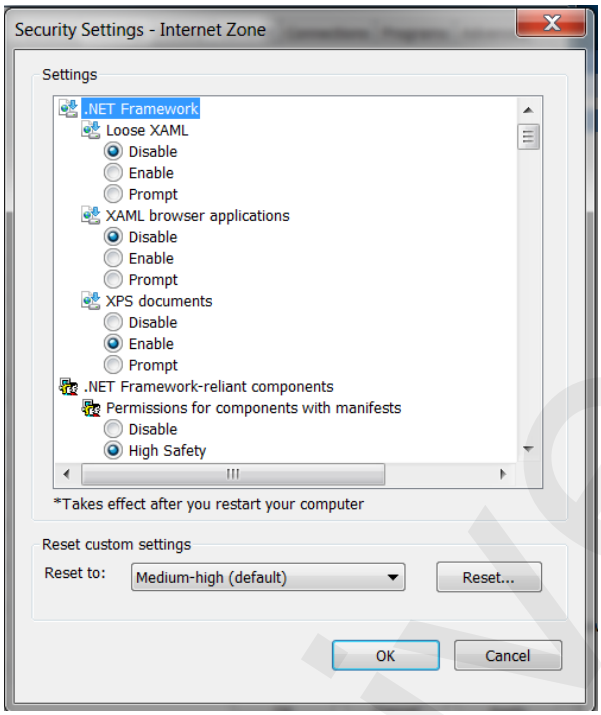


Figure 2-3: Internet Explorer 11.0, Internet Options – Custom Security Settings Window

Trusted Sites Security Setting

When including the *IESO* Portal Online IESO URLs in the IE 'Trusted Sites' zone it is recommended the following configuration settings be made:

1. Under the Tools menu select Internet Options.
2. Select the 'Security' tab. See Figures 2-2 and 2-3 above.
3. Click on the Trusted Sites zone icon to specify its security settings. The default level for the Trusted Sites zone in IE is Medium for Windows 10. It is recommended to leave as default for Windows 10. Notice that the 'Sites' button is now active.
4. Click on the 'Sites' button to activate the 'Trusted Sites' entry window. See Figure 2-4.
5. Type in the address(es) of the trusted sites for the *IESO*'s Production and Sandbox Portal environments and use the 'add' button to add them. See Figures 2-5 and 2-6. Note that the production Online IESO system has already been added in the example.

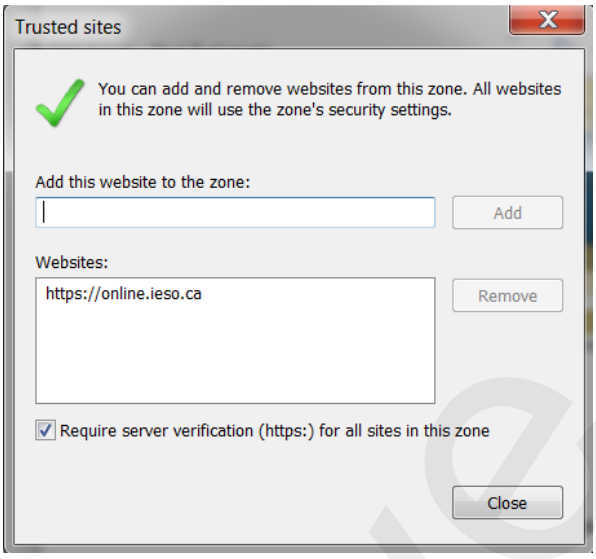


Figure 2-4: Internet Explorer 11.0, Internet Options - Trusted Sites Security –Windows 10

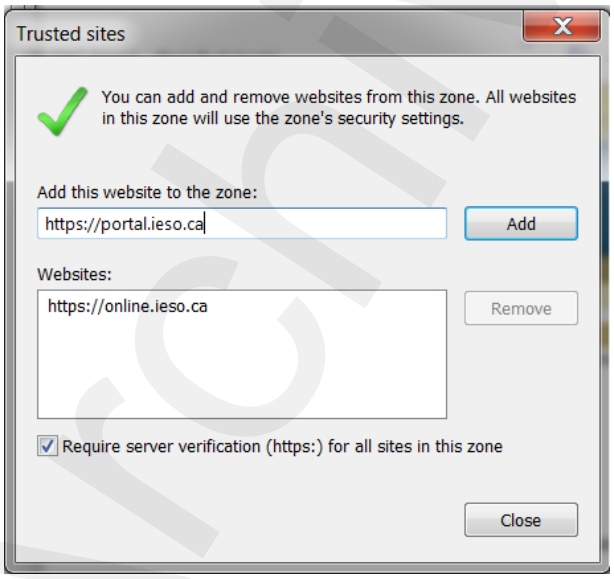


Figure 2-5: Internet Explorer 11.0, Trusted Sites Security – Web Sites Addition – Windows 10

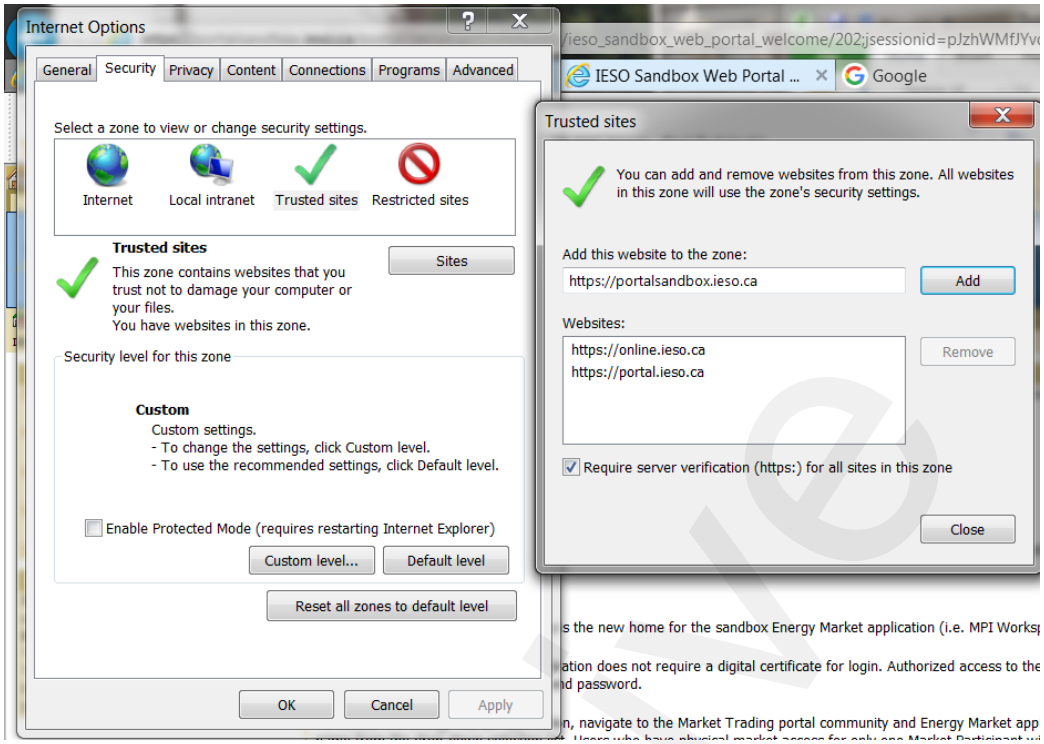


Figure 2-6: Internet Explorer 11.0, Trusted Sites Security – Web Sites Addition – Windows 10

6. Click on the “Require Server Verification (https) for all sites in this zone” option check flag if all sites entered here are https sites like the *IESO*’s Portal.
7. Click on the ‘OK’ button.
8. Click on the 'Custom Level' button to activate the Security Settings configuration window.
9. Verify settings as per Table 2-2 when *IESO* Portal URLs are in the Trusted Sites zone for and the appropriate Windows and Internet Explorer combination. If conflicts occur for other IE operations with other Web sites modify as required for optimal and secure operation of Internet Explorer. Note that choosing the ‘Prompt’ parameter value will require more user overhead than ‘Enable’.

Note: The user can use the right mouse click and then on ‘What’s This’ on each item in IE ‘Security Settings’ for an explanation of each item.

Compatibility View Settings

When including any of the *IESO* Portal, portalapps (i.e. Prudential Manager), or Online IESO URLs in the Compatibility View Settings, the following must be done:

1. Under the Tools menu select Compatibility View settings. A popup window will display. See Figure 2-7 below.

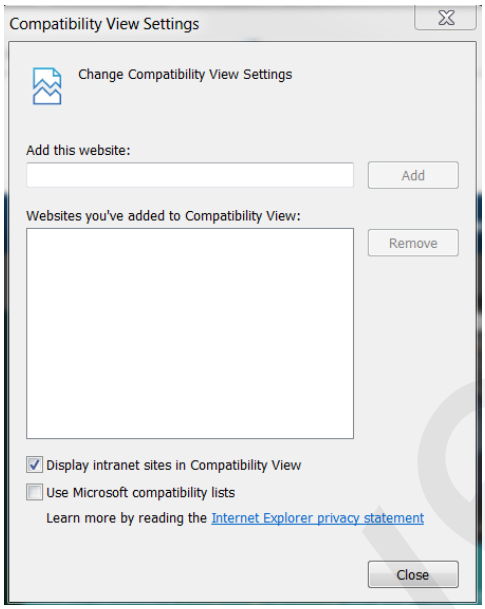


Figure 2-7: Internet Explorer Compatibility View Settings

2. Type in the URL of the Web site to add and click the add button. The domain of the Web site will be added to the list. For example, if https://portal.ieso.ca is typed in, then 'ieso.ca' will be added. It is similar for any other IESO secure Web site.
3. When the Portal, portalapps.ieso.ca, and Online IESO sites are added, the Compatibility View settings list will show as shown in Figure 2.8. Any other required Web sites can be added as needed by the participant.

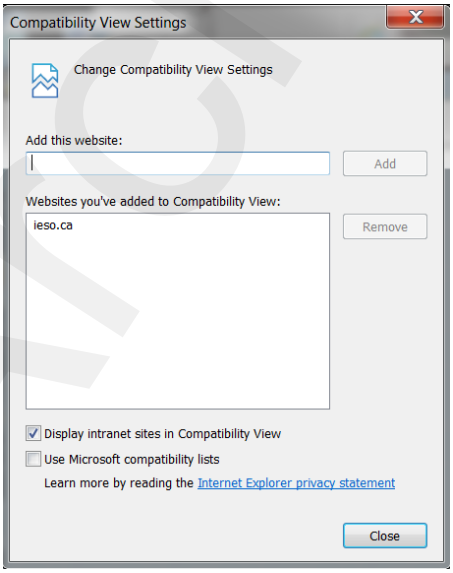


Figure 2-8: Compatibility View Settings with ieso.ca added

Table 2-2: IE Internet Options, Security Settings –Windows 10

Parameter	When Portal and other IESO URLs added to 'Trusted Sites' zone in Windows 10 and IE 11.0
General Security Level for zone	Medium
.NET Framework	
Loose XAML	No stipulation
XAML browser application	No stipulation
XPS documents	No stipulation
.NET Framework-reliant components	
Permissions for components with manifests	High safety
Run components not signed with Authenticode	Prompt
Run components signed with Authenticode	Enable
Active X Controls and Plug-ins	
Allow ActiveX Filtering	Enable
Allow Previously unused ActiveX controls to run without prompting	Enable
Allow Scriptlets	Enable
Automatic prompting for ActiveX controls	Enable
Binary and script behaviors	Enable
Display video and animation on a webpage that does not use external media player	No stipulation
Download Signed ActiveX Controls	Enable
Download Unsigned ActiveX Controls	Prompt
Initialize and script ActiveX controls not marked as safe	Prompt
Run ActiveX controls and plug-ins	Enable
Run antimalware software on ActiveX controls	Disable
Script ActiveX controls marked as safe for scripting	Enable
Downloads	
Automatic prompting for file downloads	Enable
File Download	Enable
Font Download	Enable
Enable .NET Framework setup	Enable

Parameter	When Portal and other IESO URLs added to 'Trusted Sites' zone in Windows 10 and IE 11.0
Miscellaneous	
Access data sources across domains	Enable
Allow dragging of content between domains into separate windows	Enable
Allow dragging of content between domains into the same window	Enable
Allow META REFRESH	Enable
Allow scripting of Microsoft Web browser control	Enable
Allow script initiated windows without size or position constraints	Disable
Allow web pages to use restricted protocols for active content	Prompt
Allow websites to open windows without addresses or status bars	Enable
Display mixed content	Enable
Don't prompt for client certificate selection when no certificates or only one certificate exists - (i.e. automatic certificate presentation)	Disable
Drag and drop or copy and paste files	Enable
Enable MIME sniffing	Enable
Include local directory path when uploading files to a server.	Enable
Launching applications and unsafe files	Prompt
Launching programs and files in an IFRAME	Enable
Navigate sub-frames across different domains	Enable
Render Legacy Filters	Enable
Submit non-encrypted form data	Enable
Use Pop-up blocker	No Stipulation
User data persistence	Enable
Web sites in less privileged web content zone can navigate into this zone	Enable
Scripting	
Active scripting	Enable
Allow programmatic clipboard access	Enable

Parameter	When Portal and other IESO URLs added to 'Trusted Sites' zone in Windows 10 and IE 11.0
Allow status bar updates via script	Enable
Enable XSS filter	Disable
Allow websites to prompt for information using scripted windows	Enable
Scripting of Java applets	Enable
User Authentication	
Log-on	Automatic log-on only in Intranet zone

Internet Explorer Pop-up Blocker with Windows 10 and the Portal

Internet Explorer, pop-up blocker functionality can have some beneficial and some detrimental effects depending on the needs of the browser user. When enabled with just default settings, the IE pop-up blocker affects the functionality of the Portal. The Energy Market Application System Messages and Market Status windows for example do not activate and properly display when pop-up blocking is active and not disabled for the Energy Market Application hosted in the Portal Web site. It is recommended that IE configuration settings for pop-up blocking be set so that Energy Market Application functionality is not affected.

This functionality continues as is with Internet Explorer 11.0 under Windows 10. The directions included here apply to all the combinations of Windows 10 and IE 11.0.

Internet Explorer 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 Tools menu select the Pop-Up Blocker menu option.
2. A submenu list will display. If the pop-up blocker is enabled the first submenu option will indicate Turn Off Pop-up Blocker. If it is disabled, the first submenu option will indicate Turn On Pop-up Blocker. This option works as a toggle to enable or disable the pop-up blocker. See Figure 2-9.

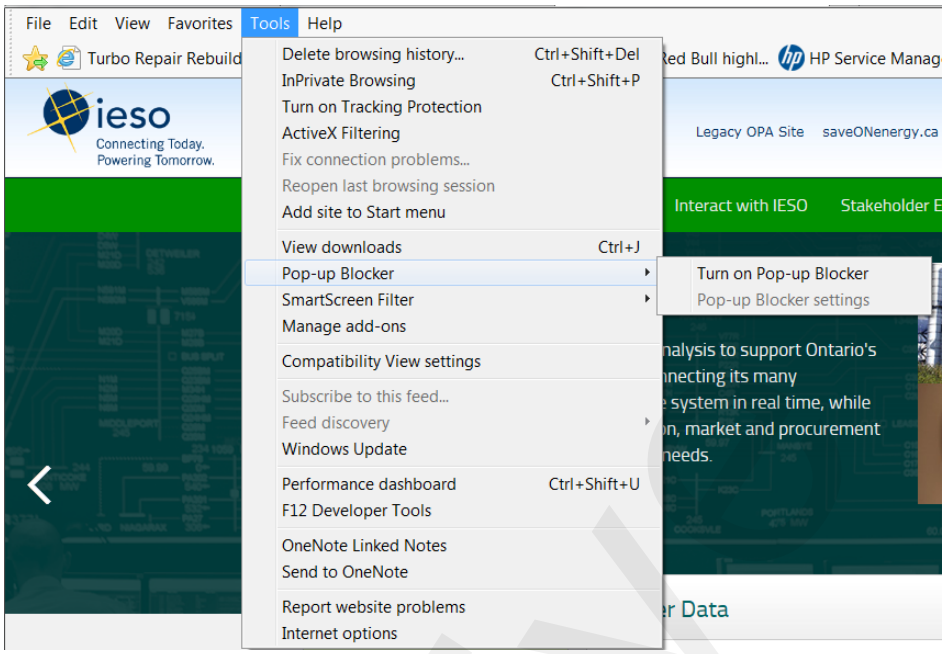


Figure 2-9: Internet Explorer, Enabling or Disabling Pop-up Blocker

Internet Explorer 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 Application within the Portal by doing the following:

1. Under the Tools menu select the Pop-Up Blocker menu option.
2. A submenu list will display. Select the Pop-up Blocker settings submenu option when the pop-up blocker has been toggled on. See Figure 2-10.
3. The Pop-up Blocker Settings windows will activate See Figure 2-12.
4. Select the desired blocking level setting (e.g. 'Low: Allow pop-ups from secure sites' as an option if pop-ups are required to be blocked from all sites except those sites protected by SSL). It is up to the discretion of the participant to choose the required blocking level setting for their needs. The low setting will allow all Energy Market Application windows as the Portal URL is a secure site.
5. Enter in the URL addresses of the Sandbox and Production Portal sites in the address of Web site to allow and use the Add button (see Figure 2-13). This will allow the proper functioning of Energy Market Application and Portal, no matter what the blocking level setting.

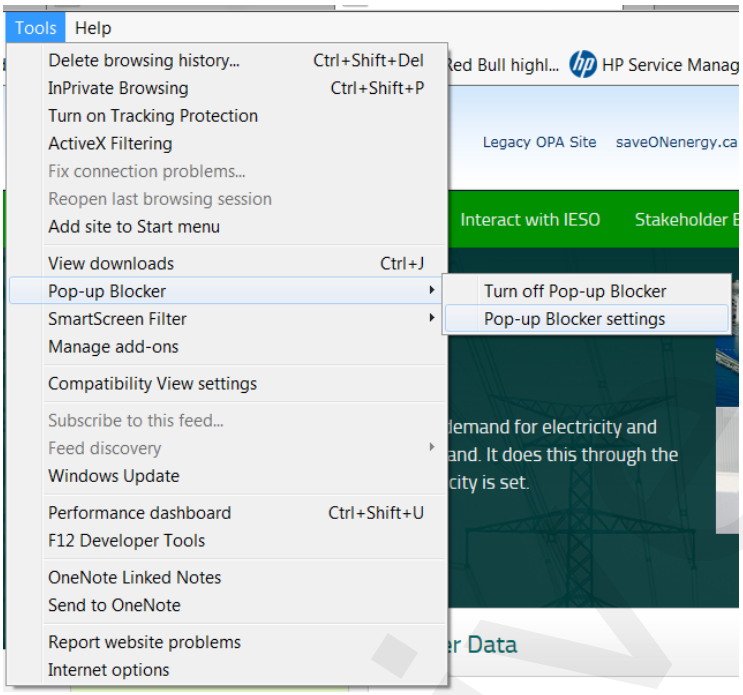


Figure 2-10: Internet Explorer, Activating Pop-up Blocker Settings

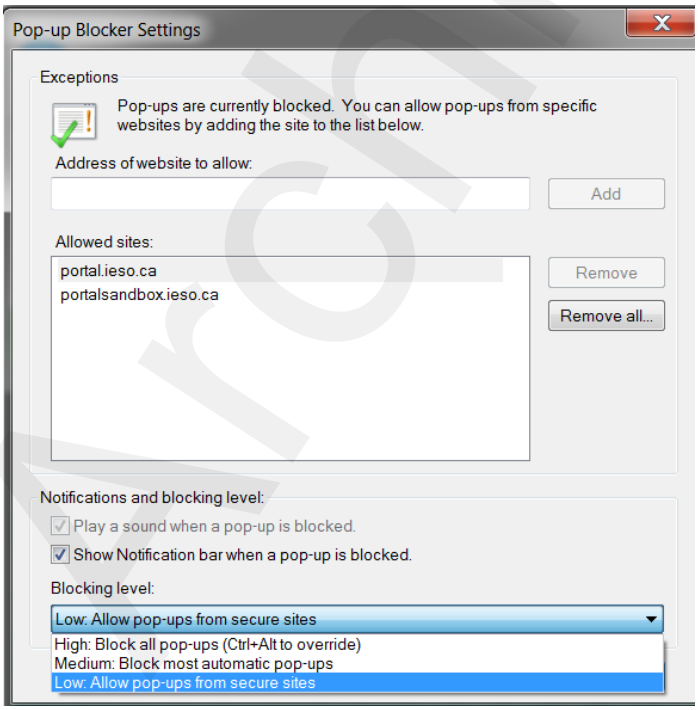


Figure 2-11: Pop-up Blocker Settings Window Filter Setting for Portal Use

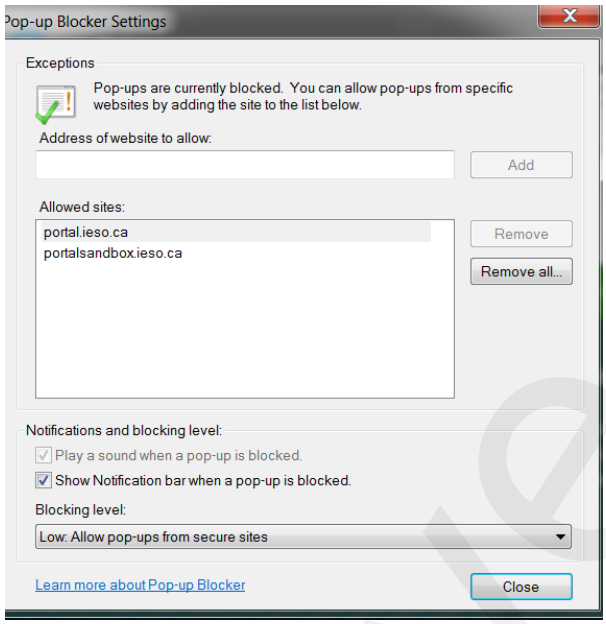


Figure 2-12: Addition of Portal URL to Allow Web Site List for Pop-ups

Java Runtime Environment

A Java runtime environment installed on a client workstation is no longer required for use with the *IESO* Portal for use with a java applet for multiple file upload. This functionality has been replaced with server side JavaScript. Please refer to the IESO Supported Client Platform web page for any required Java runtime environment where applicable.

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 or SHARED over the IESO provided Multiprotocol Label Switching (MPLS).

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 Portal or Online IESO 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."

Traffic Aggregation

The *IESO* will preserve the predictable response time of the Real Time network for participants that choose to use the MPLS Network to submit *bids*, *offers*, and access market *settlements* and metering information over the MPLS Backbone.

A single virtual circuit will be established between the *IESO* and the participant with appropriate Quality of Service and queuing controls enabled.

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* Portal, 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

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

- Portal/Online IESO Passwords must conform to the construction rules as described in the Identity Management Operations Guide.
- If a user enters an incorrect password four times in a row on the Portal 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 Portal 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 authentication questions will be asked. The question choices and their corresponding answers shall have been provided by each user at time of account registration and initial Portal login.

- In accordant with *Market Rule* amendment (MR-00376), if the user fails to answer any additional authentication questions 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 Portal/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.

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
- User ID password reset

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 direct communication with *IESO* Customer Relations.

IESO Access Management is responsible for issuing and maintaining User ID account identity credentials.

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.

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 http://www.ieso.ca/Pages/Participate/Technical-Interfaces.aspx and the Training Page by clicking on this link http://www.ieso.ca/Pages/Participate/Training.aspx 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. The REGISTRATION participant Constant Shortname is not required.

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

All Portal/Online IESO/Confidential Reports users log in with a User ID account credential for all Portal, Online IESO hosted applications and the Confidential Reports site.

The Portal is protected by Oracle 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. Online IESO is protected by Microsoft identity management technologies. The Confidential Reports site is protected by the vendor supplied technologies.

All Portal, 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 Portal User Interface User's Guide" should be referenced for Portal login procedures. The "IESO Reports API Guide" should be referenced for secure access to the Confidential Reports site. This can be found at the following link:
http://www.ieso.ca/Documents/ti/API_Guide/IESO_Reports_API_Guide.pdf.

2.3.5 Requirements for Browser Software Compatibility

Workstation Platform for Portal and Online IESO Browser Client

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

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

- Mozilla Firefox 1.0, 1.5 or 2.0.1,
- Safari 2.0 and 3.0.

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 Portal and MIM programmatic API manuals should be referred to when appropriate.

– 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 Message Exchange and Dispatch Service

Dispatch Message Exchange system is currently being used by *IESO* to send dispatch instructions to and receive responses from Participants.

A new Dispatch Service system is implemented by *IESO* and will be replacing the Dispatch Message Exchange system.

All Participants using existing Dispatch Message Exchange system must migrate to the new Dispatch Service system within a 12-month period following production rollout of the new system.

3.2 Dispatch Message Exchange

3.2.1 Overview

Participants using a *dispatch workstation* will be integrating directly with the EMS systems at the *IESO* and will require interaction with the Message Exchange system. Participants that require this module will be receiving the client software from the *IESO* via the network and will be instructed on its installation and application.

Message Exchange information will be stored in the *IESO* Operations Database (ODB), for use by the Compliance Monitor. This verifies that the requested *dispatch* actually takes place based on the measurement availability.

The participant will:

- acknowledge receipt of the message;
- accept or refuse the *dispatch* request; and
- perform the requested control action.

The Message Exchange function is used by the *IESO* to send *dispatch* instructions to the participants. This function is triggered by the dispatch request of an application (such as *energy* dispatch) to issue a message either automatically by Inter-Control Center Communications Protocol (ICCP) or by WEB-based Message Exchange or manually (off-line by telephone or fax) by the Exchange Coordinator to a participant.

The Message Exchange function sends *dispatch* instruction to the *IESO* participants using ABB's ICCP Block 4 capabilities or the WEB-based Message Exchange facilities.

In order to interface with the Message Exchange using ICCP the participants must also have ICCP Block 4 configured on their *dispatch workstations* and have specialized software to interpret and manage the ICCP block 4 messages.

WEB-based Message Exchange is an alternative facility made available to the *IESO* participants that can be used to support the Message Exchange requirements. The WEB-based Message Exchange adds additional capability to the existing Message Exchange functionality. WEB-Based Message Exchange permits *dispatch* instructions to be sent to the participants using browser compatible user

interface and application programming interface. These interfaces will be included with the delivery of this product. WEB-Based Message Exchange will be simpler to deploy than the ICCP-based Message Exchange and more cost effective for the participants, however this may be a less reliable approach. Interfaces (see Figure 3-1 below) shows the relationship that Message Exchange (ME) has with other parts of the system. Most of the functions are internal to IESO however on the right of the diagram is the interface with the participants.

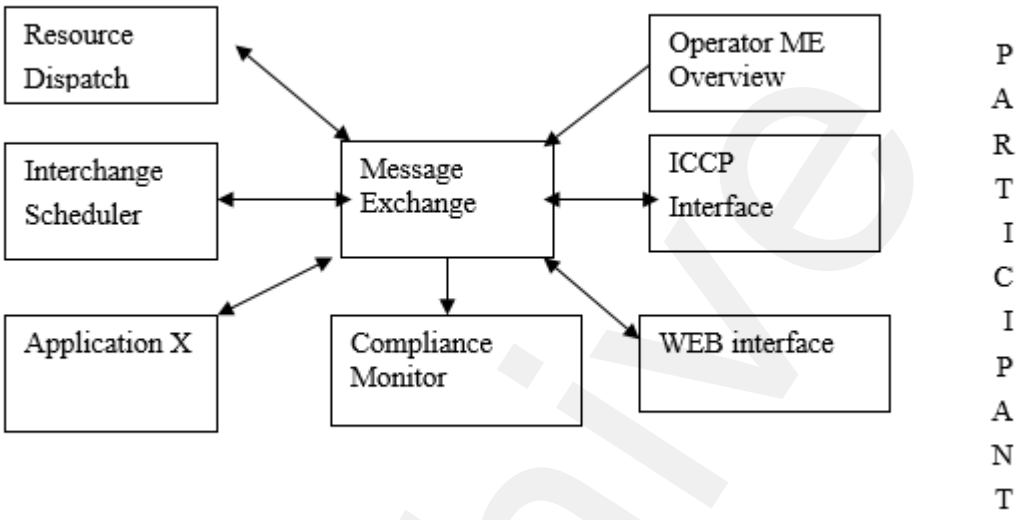


Figure 3-1: Message Exchange Interfaces

Specifics of ICCP Block 4 are discussed in the ICCP guidelines, which can be ordered from EPRI – Report TR-107176 over the Internet.

A WEB-Based Message Exchange user guide has been posted on the *IESO* Web site. The user guide provides information on message displays, user actions and contract management message displays, etc. Participants are encouraged to consult the Web site for further details and latest updates to the user guide.

3.2.2 Hardware requirements

This section provides a description of the *dispatch workstations* required by participants injecting into or withdrawing electrical power from the *IESO-controlled grid* or will receive and transmit information to the IESO.

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.

For Windows 10 and above, it is recommended that the client workstation hardware conform to Microsoft's specifications found on the Microsoft Web site: http://windows.microsoft.com/en-us/windows/windows-help?os=winxp#windows=windows-7

The following provides the minimum hardware requirements.

Processor

The minimum required processor speed is an Intel I5.

Memory

The PC must have a minimum of 4 GB megabytes of internal RAM.

Hard Disk

The PC must have at least four gigabytes of available disk space on a typical 128 GB hard drive.

Interface Cards

The network card must support a high-speed (10 Mbps or greater) network, as it will be required to communicate over Ethernet to an IESO supplied router at the participant site. The wiring between the *dispatch workstation* and the router is the responsibility of the participant. The *IESO* supplied router will communicate over private network (MPLS) to the *IESO*.

Monitor and Graphic Card

The supported monitor must be XVGA with a graphic card that is configurable to 1024 x 768 pixels with 'small font' and 65536 colors at a minimum. A higher resolution of 1920 x 1080 pixels is however, recommended.

Sound Card

The PC must include an appropriate sound card and speakers for receiving audible alarms.

Printer

The recommended printer is high resolution with at least 600 dpi and supports multiple fonts.

3.2.3 Software Requirements

Operating System

The PC should be operating with Windows 10 with support for TCP/IP protocol. It is recommended that the latest operating system patches be maintained.

Internet Browser

For WEB based Message Exchange the PC should include the IE 11.0.

Connectivity

All *dispatch workstations* must maintain a live connection that will allow workstations to receive, send, and acknowledge the messages with the minimum throughput established by the *IESO*.

Power Supply

Given its importance, it is strongly recommended that the participant(s) provide an Uninterruptible Power Supply (UPS) to power the *dispatch workstation*.

3.2.4 Functional Parts

Message Exchange (ME) consists of several independent functional parts:

a. An ICCP Server responsible for establishing and maintaining the communication between utilities using the ICCP protocol and maintains the communication parameters and status for each link.
b. A Web Server (Servlet or Application Server) responsible for establishing and maintaining communication between participants using the https protocol and managing user logins, client requests, publishing client response to SCADA (Supervisory Control and Data Acquisition), subscribing to & performing action requests from SCADA and publishing results of action requests to SCADA.
c. A Web Client providing user interface for the WEB-Based Message Exchange java applet. The software as shown on the "IESO Supported Client Platform" web page is required in order to execute the Message Exchange Applet.
d. The ME Database Server is responsible for storing and retrieving the messages and their status. This database will support both WEB & ICCP.
e. The ME Application Server will co-ordinate the message exchange between different functions. It is responsible for message scheduling and tracking (both WEB and ICCP).

3.2.5 Dispatch Messaging

The *dispatch* messages are generated automatically by the *dispatch algorithm* every five minutes. The Exchange Coordinator (EC) monitors the *dispatches* and the EC can prevent the messages from being sent out in the event of a system disturbance while activating *operating reserve*.

The availability and reliability of the supporting facilities must be such that the following criteria is met:

a. The Exchange Coordinator (*IESO* BES Control Room Operator), in not more than sixty seconds after issuance of the *dispatch* message, must receive the acknowledgement and compliance indication after issuance of the dispatch instruction.
b. The acknowledgement of receipt of a *dispatch* message is automatically performed by the Client application (either *IESO* provided or participant). The compliance is a manual action by the participant to accept or reject the instruction.
c. The *IESO* shall manage and/or control the ICCP and Web-Based communications facilities that support the transmission of *dispatch instructions* to the participants' *dispatch* agent at the point of system injection.
d. Failure of any of the facilities such that the *dispatch* message and/or the reply are not sent/received is alarmed through monitoring software to the Exchange Coordinator upon detection. The alarm is displayed within the message dispatch tool and it will be logged in the systems control log. The alarm indicates the actual, or most likely, reason for the failure.
e. An *outage* to any of the supporting message *dispatch* facilities must be addressed with the highest priority.

Dispatches Processed Through Message Exchange

Energy Dispatch

The *IESO* issues *dispatch instructions* for each *registered facility*, other than a *boundary entity* and an hour-ahead *dispatchable load facility*, prior to each *dispatch interval*, indicating for that dispatch interval:

- The target *energy* level to be achieved (in MW) by the *facility* at the end of the *dispatch* interval at a rate, in the case of a *dispatchable load*, equal to the rate provided by the participant as *dispatch data*, and in the case of a *generation facility* equal to the most limiting of:

- The last *dispatch* instruction and offered ramp rate: or
- Actual MW output and the *generation facility*'s effective ramp rate.

Reserve Dispatch

The *IESO* will process reserve *dispatches* through the Message Exchange. Reserve dispatches are targets for capacity, in the reserve class specified that are available from a participant's resource after acceptance of the *dispatch* instruction.

Reserve Activation

The *IESO* will process reserve activation *dispatches* through the Message Exchange. *Energy dispatches* are target energy output or load reduction from a participant's resource. The participant's resource is expected to follow the *emergency* ramp rate specified during registration of the resource and be at the target within the timeframe specified by the *operating reserve market* for which the *dispatchable generation facility*/*load facility* was scheduled.

Automatic Generation Regulation Activation

The *IESO* will specify *AGC* obligations of a resource through the Message Exchange. The AGC obligations include the *Regulation* Range and may include a specified Base Point that the participant's resource is required to support for a specified period of time.

Voltage Regulation Dispatch

IESO will be installing the capability to specify voltage *regulation* dispatches for *Load* and *Generator* participants through the Message Exchange. Currently the IESO continues to manage the voltage regulation dispatches manually. Voltage regulation dispatches can be specified in terms of terminal voltage set point or MVAR output. Voltage regulation dispatches are targets for terminal voltage and MVAR output for a participant's resource that should be reached within 5 minutes of acceptance of the *dispatch* instruction.

Invoking the Call Option

IESO will be installing the capability to inform participants that they are required for Must Run or Voltage Support through the Message Exchange. Currently the IESO continues to inform participants, manually, that they are required for Must Run or Voltage Support. The Call *dispatch* will identify the *dispatch period* that the participant's resource is required for. The participant is expected to bid/offer into the market as defined in the "Market Rules", for the specified dispatch period.

3.2.6 Dispatch Message Structure

General Structure of All Dispatch Messages

Dispatch messages are composed of a message header and a message body. The content of messages is not 'case sensitive'.

The message header identifies the message and is a common format for all messages.

The HEARTOUT, HEARTIN, ACCEPT, REJECT, RECEIPT, CONFIRMATIONOK, AND CONFIRMATIONNOTOK only include the header information.

AGC dispatch messages may be sent in one of two forms:

1. *Dispatch* Message Body – *Regulation* with Range Dispatch Only: will include the following fields:
    - Persistent Resource

- DISPATCH_TYPE = ‘RGR’
- Startstop = ‘Start’
- RESOURCE_ID
- REGULATION_RANGE = The regulation range in MW expected from the resource.
- DELIVERY_START_TIME
- DELIVERY_STOP_TIME

2. *Dispatch* Message Body – *Regulation* with Range and Fixed Base-Point *Dispatch*: will include the following fields:
    - Persistent Resource
    - DISPATCH_TYPE = ‘RGS’
    - Startstop = ‘Start’
    - RESOURCE_ID
    - AMOUNT = The fixed base point in MW that the unit will operate at while on AGC.
    - REGULATION_RANGE = The regulation range in MW expected from the resource.
    - DELIVERY_START_TIME
    - DELIVERY_STOP_TIME

For details of the *Dispatch* Message Structures and sample examples of all the message types, please refer to the “Web Based Message Exchange – Market Participant’s Guide” document, which is available on *IESO*’s Web site (see the Technical Interfaces page of *IESO*’s Web site).

3.2.7 Dispatch Message Scenarios

Heart beat messages are sent by the *IESO* to determine whether the participant is able to receive dispatch instructions from the *IESO*. The following scenario table describes this:

Table 3-1: Dispatch Message Scenarios - Heart Beat Messages

IESO Action	Market Participant Response	Comment
HEARTOUT	HEARTIN	The *IESO* will send a HEARTOUT message every 60 seconds to check for an active *Market Participant* Message Exchange client. If the *IESO* does not receive the HEARTIN response from the client with a specified period of time (currently configured to 10s) the *Market Participant* client is considered out of service and the Exchange Coordinator be informed of the problem.

The following scenario table demonstrates the Based on the *bids* and *dispatch* scheduling optimizer (DSO) *dispatches* GENERIC-LT.G2 to 268MW at 2000/08/30 9:05 with the expectation that that the instruction will be met at 2000/08/30 9:10. The *dispatch Market Participant* accepts the *dispatch* and complies with the instruction.

Table 3-2: Dispatch Message Scenarios - Example of Dispatch Sent by IESO with Market Participant Response to Accept

IESO Action	Market Participant Response	Comment
ENERGY DISPATCH: RESOURCE_ID=GENERIC-LT.G2 DISPATCH_TYPE=ENG AMOUNT=268 DELIVERY_DATE=2000/08/30 DELIVERY_HOUR=10 DELIVERY_INTERVAL=2	RECEIPT	The *Market Participant* client should immediately send a RECEIPT message back to the *IESO* acknowledging that the message has been received.
	ACCEPT	The *Market Participant* client should send an ACCEPT message to inform the *IESO* that they intend to comply with the *dispatch*.
		The *IESO* receives the ACCEPT message and initiates compliance monitoring of the requested *dispatch*.
CONFIRMATIONOK		The CONFIRMATIONOK message is sent to confirm that the ACCEPT message was received and acknowledged by the *IESO*.

The following scenario table demonstrates what will happen when the participant rejects a dispatch message:

Table 3-3: Dispatch Message Scenarios - Example of IESO sends Dispatch Message and Market Participant responds Reject

IESO Action	Market Participant Response	Comment
ENERGY DISPATCH: RESOURCE_ID=GENERIC-LT.G2 DISPATCH_TYPE=ENG AMOUNT=268 DELIVERY_DATE=2000/08/30 DELIVERY_HOUR=10 DELIVERY_INTERVAL=2	RECEIPT	The *Market Participant* client should immediately send a RECEIPT message back to the *IESO* acknowledging that the message has been received.
	REJECT	The *Market Participant* should send a REJECT message to

IESO Action	Market Participant Response	Comment
		inform that they do not intend to comply with the *dispatch*.
		The Exchange Coordinator is informed that the *dispatch* was rejected.
CONFIRMATIONOK		The COMFIRMATIONOK message is sent to confirm that the REJECT message was received and acknowledged by the *IESO*.
		The Exchange Coordinator will assess the impact of the REJECT and choose alternate resources as required.
		The Exchange Coordinator will request additional information from the participant to explain the reasoning behind the REJECT of the dispatch instruction.

The following scenario table demonstrates what will happen if the *market participant* does not respond to a *dispatch* instruction:

Table 3-4: Dispatch Message Scenarios - IESO sends Dispatch Instruction and No Response made by Market Participant

IESO Action	Market Participant Response	Comment
ENERGY DISPATCH: RESOURCE_ID=GENERIC-LT.G2 DISPATCH_TYPE=ENG AMOUNT=268 DELIVERY_DATE=2000/08/30 DELIVERY_HOUR=10 DELIVERY_INTERVAL=2		The *Market Participant* client should immediately send a RECEIPT message back to the *IESO* acknowledging that the message has been received. If the RECEIPT message is not received within 20 seconds the Exchange Coordinator will be made aware of the problem.
		If a response to the *dispatch* instruction is not received within 60 seconds, the *dispatch* instruction is considered to be in a timeout state, which locks out the *Market Participant* client from further accepting or rejecting the *dispatch*

IESO Action	Market Participant Response	Comment
		instruction. If, within 30 seconds after a *dispatch* instruction has timed out, *Market Participants* call and request the *IESO* to manually accept or reject the *dispatch* instruction, the *IESO* will attempt to do so on their behalf. If, within those 30 seconds, the participants do not request the *IESO* to manually accept or reject the *dispatch* instruction, the *IESO* will consider that the participants have rejected the *dispatch* instruction.

3.2.8 Real Time Network

The Real Time Network will be used for:

a. Real time data acquisition of power system data required by the *IESO* to operate the power system;
b. *Dispatch* of *automatic generation control (AGC)* control commands; and
c. *Dispatch* messaging.

Function (a) and (b) above are typically executed by an RTU, and function (c) by a *dispatch workstation*.

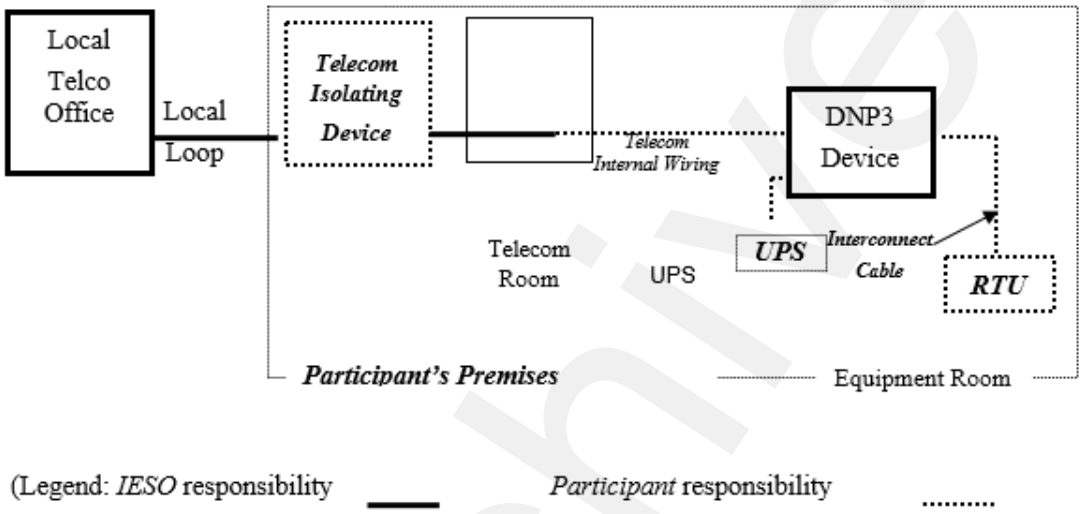
Real-time network communication with the *IESO* Control Center is typically via a MPLS communications network, but could also be via a site-to-site VPN connection over the Internet for medium performance sites. The MPLS network will be made available by the IESO to the participant, or, in the case of a medium performance site where the VPN option is preferred, the participant will provide access to the public internet. In some cases, where the size and the location of the participant's electrical plant warrants, a secondary communications system for increased reliability will also be made available.

The connection to the Real Time Network for an RTU or a functionally equivalent device e.g. PML *meter*, requires the participant to provide the following:

a. Where:
    i. MPLS access is the preferred method, physical access for the communications carrier and *IESO* to the participant site to install a local loop and other required premises equipment such as the MPLS router and a DNP3 communications device must be provided.
    Or
    ii. Where site-to-site VPN is the preferred method for a medium performance site, logical access via Internet Service Provider (ISP) to the public internet from the *IESO* network security device as well as physical access for *IESO* to install premises equipment such as a network security device and DNP3 communications device must be provided.

b. Space to house the customer premises equipment in a suitable environment (e.g. dry, clean, 0 to 40 Degrees Celsius, free of Electro-Magnetic interference, etc.)
c. A suitable power source for the customer premises equipment (typically a reliable source of 120V ac, 60 Hz – usually from a UPS with a total load capacity of 500 Watts) with at least 8 hours of survivability after loss of commercial power.
d. Access for maintenance personnel as needed.
e. Connectivity from the participant equipment to the customer premises equipment as stated for the particular device.
f. A point of contact (a person and telephone number) to enable the *IESO* to request repairs by the participant for telemetry failures.

MPLS connection diagram:



Site-to-Site VPN connection diagram:

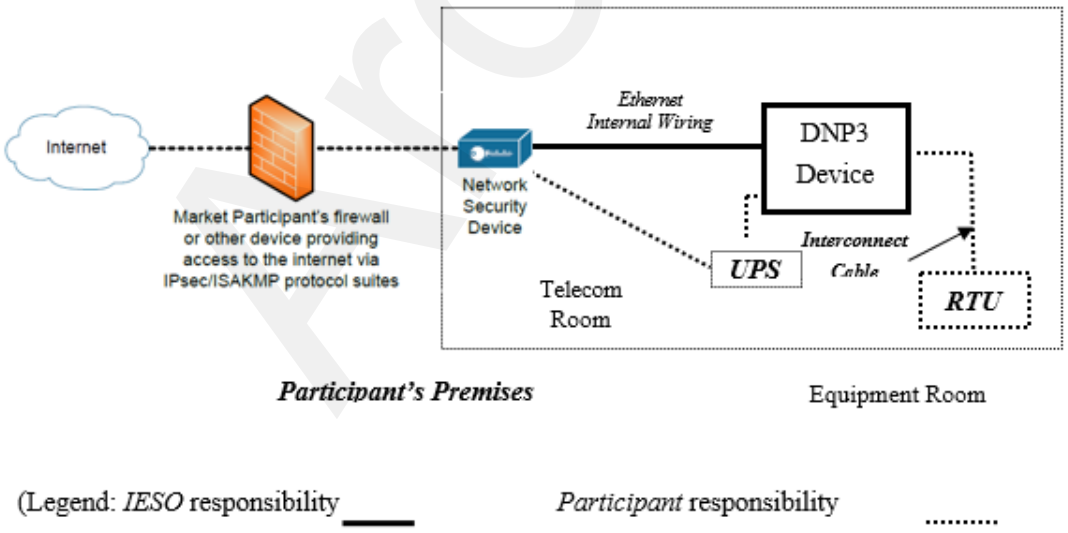


Figure 3-2: Responsibilities for Telecommunications and Site Readiness for RTUs

The connection to the Real Time Network for a dispatch workstation requires the participant to provide the following:

a. Access for the communications carrier to the participant site to install a local loop and other customer premises equipment.
b. Space to house the customer premises equipment (Router) in a suitable environment (e.g. dry, clean, 0 to 40 Degrees Celsius, free of Electro-Magnetic interference, etc.)
c. A suitable power source for the customer premises equipment, typically a reliable source of 120V ac, 60 Hz.
d. Access for maintenance personnel as needed.

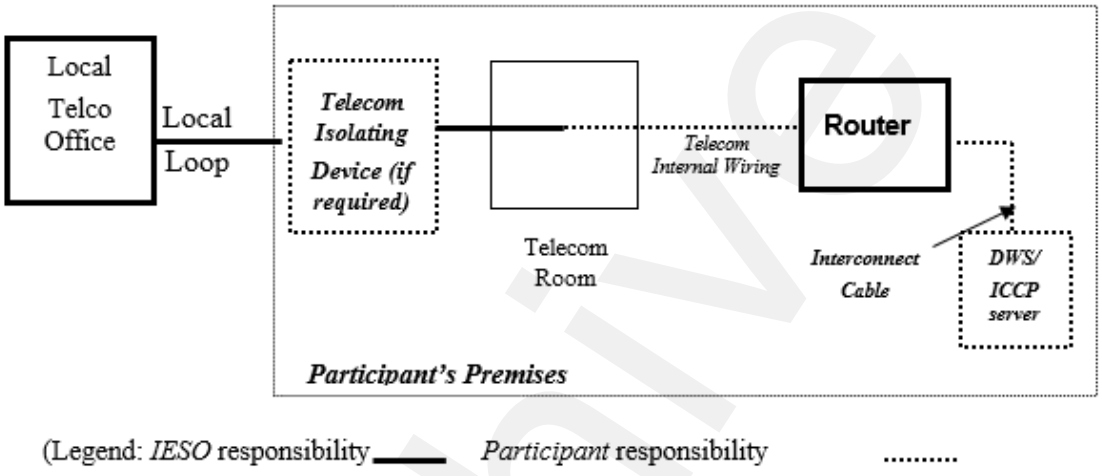


Figure 3-3: Responsibilities for Telecommunications and Site Readiness for DWS/ICCP Server

3.3 Dispatch Service

3.3.1 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).

During transitional period (Dispatch Message Exchange and Dispatch Service operate in parallel), *IESO* will be able to send dispatches for each Participant to either Dispatch Message Exchange system or Dispatch Service system.

Dispatch Service system will eventually replace Dispatch Message Exchange system.

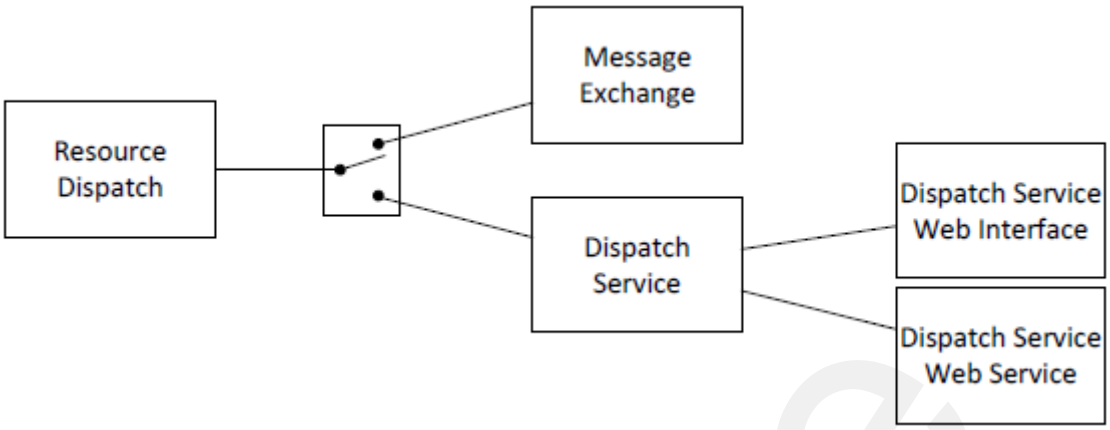


Figure 3-4: Overview of Dispatch Service System

3.3.2 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 (http://www.ieso.ca/-/media/files/ieso/document-library/training/dispatch-service-web-client-user-guide.pdf) describes the web user interface in detail.

3.3.3 Hardware and Software Requirement – Web User Interface

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

3.3.4 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.

3.3.5 Hardware and Software Requirement – Web Service

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

3.3.6 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).

3.3.7 Hardware and Software Requirement – Dispatch Notification Service

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

3.4 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.

3.4.1 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*.

3.4.2 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 'autoringdown' 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.

3.4.3 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.

3.4.4 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.

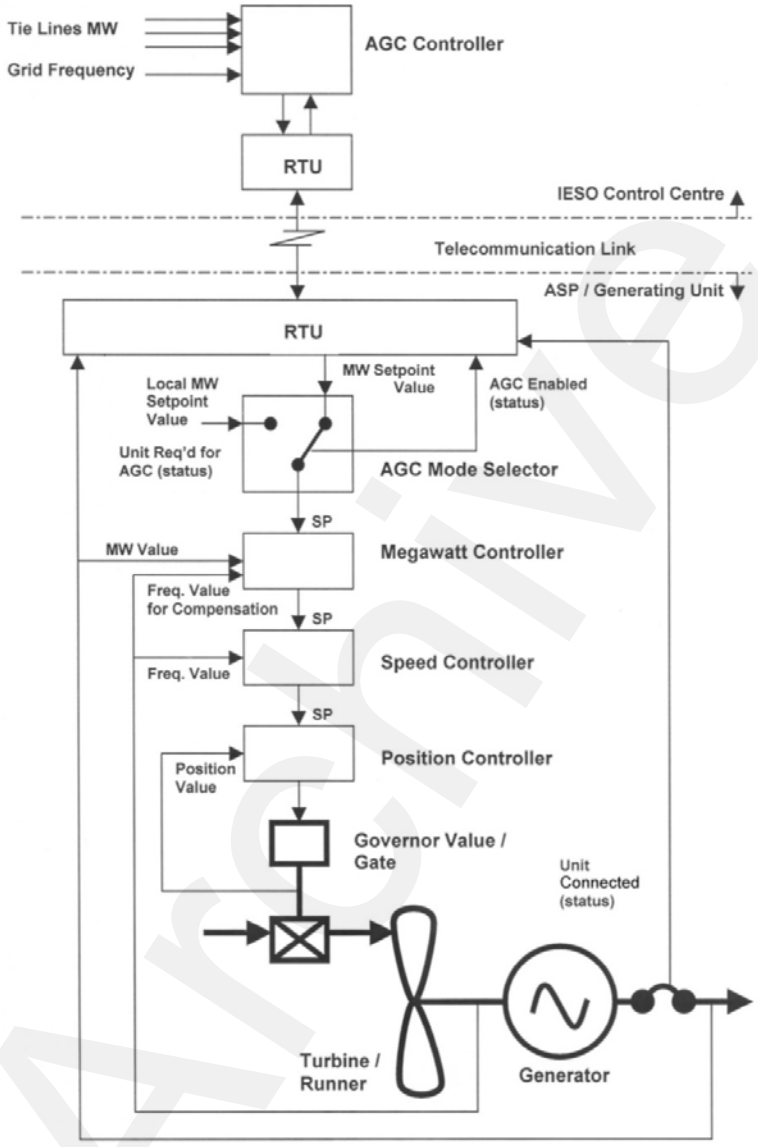


Figure 4-1: Block Diagram of Typical AGC Control Arrangement for Generation units with Remote MW Set-point Control Capability

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*.

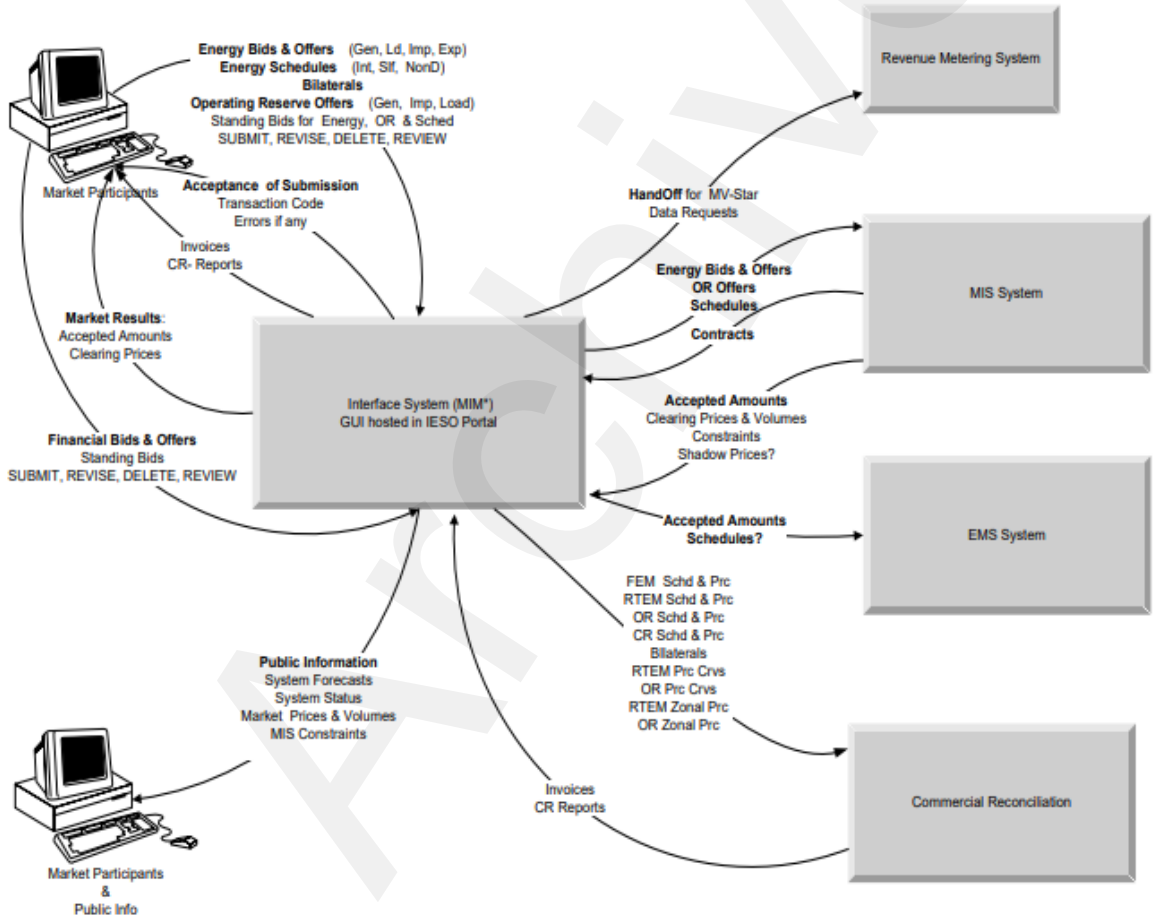


Figure 5-1: Overview of Dataflow from the Market Participant to IESO Systems

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.

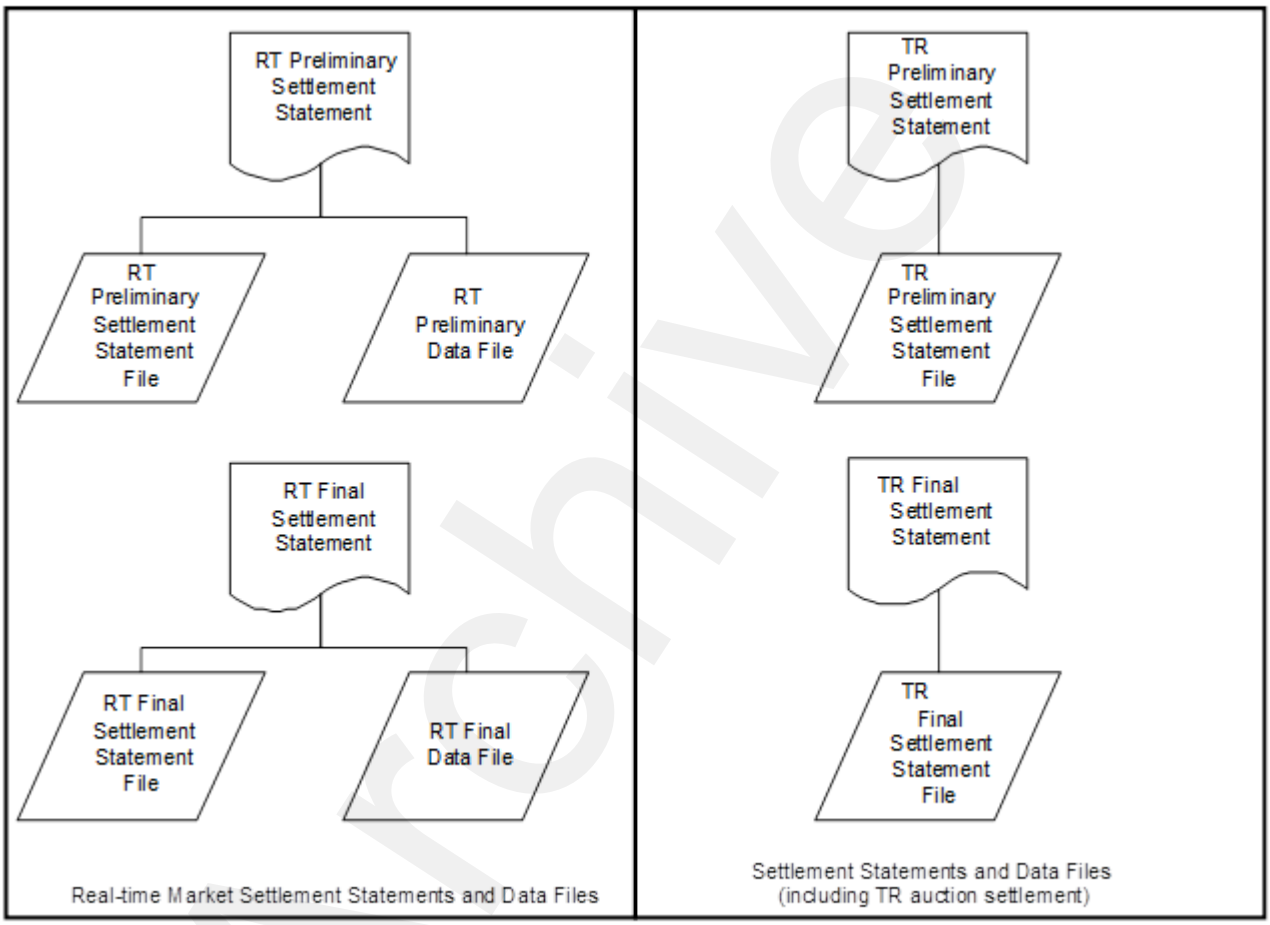


Figure 5-2: Schematic Overview for Settlement Statements and Data Files

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 Portal On-line Settlement Forms Application

Within the IESO Portal the On-line Settlement Forms application provides functionality to permit secure submission and historical search for a number of *settlement* data on-line forms. This includes but is not limited to:

- Ontario Power Generation Rebate Returned to the IESO,
- Submission of Transmission Service Charges for Embedded Generation,
- Embedded Generation and Class A Load Information.

Over time on-line *settlement* data submission forms and functionality will be updated to meet current requirements.

5.1.5 Portal Prudential Manager Application

Hosted within the IESO Portal 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.

5.1.6 Portal Transmission Rights Auction Application

The *IESO* Web based TRA application securely available via the Portal 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 must update their Portal account password every 90 Days

5.1.7 Online IESO System

The web based Online IESO system allows participants to access it using a Portal account even though it is not directly hosted by the Portal. A user logged into the Portal can click on the Online IESO System link and access it although they will have to login as SSO is not set up with 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.

The Online IESO System – Manage Meter Installation application has been added to permit management of *metering installations*.

The Online IESO System – Manage Meter Data Report Profile, Request Meter Data Report applications have been added to permit management of *meter* data reports as a replacement for MVWEB

The Online IESO System – Manage Facilities and Equipment application has been added to permit 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 replace the old workflow NOD system with equivalent and improved functionality.

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.

5.1.8 IESO Confidential Report Site

The web based Confidential Report Site allows participants to access it using a Portal account even though it is not directly hosted by the Portal. 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
Web Based Message Exchange – Market Participant's Guide	IMP_MAN_0031
IESO Reports API Guide	N/A

– End of Document –