ieso
Connecting Today.
Powering Tomorrow.

Market Manual 6

Participant Technical Reference Manual

Issue 31.0

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 *participants* and other interested visitors to the *IESO* Web site. 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 Web site 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 Web site are exact reproductions of the original documents listed. In addition, the documents and information posted on this Web site 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 31.0
Reason for Issue	Issued for baseline 36.0 for revisions due to replacement of Reliability Compliance Tool with a functionally equivalent application in the Online IESO system.
Effective Date	September 14, 2016

Document Change History

Issue	Reason for Issue	Date
For change history prior to Issue 10, see issue 17.0 of the PTRM. For change history prior to Issue 22.0, see issue 29.0 of the PTRM.		
22.0	Revised for Verizon CA Renewal May 2010 in advance of Baseline 23.1	March 26, 2010
23.0	Revised for removal of requirements for PKI certificate login for Portal Transmission Right Auction access.	June 12, 2010
24.0	Revised for update of Verizon Root CRL IP address locations	September 30, 2010
25.0	Revised for decommissioning PKI digital certificates used for MPI and MIM IDK Authentication.	June 1, 2011
26.0	Revised for Baseline 26.0	September 14, 2011
27.0	Revised in advance of Baseline 26.1 for Real Time and Participant Networks change to MPLS and alternative communications for medium performance facilities.	November 1, 2011
28.0	Revised for Baseline 27.0 in regard of need for Market Participants to register IP addresses of workstations using the MIM IDK.	March 7, 2012
29.0	Issued for Baseline 29.0. To Include new RTUs to the certified list of devices in section 4.1.2 and Revised for Baseline 30.0 to account for deployment of new *IESO* Registration System and use of Windows 7 and IE 8.0.	September 11, 2013
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

Related Documents

Document ID	Document Title
MDP_RUL_0002	Market Rules

Table of Contents

List of Figures

Table of Changes

Reference (Section and Paragraph)	Description of Change
Section 2, para 57, 95	Removed references to standalone Reliability Compliance Tool
Section 2.3.5 para 120	Removed references to standalone Reliability Compliance Tool
Section 5.1.9	Removed subsection on standalone Compliance Tool Application
Section 5.1.10	Renumbered to subsection 5.1.9 and added content regarding new Reliability Compliance Tool application within Online IESO system

1. Overview

1.1 About this Manual

1 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

2 This “Participant Technical Reference Manual” (“PTRM”) 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.

3 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”.

4 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

5 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*.

6 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, transmitters, *distributor*, *generator*, or *consumer*.

7 The material contained in various sections of the PTRM 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 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 "PTRM". Specific document references are included in each of the relevant sections of the "PTRM" as well as in the References table at the rear of the document.

1.3.1 Out of Scope

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

1.4 Limitations

9 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.

10 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" 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.

11 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

12 The "PTRM" 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*.

13 The "PTRM" 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

14 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";
- 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

15 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.

16 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/offer* 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 metering* 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.

17 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 & Security

18 (For supporting rule references, please refer to “Appendix 2.2, Section 1.4 of the *market rules*”)

2.1 Participant Workstation

19 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

20 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 7 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. At this time there are no known issues with the *IESO* Portal and the supported browsers.

21 For Windows 7.0-SP1 and above it is recommended that the client workstation hardware conform to Microsoft’s specifications found at: http://windows.microsoft.com/en-us/windows/windows-help?os=winxp#windows=windows-7.

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

Processor

22 The minimum recommended processor is an Intel I5.

Memory

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

Disk

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

Interface Cards

25 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.

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

Monitor

27 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

28 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

29 The recommended operating system is Windows 7-SP1 as shown on the *IESO* Supported Client Platform web page at :

http://www.ieso.ca/Pages/Participate/Supported-Client-Platforms.aspx

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

31 It should be note that Windows XP is no longer supported by Microsoft and the *IESO* encourages that the participants use Windows 7 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

32 All *IESO* applications within the MPI are fully tested with the *IESO* supported OS /Browser and JRE combinations. However it is recommended that participants use IE 11.0 due to end of Microsoft support for earlier browser versions.

33 128-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, Enable SSL 3.0 and Disable Enhance Protected Mode.

d. Save the changes by clicking Apply and OK.

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

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

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

37 The *IESO* Portal is accessible with Internet Explorer 8.0, 9.0, 11.0 as well as Mozilla Firefox 2.x, 3.x or Safari 2.x & 3.x (on Windows 7-SP1). These specifications are 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.

Portal On-line Outage Request Forms and Prudential Manager Browser configuration

38 The Portal Online Outage Request Forms and Prudential Manager applications have the following requirements:

39 Screen resolution of 1024 X 768 or higher

40 Internet Explorer version 11.0 with Compatibility View setting updated to include ieso.ca to the website list. IE 8.0 and 9.0 will work but are not supported.

41 Internet Explorer native XMLHTTP enabled

42 Internet Explorer pop-up blocker configured to allow pop-ups from *IESO* secure sites

Firewall

43 It is recommended that the 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

44 The *IESO* has implemented a new confidential report site... The production URL for the confidential report repository HTTPS site is: https://reports.ieso.ca/private/. The sandbox URL for the confidential report repository HTTPS site is: http://reports-sandbox.ieso.ca/.

45 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.

46 An explanation and of the access interfaces for the new confidential report site can be found at: http://www.ieso.ca/Documents/ti/API_Guide/IESO_Reports_API_Guide.pdf

Microsoft Internet Explorer Configuration for Portal and Online IESO

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

- *IESO* Energy Market Application
- Transmission Rights Auction
- On-line Settlement Forms
- On-line Outage Forms
- Prudential Manager
- Various Collaboration initiatives - 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 and Demand Response Auction applications

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

- Registration - for market participants, contacts and user accounts
- Metering Installation Registration (new)
- Facility/Equipment Registration (new)
- Meter Trouble Reporting application (replaces old MTR system)
- Notice of Disagreement application (replaces old NOD system)
- Demand Response Auction application (new)

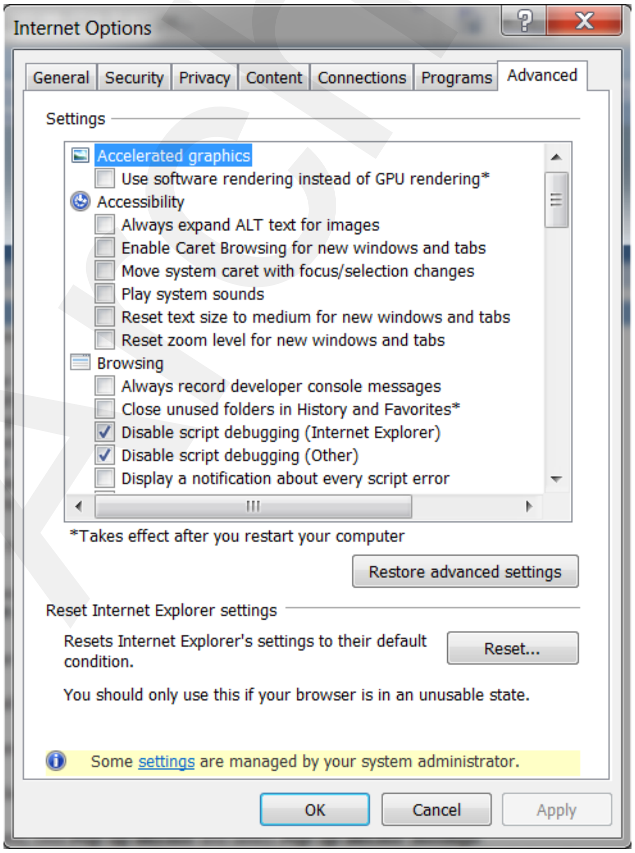
49 For the supported versions of Microsoft Internet Explorer to work properly with the Portal and Online IESO there are a number of configuration settings that need to be made. This includes configuration items in both the Advanced and Security tabs under Internet Options menu selection in Internet Explorer. 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. It is also important to recognize that Internet Explorer has differences in configuration settings between Internet Explorer 8.0, Internet Explorer 9.0 and Internet Explorer 11.0 under Windows 7.

50 Under Windows 7, Internet Explorer 8.0, 9.0 and 11.0 use the Protected Mode capability for the various security zones as described at: http://msdn2.microsoft.com/en-us/library/bb250462.aspx. The recommendation is to put the Portal and *IESO* corporate web site URL's into the 'Trusted sites' zone when using Windows 7 and turn off Protected Mode for this zone only., Windows 7 and above enforces the opening of a new browser window every time the security zone changes

Internet Options - Advanced

51 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 / Win**dows** 7.0 shown)



Settings

Accelerated graphics
- □ Use software rendering instead of GPU rendering*

Accessibility
- □ Always expand ALT text for images
- □ Enable Caret Browsing for new windows and tabs
- □ Move system caret with focus/selection changes
- □ Play system sounds
- □ Reset text size to medium for new windows and tabs
- □ Reset zoom level for new windows and tabs

Browsing
- □ Always record developer console messages
- □ Close unused folders in History and Favorites*
- ☑ Disable script debugging (Internet Explorer)
- ☑ Disable script debugging (Other)
- □ Display a notification about every script error

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Some settings are managed by your system administrator.

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

3. 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 : Internet Explorer *Adv*anced Internet Options with Windows 7 SP1

Adv*anc*ed Internet Option Parameter		**IE 8.0 – Windows 7 and above**	**IE 9.0 – Windows 7 and above**	**IE 11.0 – Windows 7 and above**
Accelerated graphics				
User software rendering instead of GPU rendering	N/A	N/A	N/A	No stipulation
Accessibility Parameters – all				
Always expand ALT text for images		No stipulation	No stipulation	No stipulation
Move system caret with focus/selection changes		No stipulation	No stipulation	No stipulation
Play system sounds		N/A	N/A	No stipulation
Reset text size to medium for new windows and tabs		No stipulation	No stipulation	No stipulation
Reset text size to medium while zooming		No stipulation	No stipulation	No stipulation
Reset Zoom level for new windows and tabs		No stipulation	No stipulation	No stipulation
Browsing Parameters				
Always record developer console messages		No stipulation	No stipulation	No stipulation
Close unused folders in History and Favorites		No stipulation	No stipulation	No stipulation
Disable script debugging (Internet Explorer)		No stipulation	No stipulation	No stipulation
Disable script debugging (Other)		No stipulation	No stipulation	No stipulation
Display a notification about every script error		No stipulation	No stipulation	No stipulation
Enable automatic crash recovery (* requires restart)		✓	✓	✓
Enable FTP folder view (outside of Internet Explorer)		✓	✓	✓
Enable Suggested Sites		No stipulation	No stipulation	No stipulation
Enable page transitions		No stipulation	No stipulation	N/A
Enable Personalized		No	No stipulation	N/A

Adv*anc*ed Internet Option Parameter		**IE 8.0 – Windows 7 and above**	**IE 9.0 – Windows 7 and above**	**IE 11.0 – Windows 7 and above**
Favorites menu		stipulation		
Enable third-party browser extensions *(requires restart)		✓	✓	✓
Enable visual styles on buttons and controls in web pages		✓	✓	✓
Go to an intranet site for a single word entry in the address bar		N/A	N/A	No stipulation
Load sites and content in the background to optimize performance		N/A	N/A	✓
Notify when downloads complete		No stipulation	No stipulation	✓
Reuse windows when launching shortcuts		No stipulation	No stipulation	N/A
Show friendly HTTP error messages		✓	✓	✓
Underline links		Always	Always	Always
Use inline AutoComplete in File Explorer and Run Dialog		N/A	N/A	No stipulation
Use inline AutoComplete in the Internet Explorer Address bar and Open Dialog		No stipulation	No stipulation	No stipulation
Use most recent order when switching tabs with Ctrl+Tab		No stipulation	No stipulation	No stipulation
Use Passive FTP (for firewall and DSL modem compatibility)		No stipulation	No stipulation	No stipulation
Use smooth scrolling		✓	✓	✓
HTTP 1.1 Settings				
Use HTTP 1.1		✓	✓	✓
Use HTTP 1.1 through proxy connections		No stipulation	No stipulation	✓
International				

Adv*anc*ed Internet Option Parameter		**IE 8.0 – Windows 7 and above**	**IE 9.0 – Windows 7 and above**	**IE 11.0 – Windows 7 and above**
Always show encoded addresses		No stipulation	No stipulation	No stipulation
Send IDN Server Names for Intranet addresses		No stipulation	No stipulation	No stipulation
Send IDN server names for non-Intranet addresses		No stipulation	No stipulation	✓
Send URL path as UTF-8		No stipulation	No stipulation	No stipulation
Send UTF-8 query strings for Intranet URLs		N/A	N/A	No stipulation
Send UTF-8 query strings for non-Intranet URLs		N/A	N/A	No stipulation
Show Information Bar for encoded addresses		No stipulation	No stipulation	No stipulation
Use UTF-8 for mailto links		No stipulation	No stipulation	N/A
Microsoft VM				
Java Console enabled		N/A	N/A	N/A
Java logging enabled		N/A	N/A	N/A
JIT compiler for virtual machine enabled		N/A	N/A	N/A
Multimedia				
Enable alternative codecs in HTML5 media elements * (requires restart)		N/A	N/A	✓
Enable automatic image resizing		✓	✓	✓
Play animations in web pages * (requires restart)		No stipulation	No stipulation	✓
Play sounds in web pages		No stipulation	No stipulation	✓
Play videos in web pages		N/A	N/A	✓
Show image download placeholders		No stipulation	No stipulation	✓
Show pictures		No stipulation	No stipulation	✓
Show image dithering		No stipulation	No stipulation	N/A

Adv*anc*ed Internet Option Parameter		**IE 8.0 – Windows 7 and above**	**IE 9.0 – Windows 7 and above**	**IE 11.0 – Windows 7 and above**
Printing				
Print backgrounds colors and images		No stipulation	No stipulation	N/A
Search from the Address bar		No stipulation	No stipulation	N/A
Security				
Allow active content from CD to run on My Computer * (requires restart)		No stipulation	No stipulation	No stipulation
Allow active content to run in files on My Computer		No stipulation	No stipulation	No stipulation
Allow software to run or install even if the signature is invalid		No stipulation	No stipulation	No stipulation
Block unsecured images with other mixed content		N/A	N/A	No stipulation
Check for Publishers certificate revocation		✓	✓	✓
Check for server certificate revocation * (requires restart)		✓	✓	✓
Check for signatures on downloaded programs		✓	✓	✓
Do not save encrypted pages to disk		No stipulation	No stipulation	No stipulation
Empty Temporary Internet Files folder when browser is closed		No stipulation	No stipulation	No stipulation
Enable DOM storage		N/A	N/A	No stipulation
Enable Enhanced Protected Mode * (requires restart)		N/A	N/A	No stipulation
Enable Integrated Windows Authentication * (requires restart)		No stipulation	No stipulation	No stipulation
Enable memory protection to help mitigate online attacks		No stipulation	No stipulation	N/A
Enable native XMLHTTP support		✓	✓	✓

Advanced Internet Option Parameter		**IE 8.0 – Windows 7 and above**	**IE 9.0 – Windows 7 and above**	**IE 11.0 – Windows 7 and above**
Phishing Filter		Turn on automatic website checking	Turn on automatic website checking	N/A
Enable SmartScreen filter		N/A	N/A	✓
Enable Strict P3P Validation * (requires restart		N/A	N/A	No stipulation
Send do not track requests to sites you visit in Internet Explorer * (requires restart)		N/A	N/A	No stipulation
Use SSL 2.0				
Use SSL 3.0				
Use TLS 1.0		✓	✓	No stipulation
Use TLS 1.1		✓	✓	✓
Use TLS 1.2		✓	✓	✓
Warn about invalid site certificates		✓	✓	N/A
Warn about certificate address match * (requires restart)		N/A	N/A	✓
Warn if changing between secure and not secure mode		✓	✓	✓
Warn if Post submittal is redirected to a zone that does not permit posts		✓	✓	✓

Note: Even though IE8.0 and 9.0 will work, the IESO is no longer supporting those versions. The settings above are for reference only.

Internet Explorer - Internet Options - Security

52 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 7 is important that the URLs be placed in the ‘Trusted sites’ zone as well as the *IESO* corporate site as discussed previously.

53 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.

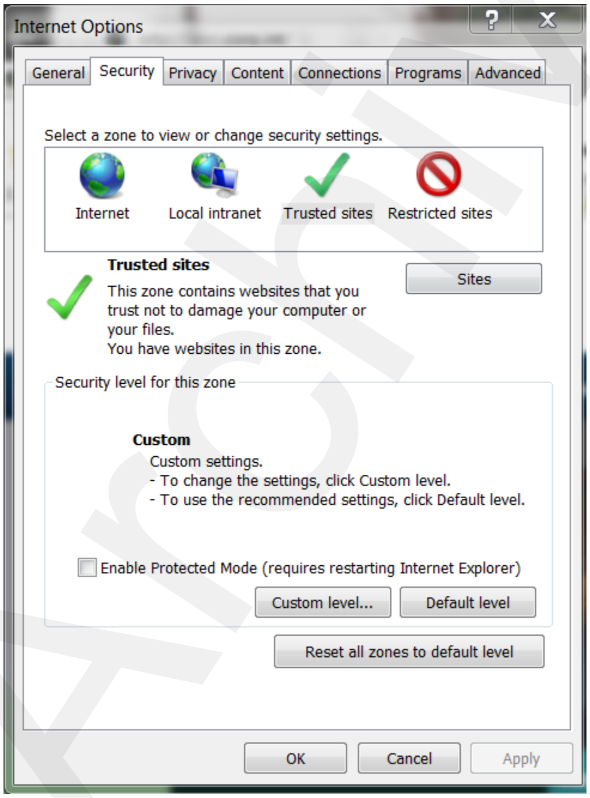
54 However the *participant's* IT security people should be involved in deciding the appropriate settings and implement based on their own rules and policies, which may take precedence over the settings recommended here. The choice is in the end, up to each *participant.*

Internet Zone Security Settings

55 When leaving the *IESO* Portal URLs by default in the IE 'Internet' zone for Windows 7 it is recommended the following settings be made:

1. Under the **Tools** menu select **Internet Options**

Select the **Security** tab. See Figure 2-2 (IE 11 / Windows 7 shown). For Windows *7* 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 7 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.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Sites

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

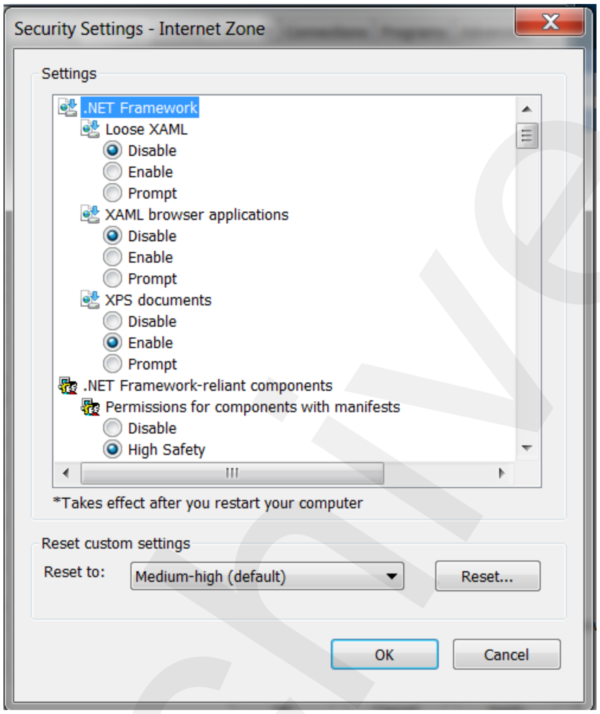
Reset all zones to default level

OK | Cancel | Apply

Figure 2-2: Internet Explorer 11.0, Internet Options - Security - Windows 7

2. 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.
3. Click on the 'Custom Level' button to activate the Security Settings configuration window. See Figure 2-3. (IE 11 / Windows 7 shown)

4. 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.
5. Click on the "OK" button to accept all changes.



Security Settings - Internet Zone

Settings

.NET Framework
  Loose XAML
    ● Disable
    ○ Enable
    ○ Prompt
  XAML browser applications
    ● Disable
    ○ Enable
    ○ Prompt
  XPS documents
    ○ Disable
    ● Enable
    ○ Prompt
.NET Framework-reliant components
  Permissions for components with manifests
    ○ Disable
    ● High Safety

*Takes effect after you restart your computer

Reset custom settings

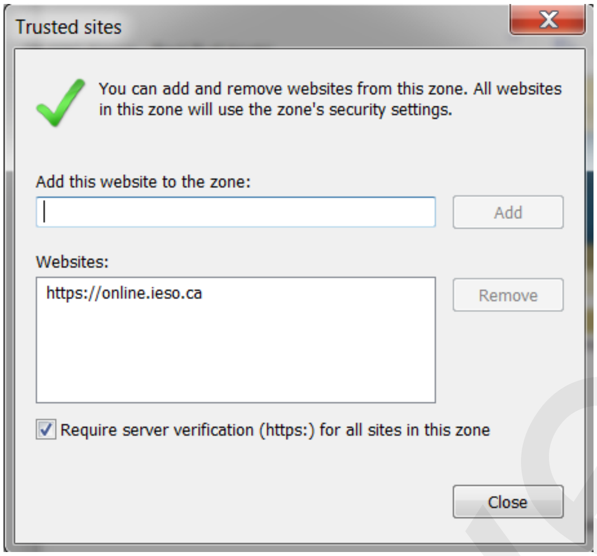
Reset to: Medium-high (default)

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

Trusted Sites Security Settings

56 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 to 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 7. It is recommended to leave as default for Windows 7. Notice that the **'Sites'** button is now active.
4. Click on the **'Sites'** button to activate the 'Trusted Sites' entry window. See Figure 2-5
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 Figure 2-5 and 2-6. Note that the production Online IESO system has already been added.



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

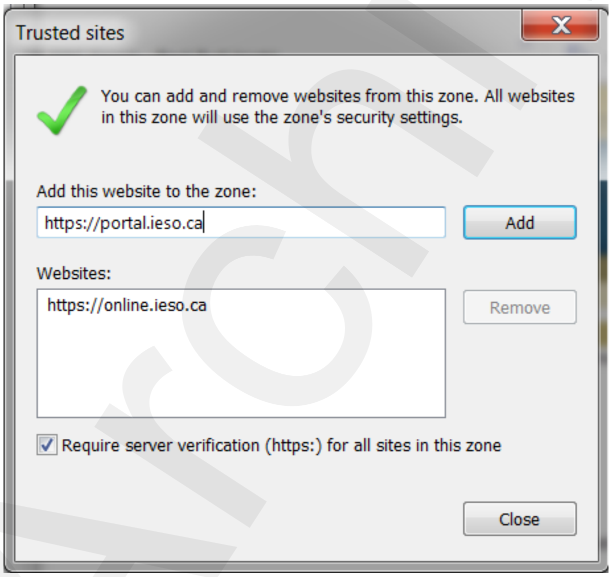
Add this website to the zone:

Websites:

https://online.ieso.ca

☑ Require server verification (https:) for all sites in this zone

Figure 2-4: Internet Explorer 11.0, Internet Options - Trusted Sites Security –Windows 7



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

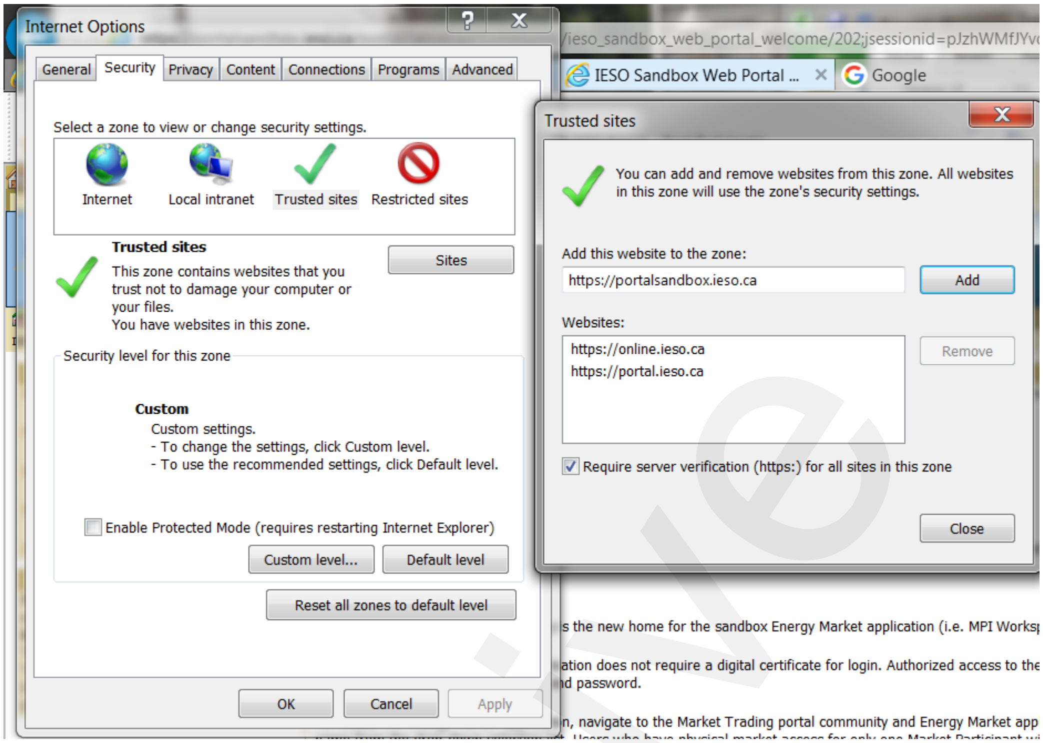
https://portal.ieso.ca

Websites:

https://online.ieso.ca

☑ Require server verification (https:) for all sites in this zone

Figure 2-5: Internet Explorer 11.0, Trusted Sites Security - Web Sites Addition -Windows 7



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Select a zone to view or change security settings.

Internet | Local intranet | Trusted sites | Restricted sites

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

Sites

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

Custom level... | Default level

Reset all zones to default level

OK | Cancel | Apply

/ieso_sandbox_web_portal_welcome/202;jsessionid=pJzhWMfJYv

IESO Sandbox Web Portal ... | Google

Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:
https://portalsandbox.ieso.ca
Add

Websites:
https://online.ieso.ca
https://portal.ieso.ca
Remove

☑ Require server verification (https:) for all sites in this zone

Close

s the new home for the sandbox Energy Market application (i.e. MPI Works

ation does not require a digital certificate for login. Authorized access to the
d password.

n, navigate to the Market Trading portal community and Energy Market app

Figure 2-6: Internet Explorer 11.0, Trusted Sites Security - Web Sites Addition –Windows 7

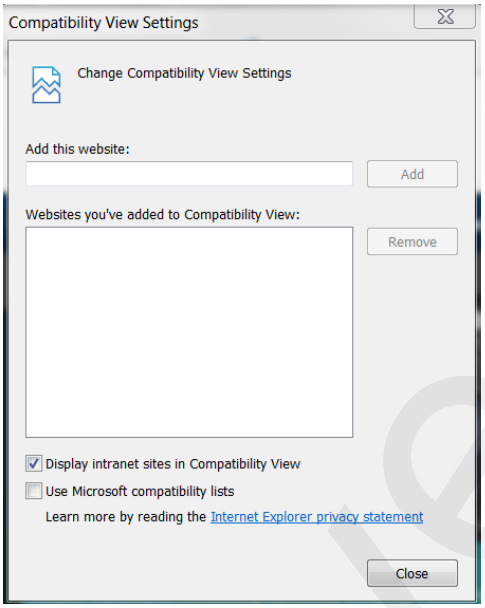
6. Click on the "Require Server Verification (https) for all sites in this zone" option check flag if all sites entered here are https sites like the *IESO*'s Portal.
7. Click on the 'OK' button.
8. Click on the 'Custom Level' button to activate the Security Settings configuration window.
9. Verify settings 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

57 When including any of the *IESO* Portal, portalapps (i.e. On-line Outage Forms, 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.


Compatibility View Settings
Change Compatibility View Settings
Add
Remove
Close

Add this website:

Websites you've added to Compatibility View:

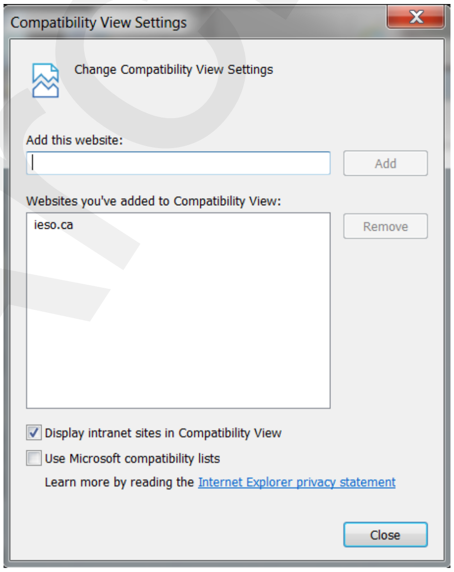
☑ Display intranet sites in Compatibility View

□ Use Microsoft compatibility lists

Learn more by reading the Internet Explorer privacy statement

Figure 2-7: Internet Explorer Compatibility View Settings

2. Type in the URL of the website to add and click the add button. The domain of the website will be added to the list. For example if https://portal.ieso.ca is typed in 'ieso.ca' will be added. It is similar for any other *IESO* secure website.
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 websites can be added as needed by the *participant*.


Compatibility View Settings
Change Compatibility View Settings
Add
Remove
Close

Add this website:

Websites you've added to Compatibility View:

ieso.ca

☑ Display intranet sites in Compatibility View

□ Use Microsoft compatibility lists

Learn more by reading the Internet Explorer privacy statement

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

Table 2-2: IE Internet Options, Security Settings –Windows 7-SP1

Parameter		**When Portal and other *IESO* URLs added to 'Trusted Sites' zone in Windows 7-SP1 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
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
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		
Logon		Automatic logon only in Intranet zone

Internet Explorer Pop-up Blocker with Windows 7-SP1 and the Portal

58 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.

59 This functionality continues as is with Internet Explorer 11.0 under Windows 7. The directions included here apply to all the combinations of Windows 7 and IE 11.0.

Internet Explorer Turn Pop-up Blocker On or Off

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

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.

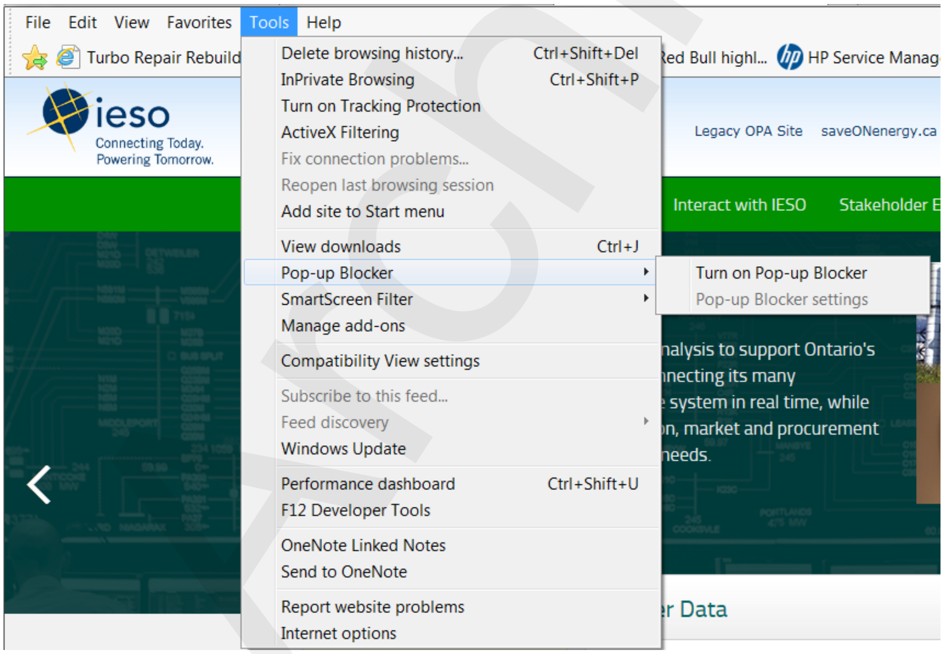


Figure 2-9: Internet Explorer, Enabling or Disabling Pop-up Blocker

Internet Explorer Configure Pop-up Blocker Settings

61 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:

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.

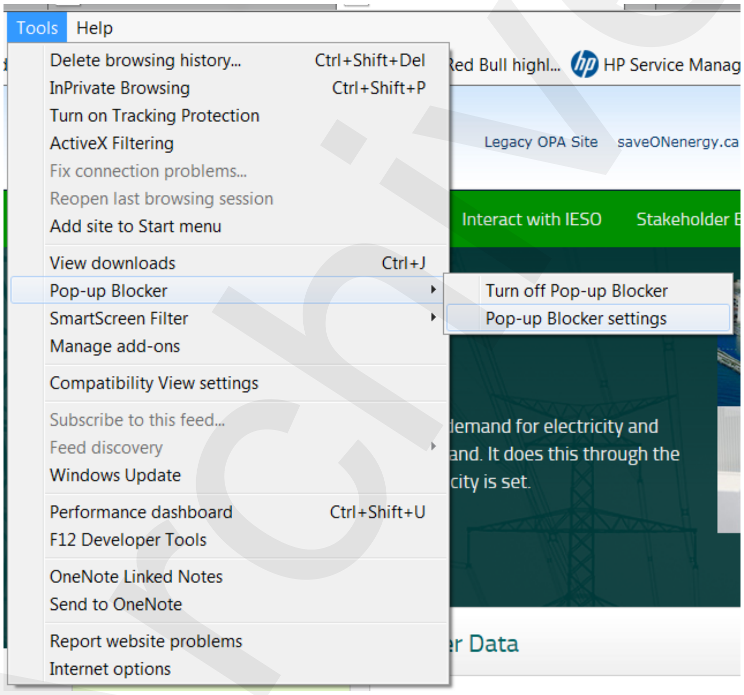
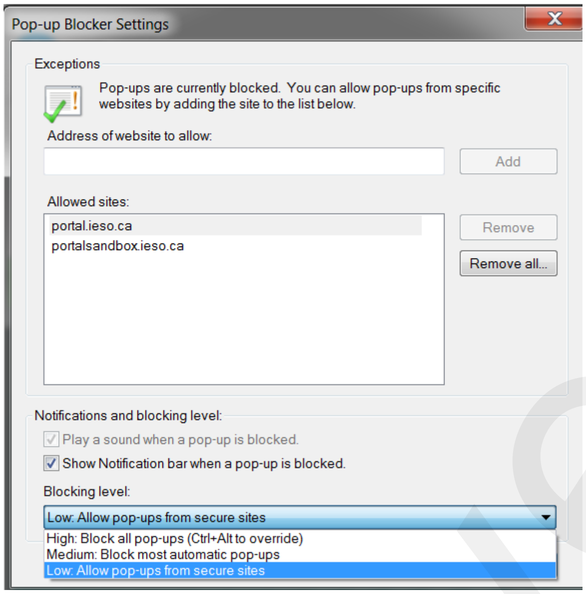


Figure 2-10: Internet Explorer, Activating Pop-up Blocker Settings



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.

Address of website to allow:

Allowed sites:

portal.ieso.ca
portalsandbox.ieso.ca

Notifications and blocking level:

☑ Play a sound when a pop-up is blocked.

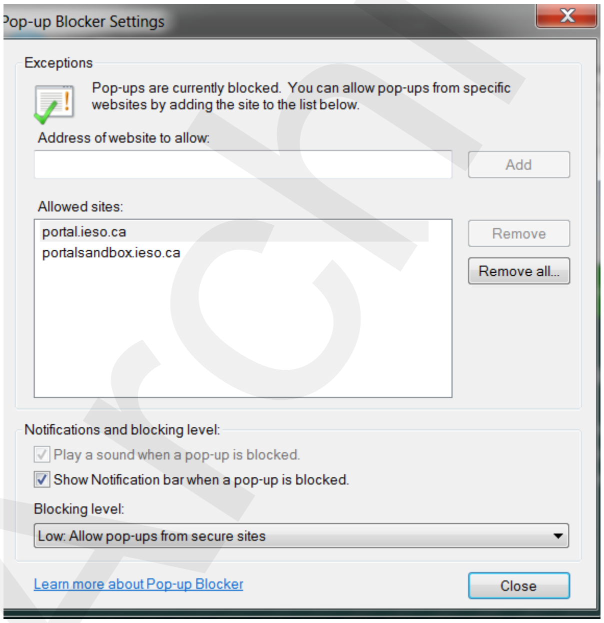
☑ Show Notification bar when a pop-up is blocked.

Blocking level:

Low: Allow pop-ups from secure sites

High: Block all pop-ups (Ctrl+Alt to override)
Medium: Block most automatic pop-ups
Low: Allow pop-ups from secure sites

Figure 2-11: Pop-up Blocker Settings Window Filter Setting for Portal & Energy Market Application Use



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.

Address of website to allow:

Allowed sites:

portal.ieso.ca
portalsandbox.ieso.ca

Notifications and blocking level:

☑ Play a sound when a pop-up is blocked.

☑ Show Notification bar when a pop-up is blocked.

Blocking level:

Low: Allow pop-ups from secure sites

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

Java Runtime Environment

62 Please refer to the *IESO* Supported Client Platform web page for the required Java runtime environment. Obtaining this software from the Oracle - Java web site and its installation on the workstation is detailed in the *Identity Management Operations Guide*. It does not need to be set as the default for the browser however in either the Java control panel or IE Internet Options.

63 Only a user with administrative rights may be able to set the default use of the JRE Plug-in with IE or not.

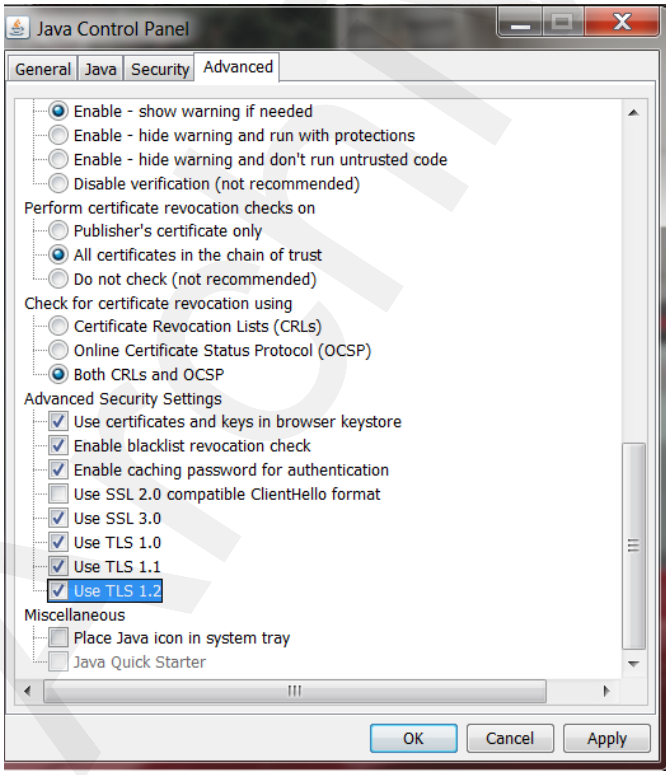
64 The JRE should be installed on the workstation properly configured to enable the Energy Market Application’s applets to function when the user accesses them in the Portal with Internet Explorer. These can be checked under the Java control panel.

65 Ensure the setting ‘Place Java icon in system tray’ is checked in the Java control panel. This will allow access to the Java console via the right mouse button.

66 Ensure that ‘Enable logging’ is checked under Debugging in the Java control panel.

67 Ensure that ‘Hide console’ is checked under Java Console in the Java control panel. This will prevent the Java console from always activating when a user navigates to the Energy Market application in the Portal when using Internet Explorer.

68 Ensure that Use SSL 3.0 and use TLS 1.0 are checked under Security in the Java control panel and in Internet Option in IE. See Figure 2-13 below. The participant may choose to check TLS 1.1 and 1.2 as well where applicable. If SSL 3.0 is not checked, a Java general exception error happens when the user navigates to the Portal to access the Energy Market Application with Internet Explorer.



● Enable - show warning if needed
○ Enable - hide warning and run with protections
○ Enable - hide warning and don't run untrusted code
○ Disable verification (not recommended)

Perform certificate revocation checks on
○ Publisher's certificate only
● All certificates in the chain of trust
○ Do not check (not recommended)

Check for certificate revocation using
○ Certificate Revocation Lists (CRLs)
○ Online Certificate Status Protocol (OCSP)
● Both CRLs and OCSP

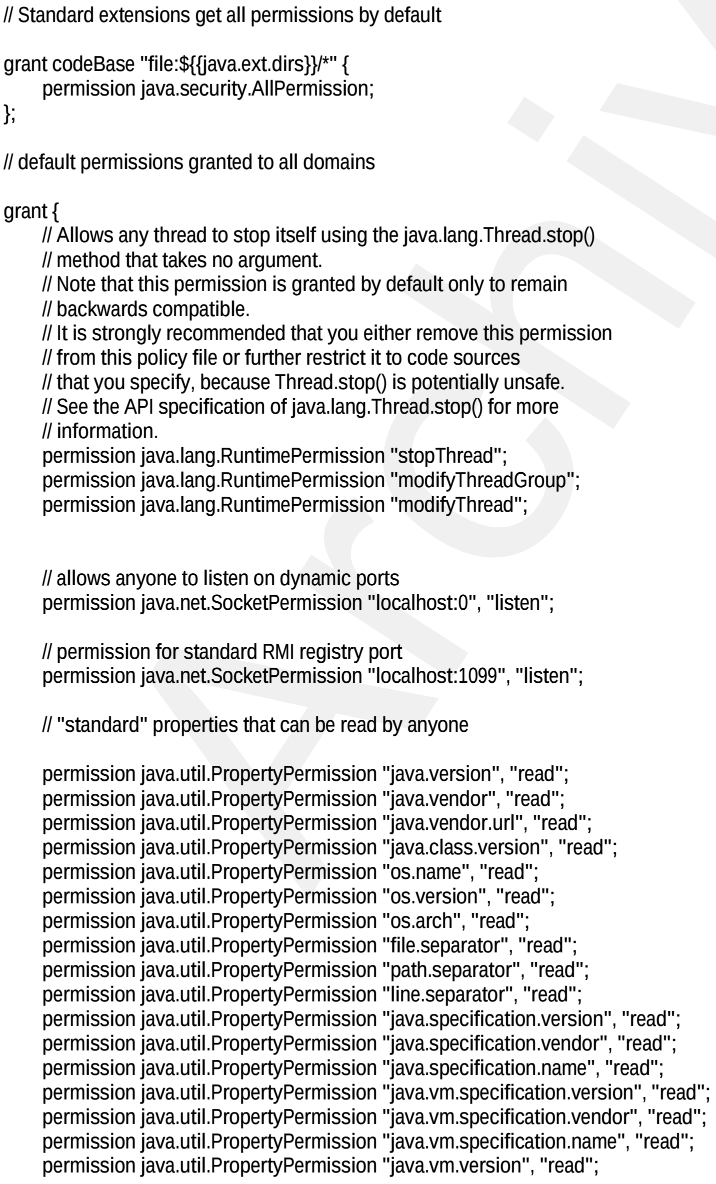
Advanced Security Settings
☑ Use certificates and keys in browser keystore
☑ Enable blacklist revocation check
☑ Enable caching password for authentication
□ Use SSL 2.0 compatible ClientHello format
☑ Use SSL 3.0
☑ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2

Miscellaneous
□ Place Java icon in system tray
□ Java Quick Starter

Figure 2-13: Java Control Panel Settings

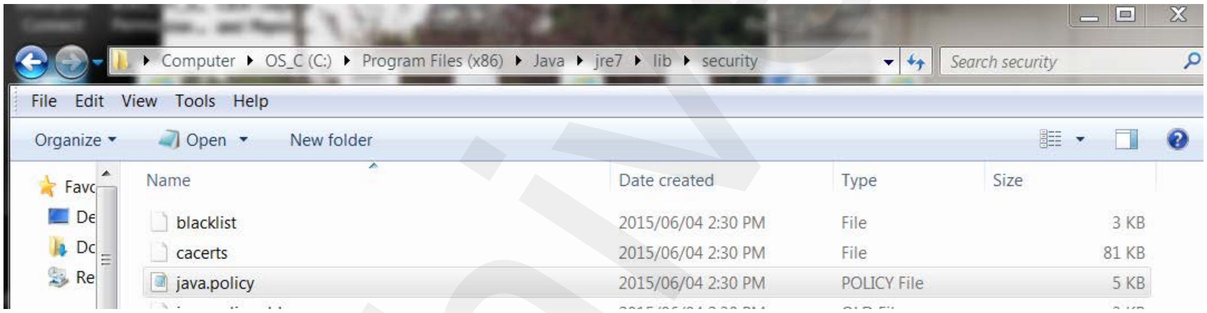
IESO Java Policy File

69 An edited Java policy file which will replace the default Oracle java install one with the file name “**java.policy**” contains additional security settings needed for the Energy Market application and Portal Collaboration file upload functionality when using Java 1.7.0_51 and above. The previous “**.java.policy**” file provided was located in the User’s home directory and is no longer valid and will not work with the recommended version of java as Oracle has made significant changes to java security. The edited java.policy file must be installed on a user’s workstation in the **C:\Program Files (x86)\Java\jre7\lib\security** location to replace the existing one for securing the Energy Market application and Portal Collaboration file upload as shown below in Figure 2.14. This is a simple text-format file available from the *IESO* Technical Interfaces page. The edited **java.policy** file for use with the Energy Market Application in the Portal should have the following content for java permissions:



```
// Standard extensions get all permissions by default

grant codeBase "file:${{java.ext.dirs}}/*" {
      permission java.security.AllPermission;
};

// default permissions granted to all domains

grant {
      // Allows any thread to stop itself using the java.lang.Thread.stop()
      // method that takes no argument.
      // Note that this permission is granted by default only to remain
      // backwards compatible.
      // It is strongly recommended that you either remove this permission
      // from this policy file or further restrict it to code sources
      // that you specify, because Thread.stop() is potentially unsafe.
      // See the API specification of java.lang.Thread.stop() for more
      // information.
      permission java.lang.RuntimePermission "stopThread";
      permission java.lang.RuntimePermission "modifyThreadGroup";
      permission java.lang.RuntimePermission "modifyThread";


      // allows anyone to listen on dynamic ports
      permission java.net.SocketPermission "localhost:0", "listen";

      // permission for standard RMI registry port
      permission java.net.SocketPermission "localhost:1099", "listen";

      // "standard" properties that can be read by anyone

      permission java.util.PropertyPermission "java.version", "read";
      permission java.util.PropertyPermission "java.vendor", "read";
      permission java.util.PropertyPermission "java.vendor.url", "read";
      permission java.util.PropertyPermission "java.class.version", "read";
      permission java.util.PropertyPermission "os.name", "read";
      permission java.util.PropertyPermission "os.version", "read";
      permission java.util.PropertyPermission "os.arch", "read";
      permission java.util.PropertyPermission "file.separator", "read";
      permission java.util.PropertyPermission "path.separator", "read";
      permission java.util.PropertyPermission "line.separator", "read";
      permission java.util.PropertyPermission "java.specification.version", "read";
      permission java.util.PropertyPermission "java.specification.vendor", "read";
      permission java.util.PropertyPermission "java.specification.name", "read";
      permission java.util.PropertyPermission "java.vm.specification.version", "read";
      permission java.util.PropertyPermission "java.vm.specification.vendor", "read";
      permission java.util.PropertyPermission "java.vm.specification.name", "read";
      permission java.util.PropertyPermission "java.vm.version", "read";
```

```
    permission java.util.PropertyPermission "java.vm.vendor", "read";
    permission java.util.PropertyPermission "java.vm.name", "read";
    permission java.lang.RuntimePermission "getProtectionDomain";
    permission java.security.SecurityPermission "removeProvider.IAIK";
    permission java.security.SecurityPermission "insertProvider.IAIK";
    permission java.security.SecurityPermission "putProviderProperty.IAIK";
    permission java.security.SecurityPermission "removeProvider.Entrust";
    permission java.security.SecurityPermission "insertProvider.Entrust";
    permission java.security.SecurityPermission "putProviderProperty.Entrust";
    permission java.io.FilePermission "<<ALL FILES>>", "read, write";
    permission java.util.PropertyPermission "*", "read, write";
    permission java.lang.RuntimePermission "queuePrintJob";
    permission com.sun.deploy.security.SecureCookiePermission "origin.https://portal.ieso.ca:443",
        "listen,accept,read,connect,modify,resolve";
    permission com.sun.deploy.security.SecureCookiePermission "origin.https://portalsandbox.ieso.ca:443",
        "listen,accept,read,connect,modify,resolve";
    permission java.net.SocketPermission "142.9.3.121:443", "connect,accept,resolve";
    permission java.net.SocketPermission "142.9.6.121:443", "connect,accept,resolve";

};
```

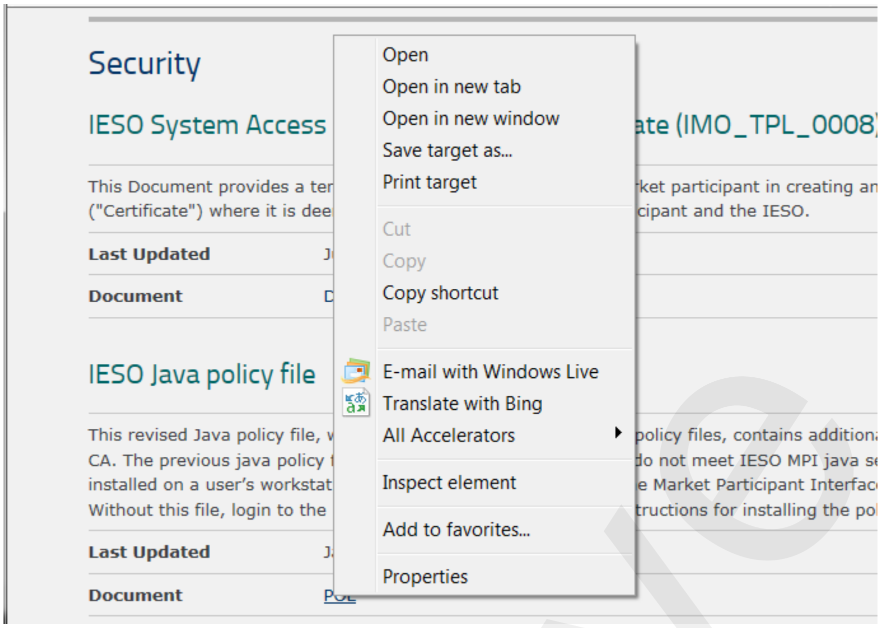

Computer ▸ OS_C (C:) ▸ Program Files (x86) ▸ Java ▸ jre7 ▸ lib ▸ security
Search security
File
Edit
View
Tools
Help
Organize
Open
New folder
Favo
De
Dc
Re

Name	Date created	Type	Size
blacklist	2015/06/04 2:30 PM	File	3 KB
cacerts	2015/06/04 2:30 PM	File	81 KB
java.policy	2015/06/04 2:30 PM	POLICY File	5 KB

Figure 2-14: Location of Java Policy File

Without the edits to the java policy file with the above content in the directory location shown, the Energy Market Application applet java code will not function correctly and multiple file upload capability with Portal Collaboration will fail. Under such circumstances an "***applet not inited***" error on the browser status line at the bottom may display and/or a dialogue box with an error message with the content **"(java.security.SecurityPermission removeProvider.IAIK)"** or others and uploading of multiple files to the *IESO* Collaboration communities will not work.

70 To download the file from the Technical Interfaces page (http://www.ieso.ca/Pages/Participate/Technical-Interfaces.aspx#) the user can use the right mouse button /cursor click on the file's POL link on the web-site and choose to save to the required location as shown in Figure 2-15. This will activate the typical Windows "Save As" window to allow the user to choose the directory location to save the file to.


Security

IESO System Access ate (IMO_TPL_0008)

This Document provides a ter ket participant in creating an
("Certificate") where it is dee cipant and the IESO.

Last Updated	J
Document	D

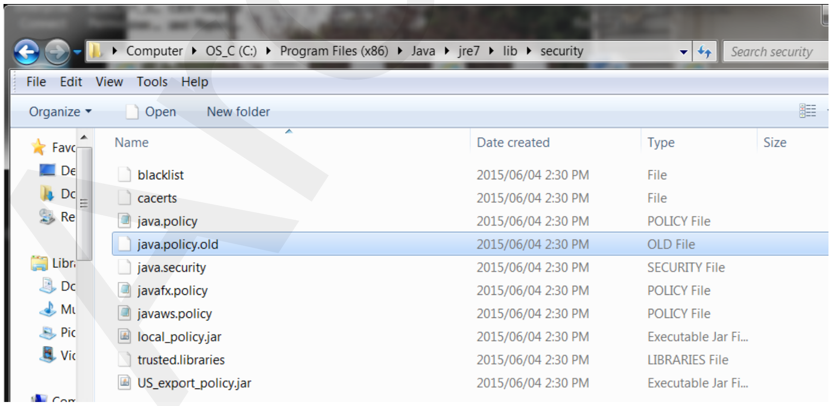
IESO Java policy file

This revised Java policy file, v policy files, contains addition
CA. The previous java policy do not meet IESO MPI java se
installed on a user's workstat e Market Participant Interfac
Without this file, login to the tructions for installing the po

Last Updated	J
Document	PDF

Figure 2-15: Right Mouse Button 'Save Target as ..." Function to Download Java Policy File

71 To download the file, the user must choose the 'Save as type' option "All Files" and choose the appropriate **C:\Program Files (x86)\Java\jre7\lib\security** directory path. The file name must not be changed. However it is recommended that the existing default java.policy file <u>be renamed first</u> to java.policy.old as a backup. See Figure 2-16. Alternatively the existing java.policy file can be manually edited with the java permissions statements content shown above. Once this has been done use of the Energy Market Application within the portal with IE should be successful and uploading of multiple files to the *IESO* Collaboration communities will work where permitted.


Computer ▸ OS_C (C:) ▸ Program Files (x86) ▸ Java ▸ jre7 ▸ lib ▸ security
Search security
File Edit View Tools Help
Organize ▾ Open New folder
Favo
De
Dc
Re
Libr
Dc
Mu
Pic
Vic
Com

Name	Date created	Type	Size
blacklist	2015/06/04 2:30 PM	File	
cacerts	2015/06/04 2:30 PM	File	
java.policy	2015/06/04 2:30 PM	POLICY File	
java.policy.old	2015/06/04 2:30 PM	OLD File	
java.security	2015/06/04 2:30 PM	SECURITY File	
javafx.policy	2015/06/04 2:30 PM	POLICY File	
javaws.policy	2015/06/04 2:30 PM	POLICY File	
local_policy.jar	2015/06/04 2:30 PM	Executable Jar Fi...	
trusted.libraries	2015/06/04 2:30 PM	LIBRARIES File	
US_export_policy.jar	2015/06/04 2:30 PM	Executable Jar Fi...	

Figure 2-16: Renaming existing Java Policy File to "java.policy.old"

Internet Connection

72 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

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

74 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). *Participants* who require high performance or reliability may wish to consider the PRIVATE or SHARED network alternatives.

75 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

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

77 *Participants* will access the *IESO* using *IESO* supplied authentication credentials which are subject to the limitations and conditions defined in the Market Rules. 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* website). 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).

78 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

79 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*.

80 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.

81 *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.

82 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.

83 The current list of preferred telecommunications carriers consists of the following: Allstream, Bell Canada, Hydro One Telecommunications, and Rogers Communications.

2.2.3 Shared Network

84 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.

85 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.

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

Connecting to the Supplied Ethernet Port

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

88 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

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

90 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

91 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.

92 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

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

94 The *market rules* requires that the *IESO* implement access control protocols to protect the unauthorized disclosure of *confidential information* transmitted by electronic communications. The use of UserID 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.

95 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.

Account Suspension and Auditing

96 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

97 *IESO* ITOPS Customer Support , 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.

98 *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*,

99 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
-

100 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 ITOPS Customer Support is responsible for issuing and maintaining User ID account identity credentials.

2.3.3 Energy Market Application hosted within the IESO Portal

Energy Market Application Applet

101 All *participants* must have the ability to use the browser-based solution.

102 *Participants* can download the "*Identity Management Operations Guide*" and the "*Market Participant Energy Market Graphical User Interface User's Guide*" (see the Technical Interfaces Page of *IESO*'s Web site) for instructions on interface use.

103 An Energy Market applet is automatically downloaded after an individual logs into the *IESO* secure Portal and navigates to the Energy Market Application.

104 *Bids* and *offers* may be submitted via the Energy Market Application in the Portal in two ways: Template and HTML Form.

105 The Energy Market Applet requires communications access 'via' the following port: 443 (SSL protocol)

MIM Programmatic API Application (Application Based Solution)

106 *Participants* can choose to use the application based MIM programmatic API solution with a *participant* custom application. This is an alternative method for accessing the Energy Market Application functionality hosted with the IESO Portal. Under such conditions 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.

107 The MIM API Application can be downloaded from the *IESO* Web site as a part of the IDK (IESO Development Kit) (see the Technical Interfaces Page of *IESO*'s Web site).

108 The MIM programmatic API provides the same market application functionality as the Energy Market Application in the Portal. However only Template based *bids* and *offers* may be submitted using the MIM programmatic API. HTML Form data cannot be submitted using the MIM programmatic API Application because HTML Form data is browser based and the MIM programmatic API Application is not using a browser.

109 See MIM MPI Applet section for UserID details.

110 The USERID used for authentication with the MIM programmatic API is the REGISTRATION User Login Name, concatenated with an @ symbol, and finished with the REGISTRATION *participant* Constant Shortname. See the Technical Interfaces Page of IESO's Web site for details on how the REGISTRATION User Login Name and REGISTRATION participant Constant Shortname are created. Below is an example of the syntax of the USERID:

REGISTRATION_User_Login_Name@REGISTRATION_MP_Shortname

111 The required "REGISTRATION Profile" (Registration Profile) is accessed via the USERID during login with the MPI programmatic API.

112 When an End Entity at the *participant* authenticates using the API, the USERID is presented by the system and is used to fetch the "REGISTRATION Profile" from the MIM Netscape Directory Server. The "REGISTRATION Profile" provides the required access permissions to the USERID upon login.

113 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. The *participant* uses an *IESO* identity credential to authenticate to the *IESO*. The End Entity is able to automatically navigate the *IESO* site based on the End Entity's "REGISTRATION Profile."

114 *Participants* that choose to access the Real Time Energy Market bid site via the MIM programmatic API (i.e. using the MIM IDK) will need to register the IP addresses of the workstations where the API is being used, with the *IESO*. This is required for both production and sandbox environments to enable access to the bid site through the *IESO* firewall.

115 The MIM programmatic API Application requires access to the following port: 443 (SSL). *Participants* with firewalls *must have* this ports open *f*or communication with

the. The *"IESO Developer's Toolkit (IDK), Implementation Manual" should also be referenced for information on* defining communications.

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

116 All Portal/Online IESO/Confidential Reports users login with a UserID account credential for all Portal, Online IESO hosted applications and the Confidential Reports site.

117 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.

118 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.

119 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: 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

120 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.

121 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

122 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

123 The *relevant* IESO Portal and MIM programmatic API manuals should be referred to when appropriate.

– End *of Section* –

3. D*is*patch Information

124 (For supporting rule references, please refer to “Appendix 2.*2, Sections 1.1 & 1.3 of* the *market rules”*)

3.1 Dispatch Workstations

125 *This sect*ion provides descri*ption 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*.

3.1.1 Hardware Requirements

Platform

126 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 7 operating systems. Displays may be rendered incorrectly if a Windows Operating System is not used.

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

The following provides the minimum hardware requirements:

Processor

128 The minimum required processor speed is an Intel I5.

Memory

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

Hard Disk

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

Interface Cards

131 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

132 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

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

Printer

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

3.1.2 Software Requirements

Operating System

135 The PC should be operating with Windows 7 with support for TCP/IP protocol. It is recommended that the latest operating system patches be maintained.

Internet Browser

136 For WEB based message exchange the PC should include the IE 8.0 or IE 9.0 browser.

Connectivity

137 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

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

3.2 Dispatch Message Exchange

3.2.1 Overview

139 *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.

140 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.

141 The *participant* will:

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

142 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*.

143 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*.

144 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.

145 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.

146 Interfaces (see figure 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*.

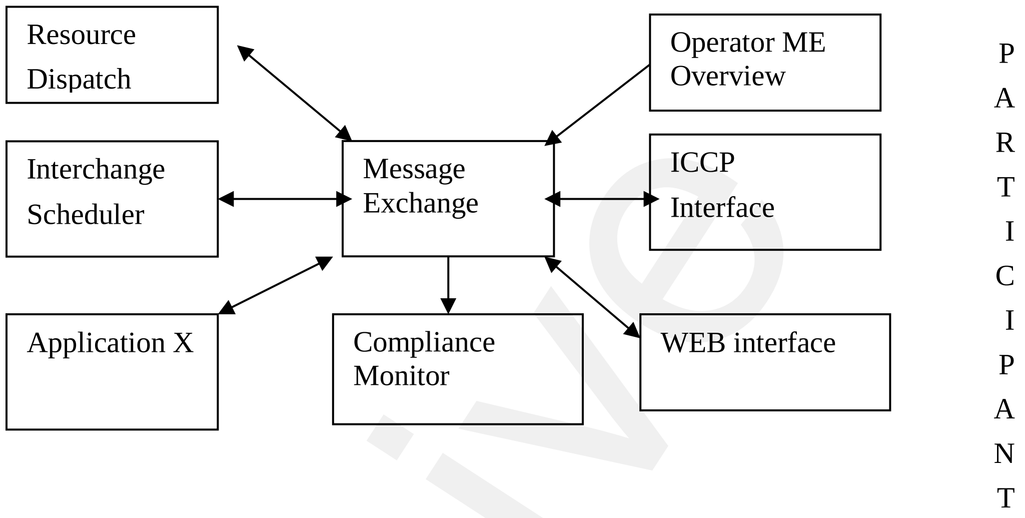


Figure 3-1: Message Exchange Interfaces

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

148 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 Functional Parts

149 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).

3.2.3 Dispatch Messaging

150 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*.

151 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

152 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 *generations facility's* effective ramp rate

Reserve Dispatch

153 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

154 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/load facility* was scheduled.

Automatic Generation Regulation Activation

155 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

156 *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

157 *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 define in the "Market Rules", for the specified *dispatch period*.

3.2.4 Dispatch Message Structure

General Structure of All Dispatch Messages

158 *Dispatch* messages are composed of a message header and a message b3.2ody. The content of messages is not 'case sensitive'.

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

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

161 *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

162 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).

3.2.5 Dispatch Message Scenarios

163 Heart beat messages are sent by the *IESO* to determine whether the *participant* is able to receive *dispatch instructions* from the *IESO*.

IESO – Action	MP –Response	Comment
HEARTOUT	HEARTIN	The *IESO* will send a HEARTOUT message every 60s to check for an active MP 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 MP client is considered out of service and the Exchange Coordinator be informed of the problem.

164 The following scenario 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* MP accepts the *dispatch* and complies with the instruction.

IESO – Action	MP – 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 MP client should immediately send a RECEIPT message back to the *IESO* acknowledging that the message has been received.

	ACCEPT	The MP 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 COMFIRMATIONOK message is sent to confirm that the ACCEPT message was received and acknowledged by the *IESO*.

165 The following scenario demonstrates what will happen when the *participant* rejects a *dispatch* message.

IESO – Action	MP – 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 MP client should immediately send a RECEIPT message back to the *IESO* acknowledging that the message has been received.

	REJECT	The MP should send a REJECT message to 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.

166 The following scenario demonstrates what will happen if the *participant* does not respond to a *dispatch instruction.*

IESO – Action	MP – 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 MP 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 20s 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 MP client from further accepting or rejecting *the dispatch instruction*. If, within 30 seconds after a *dispatch instruction* has timed out, *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.*

3.3 Real Time Network

167 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.

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

169 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.

170 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. i) Where 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 – 40°C, free of Electro-Magnetic interference, etc.)

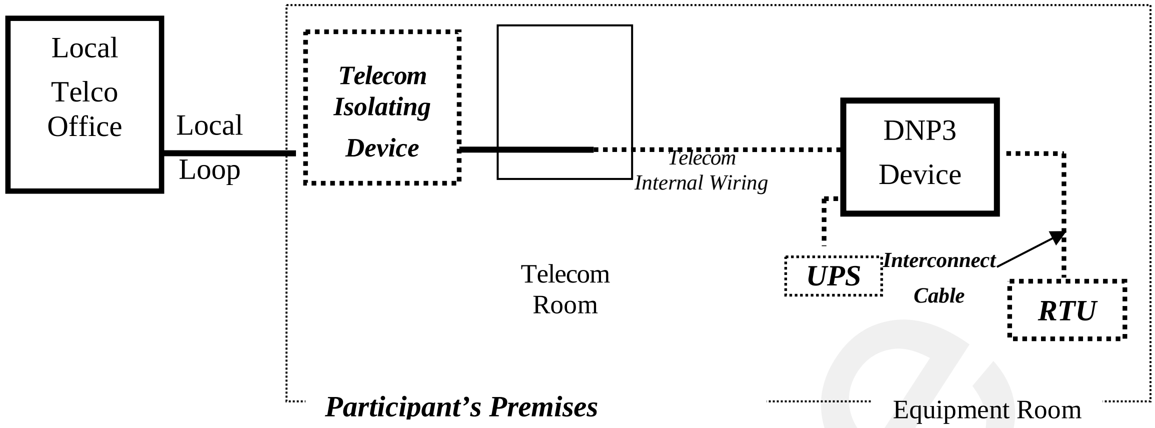
c. A suitable power source for the customer premises equipment (typically a reliable source of 120V ac, 60 Hz – usually from a UPS with a total load capacity of 500 Watts) with at least 8 hours of survivability after loss of commercial power.

d. Access for maintenance personnel as needed.

e. Connectivity from the *participant* equipment to the customer premises equipment as stated for the particular device.

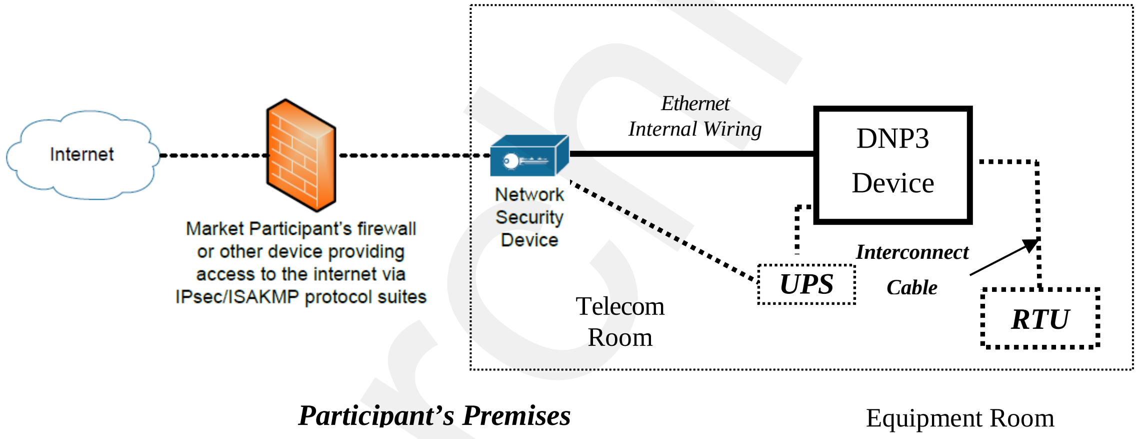
f. A point of contact (a person and telephone number) to enable the *IESO* to request repairs by the *participant* for telemetry failures.

MPLS connection diagram:



(Legend: *IESO* responsibility ▬▬ *Participant* responsibility) ....

Site-to-Site VPN connection diagram:



(Legend: *IESO* responsibility ▬▬ *Participant* responsibility) ....

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

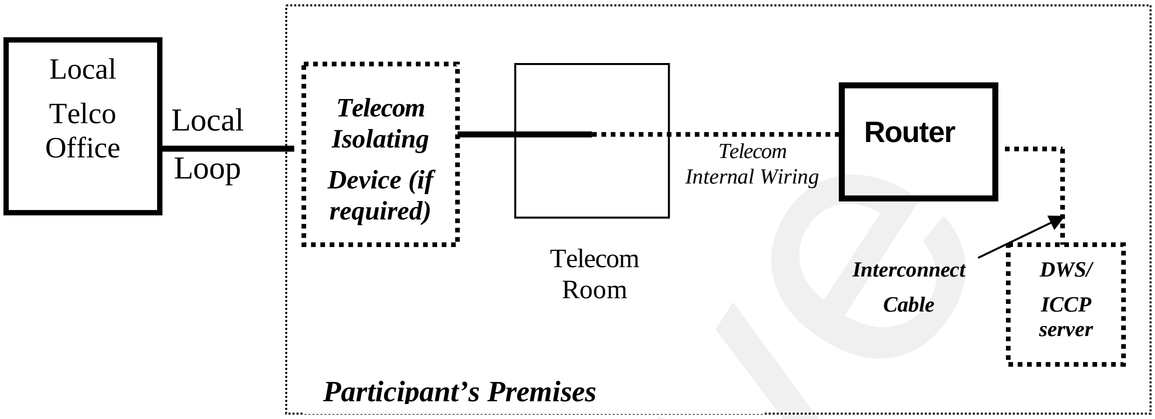
171 The connection to the Real Time Network for a *dispatch workstation* requires the *participant* to provide the following:

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 – 40°C, 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.



(Legend: *IESO* responsibility ▬▬ *Participant* responsibility)......

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

3.4 Voice Communication Specifications

172 Voice communications are broken into two categories:

- Normal-priority path *participants*; and
- High-priority path *participants*.

173 The determination for whether a *participant* requires a High Priority path is defined in the "Market Rules" 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*.

174 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" (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

175 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

176 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.

177 An 'autoringdown' circuit and other similar dedicated facilities may be considered as High Priority and 'hardened' depending on location.

178 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.

179 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.

180 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

181 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

182 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 & AGC

183 (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

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

185 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.

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

187 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

188 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.

189 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.

190 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.

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

192 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.

193 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.

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

4.1.3 Field Instrumentation Standards

195 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.

196 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.

197 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.

198 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

199 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

200 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” and through consultation with the *IESO*.

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

Analogue Points

202 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 – 100 MW to an analogue representation of 4-20 mA or 0-1 mA. *Participants* may contact the *IESO* for more detailed information.

Status Points

203 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

204 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.

205 The RTUs must be operated in an environment of –40°C to +80°C and 95% non-condensing relative humidity.

4.1.6 Communications Specification

206 The RTUs can communicate with the *IESO* using either a serial port (operating in the range of 4.8 - 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*.

207 The Real Time Network's customer premises equipment (FRAD and DSU) require a secure source of power supplying 115 Vac. The use of an inverter, backed with at least 8 hours of battery power, will normally provide this *reliability*. The inverter may also supply power to the RTU. If required, the *IESO* can recommend a dedicated inverter and a bypass-switch for powering the telecommunications equipment. In this case, the primary source of power will be a *participant* provided dc supply to the inverter in the range of 100-280 Vdc capable of supplying the load for at least 8 hours and a secondary 115V ac source connected to the bypass switch.

208 For the *IESO* supplied telecommunications equipment, the acceptable environment is 0°C to +40°C and 5% - 90% non-condensing relative humidity.

4.1.7 RTU Site Certification

209 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.

210 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.

211 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.

212 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.

213 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.

214 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.

215 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

216 *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.

217 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 setpoint 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.

218 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.

219 Units which do not have remote MW setpoint 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*.

220 Units which have MW controllers with remote MW setpoint capability can choose to use either a pulse width to raise or lower the MW setpoint value or they can chose to use a direct MW setpoint value provided by the *IESO's AGC* controller. A direct MW setpoint 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 setpoint capability. A typical block diagram of the entire *AGC* control loop is shown in Figure 4-1 below.

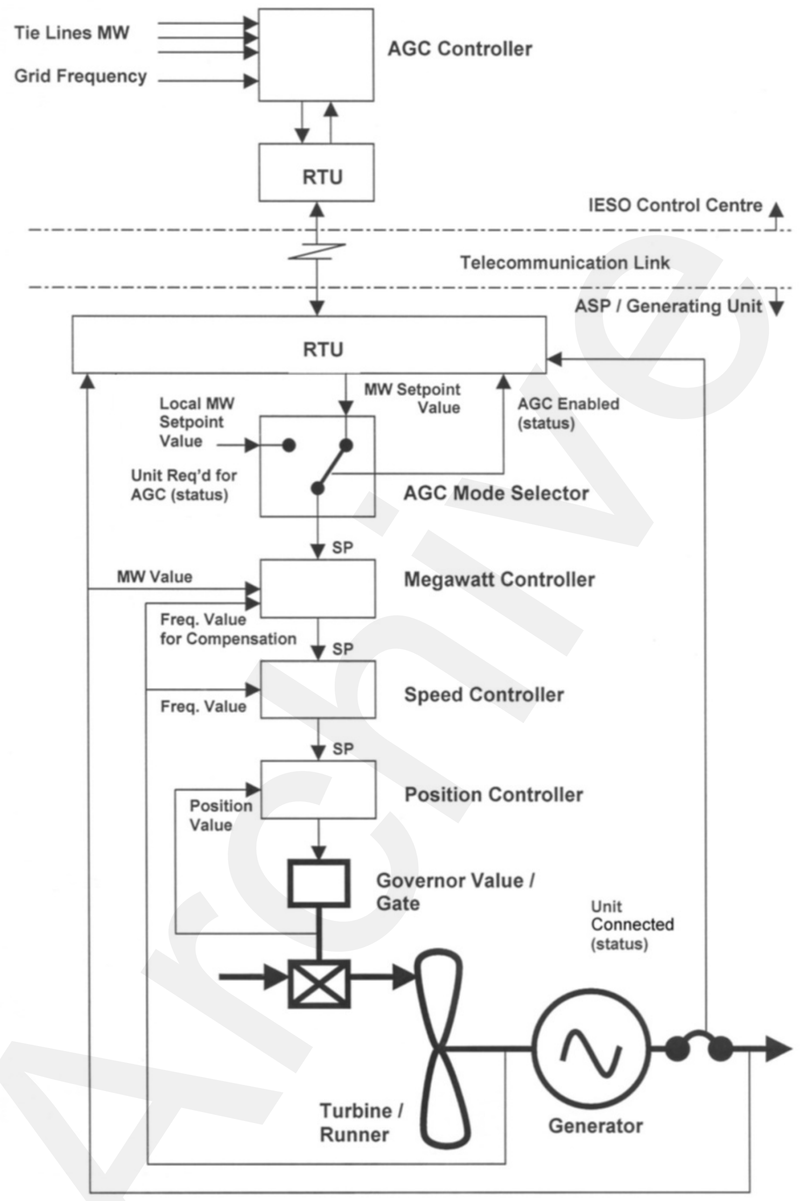


Figure 4- 1 Block Diagram of Typical AGC Control Arrangement for Generation units With Remote MW Setpoint Control Capability

221 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.

222 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.

5. Market Applications

5.1 Market Application Systems Information

5.1.1 Overview of Dataflow Systems

223 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*.

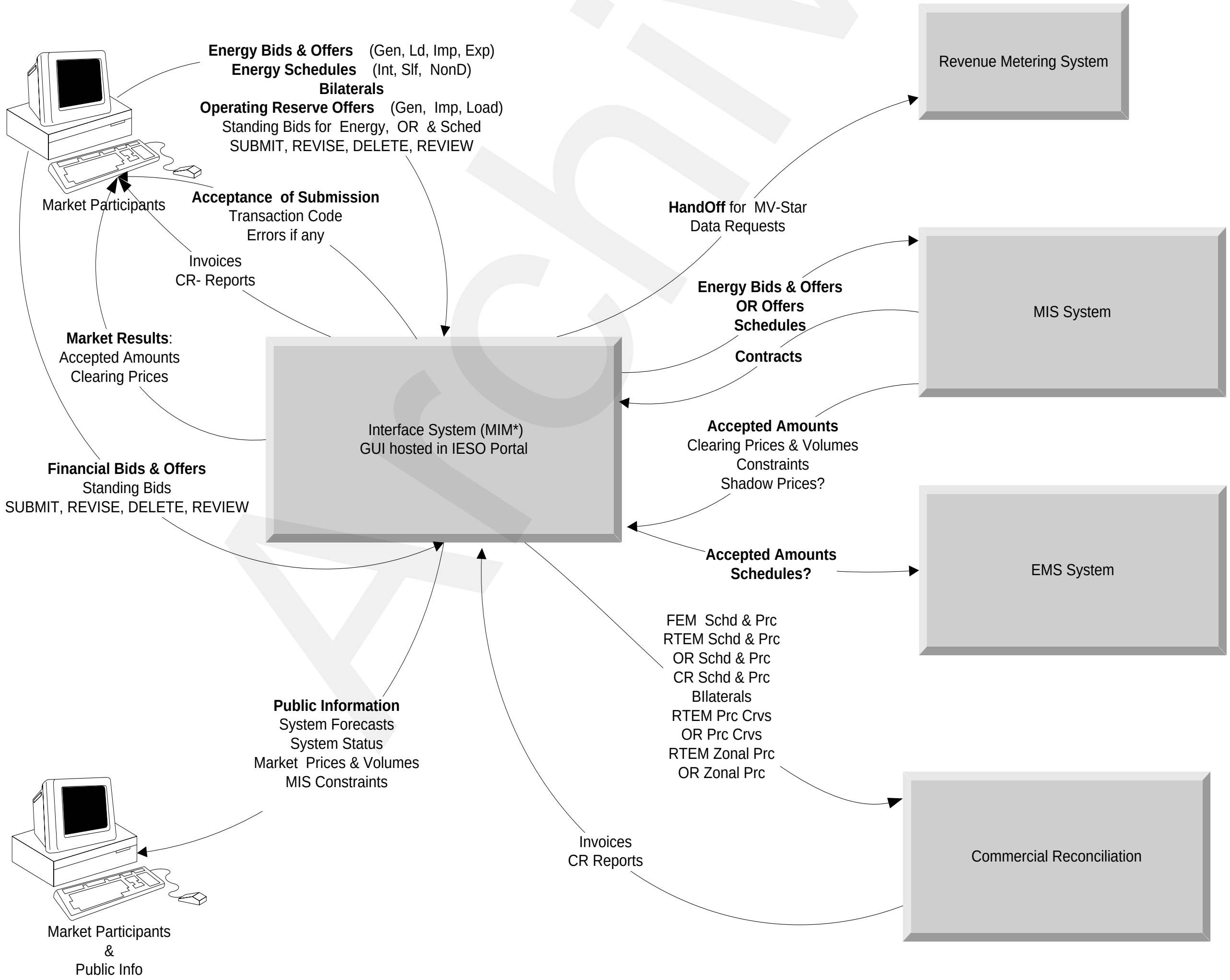


Figure 5-1: Overview of Dataflow from the MP to IESO systems

5.1.2 Energy Market Application

224 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 default *IESO* provided GUI , hosted in the *IESO* Portal using Web Page based Forms;

b. Through a default *IESO* provided GUI hosted in the *IESO* Portal by uploading and downloading ASCII data files; and/or

c. Through a programmatic interface via an *IESO* provided API (IDK).

Bidding Templates

Template Format

225 There will be upwards of 25 data template file formats for submitting and downloading data. All template files are simple Comma Separated Text (CST) files containing only ASCII characters with no hidden formatting information.

226 These CST files will be subject to validation. The extension of the file is NOT important as the file format described in the data template and validation rule documents, which are located on the Technical Interfaces page of *IESO*'s Web site, determines whether the file is accepted. Three types of validation rules are recognized, which consist of: syntax validation, technical feasibility checks, and commercial acceptability checks. Invalid data will be rejected with the appropriate error messages being posted to the sender.

Template File Structure

227 A single transmission file may contain one or more *bids*. The entire file will be considered as one transaction. Each file must have a file header with information common to the entire file. The file header can be followed by one or more *bids*. Each *bid* begins with a *bid* header followed by one *bid* body. The file header defines the application process and in some cases the market process and the data that is common to *bids* that belong to the transaction. Data associated with a *bid* is entered into a data template in a predefined structure.

Rules for Submitting Data & Using Template Files

228 Except where otherwise mentioned, the following rules are common to all the data template files:

a. A template file is a simple comma separated text file containing only ASCII characters. No hidden formatting information is allowed.

b. PM keyword in the file header indicates that the transaction is targeted for the *physical market*. The FM keyword in the file header indicates that the transaction is targeted for the Financial Market.

c. RTEM, SCHEDULE, BILATERAL, OPER_RESV or CAP_RESV keyword in the transaction header of PM template file indicates that the transaction is targeted for the real-time *energy market*, *real-time schedule* market, bilateral contract market, *operating reserve market* or the *capacity reserve market* respectively. The above markets may contain all 24 hours data or data for a range of hours or just the data for a particular hour.

d. The Bid_Type field describes the type of resource submitting the *bid/offer*. The following keywords, and their assigned definitions, are used within the context of these templates:

- *GENERATOR*: A generation resource located within the *IESO-controlled grid* in Ontario.
- LOAD: A load located within the *IESO-controlled grid* in Ontario.
- INJECTION: A generation resource located outside Ontario. Can also be considered as imports by *IESO*.
- OFFTAKE: A load located outside Ontario. Can also be considered as exports by *IESO*.

e. Standard time will be used for the date fields. There will be no 23-hour short days and no 25-hour long days. All days will have 24 hours.

f. Blank lines are permitted in the data files, and are ignored. White space is also ignored. Comma is used as the only data field separator.

g. Comment lines must begin with \\. Comments can also be added at the end of a data line but it must be preceded by \\. Any text following \\ will be interpreted as comment and will be ignored. Comments cannot extend past across multiple lines unless each line begins with a \\.

h. A semi-colon is a record terminator. It will be used as a file header, *bid* header, and *bid* body delimiter. The record terminator is not needed for those records that are comment lines. A data record must be on a single line. There is no maximum length for a line in an incoming file so long as a record terminator is specified for record termination. The record terminator signals the end of the record instead of the end-of-line character.

i. The asterisk character is used to separate multiple *bids/offers* in a single file. The asterisk character should be used before and after each *bid*, which can contain up to 24 hours of data.

j. All data information in a given template must be included in exactly the same order as listed. Any additional information or omissions will be considered as an error and will be rejected.

k. An optional field can have a value or null. If a value has been entered, it will take precedence over the default value. All fields are mandatory if not specified otherwise. Optional fields are denoted with field names enclosed within [square brackets] in the template definitions.

l. All mandatory fields must have values entered. If there is no data for a particular field then NULL value should be submitted. For example, ‘value1,,value2’ contains a NULL value between value1 and value2.

m. Each tuplet of data, as in the case of (Price, Quantity) or (RampBreakQuantity, RampUp, RampDown) must be enclosed within parentheses. The entire set of tuplets, i.e. the curve itself, must be enclosed within curly brackets. For the RTEM, the Price/Quantity data for an hour or range of hours can have up to 20 tuplets of values with a minimum of two tuplets. For *Energy* Ramp Rate tuplets, the maximum is 5 tuplets with a minimum of 1 tuplet. Whatever the number of tuplets is, the data must be included first within parenthesis and then within curly brackets. As an example '1, {(23.50,0), (23.50,70)}' means that the price curve for 1AM has a two P, Q pairs.

n. A shorthand notation can be used for specifying *bid* data that does not change across a contiguous range of hours. The format of the shorthand notation is 'x-y' for an hour field and '{(p1, q1), (p20, q20)}' for a price curve, where x and y are the start and end hours that have the same value or the same curve. As an example, the shorthand notation '1-5, 70' implies that the value 70 is valid for all hours from 1 AM through 5AM. This shorthand notation is valid for incoming *bids*. This data, once received, will be stored on a per hour basis. This also implies that outgoing data will be given on an hourly basis.

o. When using shorthand notation the hours must be in ascending order only. If there are any overlaps the records are invalid and will be rejected. As an example

1-5
7-10
2-3 → will be rejected
1-5
7-10
6 → will be rejected

p. Rejected records will be identified to the *participant* through a report created at the end of the transmission, identifying the rejected records and the reason for rejection.

q. Output data templates may use the letters 'N/A' to indicate that the data value is not available.

r. Data that is in the form of text strings must be entered within double quotes (i.e. " "). Such data cannot have double quotes embedded within it. For example field 'other_reason', which is a text string should be submitted within double quotes (i.e. " ").

s. All *bid* submission templates can be used for download purposes also. The valid *bid* data that will be downloaded will be in a similar format as it is during an upload. As mentioned above, hour ranges will not be used to download data but on a per hour basis. The downloaded data can be updated/modified, if needed, and then resubmitted without having to make any formatting changes.

Bid Data Validation

229 There is no sequence, template files can be submitted at any time. 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.

230 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.

231 *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.

Template Description and Samples

232 All sample data templates (described below) and associated data sample files are provided at the *IESO* Web site under Technical Interfaces (*Participant* Submissions) for viewing or downloading. Comment lines may be included within the template to explain its structure. Comments are not required in the actual templates. Data values are included to illustrate the structural characteristics. Since these values were randomly chosen, there may not be a logical consistency across the data fields. In addition, some data, such as *Participant* ID and Resource ID have been edited for confidentiality reasons.

The ***Energy* Template** is used to specify the *bids* or *offers* for various resources like *generators*, loads, off-takes and injections. This template can be used for data submission in any window and can be used to view the energy data. These will be version sensitive and new versions will be available to all *Participants* when available. Older versions cannot be used when a new version is issued.

- The **Bilateral Contract Template** is used to specify the hourly amount exchanged between two *participants*. This template can also be used to view the bilateral contract data.
- **Real Time *Energy* Schedule Template** is used to specify the schedules for various resources. *participants* will use this template to send their schedule data to the *IESO*. This template can also be used to view the schedule data. This template can be used by *participants* that are:
- Self-scheduling generators, or
- Intermittent generators
- **Operating Reserve Template** is used by *participants* to send their *bid/offer* data to the *IESO*. It can also be used to view the operating reserve data. All operating reserve *ancillary service* data loading use the same template. There are 3 types of Reserves supported and they are 10-min Non-Spin Reserve, 10-min Spin Reserve & 30-min Reserve.
- **The *Capacity Reserve Bid* Template** is used to send *bid/offer* data to *IESO*. This template can also be used to view the *bid/offer* data.

  Note: The Capacity Reserve Market is not yet implemented.
- **Public Market Information,** which is available on the Technical Interfaces page of *IESO*'s Web site, is used by *participants* to view the public market information and/or the market results.
- **Private *Participant* Information,** which is available via through the MPI or API is used by *participants* to view their dispatch information.

233 Although the *IESO* is not bound to rigorously follow any particular ISO standard it recognizes the benefit of taking some of them into account. ISO 9001 regulations are considered in the attempt for achieving quality interfaces.

5.1.3 Settlements Application

234 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 (https://reports.ieso.ca/private/

235 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.

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

Settlement Statement Files

237 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.

238 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 markets* 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" 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".

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

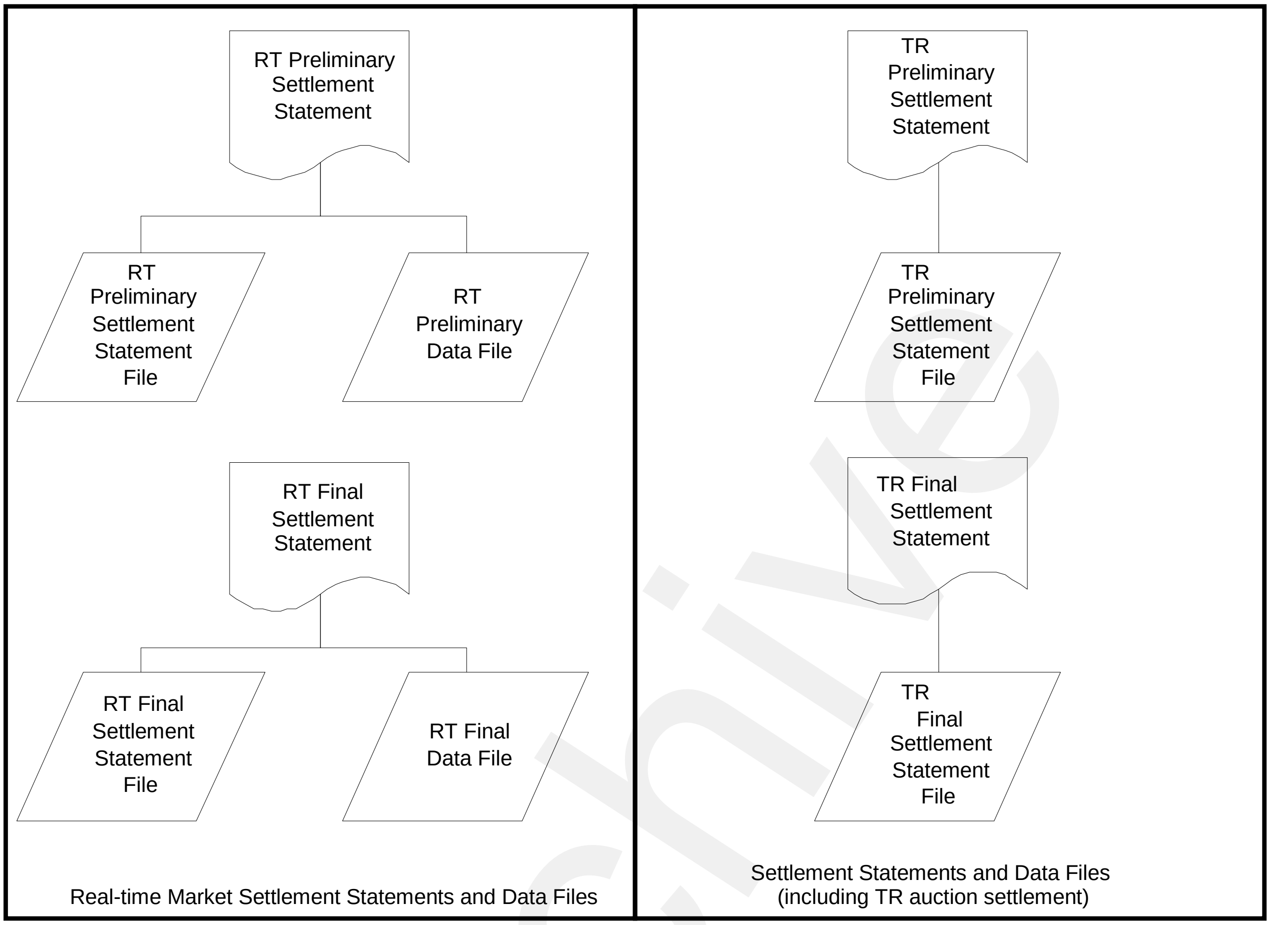

RT Preliminary Settlement Statement
RT Preliminary Settlement Statement File
RT Preliminary Data File
RT Final Settlement Statement
RT Final Settlement Statement File
RT Final Data File
Real-time Market Settlement Statements and Data Files
TR Preliminary Settlement Statement
TR Preliminary Settlement Statement File
TR Final Settlement Statement
TR Final Settlement Statement File
Settlement Statements and Data Files (including TR auction settlement)

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

239 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.

240 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

241 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 *IESO Settlement Schedule & Payment Calendar* (“Market Rules” 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".
- 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

242 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 On-Line Outage Forms Application

243 Within the *IESO* Portal the On-line Outage Forms application provides functionality to permit secure submission and historical search for outage data previously submitted via *IESO* Form 1360: Outage Request.

5.1.6 Portal Prudential Manager Application

244 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.

5.1.7 Energy Market Application Interfaces

245 The Market Information Management (MIM) system, accessible via the Energy Market Application hosted in the *IESO* Portal allows the *participant* to interface with the *IESO*. Specifically, the Energy Market Application represents the secure internet-based client gateway to functionality provided by the *IESO energy* bidding system.

246 The *participants* can interact with the MIM using the following two methods:

- Internet Explorer browser used to login to the *IESO* Portal to access the Energy Market Application. The browser based Energy Market Application interprets tag languages such as HTML. It allows client interaction through the keyboard/mouse; and

- MIM Client API (IAPI). The API emulates the functions of the browser. It allows Clients programmatic access to the MIM functionality using third party applications.

247 The MIM Application Interface (API) code will allow *participants* to customize their interface to interact with the *IESO*. Using the Java interface, these API's provide access to MIM. They act as wrappers to validate and normalize parameters passed to the MIM system through Java class libraries. It is these same class libraries that also run within the Communicator browser environment and are fetched when the secure MIM site is first visited. These library routines provide the following functionality:

- Template Upload;
- Template Download;
- System Message Download; and
- Market Status Download; and

248 To support platform independence, as of IDK 1.46 a Java interface is supported by the *IESO*. To download the latest version of the IDK visit the Technical Interfaces page of the *IESO*'s Web site.

249 Client-side certificates are no longer required to access the MIM via the API. As of summer 2011 UserID/Password identity credentials have been supported. To use the API, it is necessary to establish an SSL session with the MIM Web server. *Market participants* will need to register all participating MIM API client system IP addresses with the *IESO* to transition to UserID/Password identity credential usage with the MIM API.

250 In summary the following hardware/software recommendations are made :

- Minimum 4 GB of system memory;
- Intel based PC running Windows 7 SP1, or higher;
- Java Runtime Environment at a minimum as shown on the "*IESO* Supported Client Platform" Web Page. This contains the required JVM and runtime classes;
- Internet Explorer to download the IAPI bundle; and
- *IESO* issued UserID credentials and the software to establish a secure (e.g. SSL) session with the MIM server.
- Workstation IP address(es) registered with *IESO* to permit communications through *IESO* firewall.

251 Detailed information on these functions can be found in the "*IESO Developer's Toolkit (IDK), Implementation Manual*" which is available at on the Technical Interfaces page of *IESO*'s Web site. It provides details of the following six functions:

- Login to MIM;
- Upload *Bids*;
- Download *Bids*;
- Download System Messages; and
- Download Market Status Information.

5.1.8 Portal Transmission Rights Auction Application

252 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

5.1.9 Online IESO System

253 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 the will have to login as SSO is not set up with it.

254 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 etc..

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

256 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

257 The Online IESO System – Manage Facilities and Equipment application has been added to permit management and registration of equipment and facilities installations.

258 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.

259 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.

260 The Online IESO - Submit DR Auction Offer, Manage Demand Response Commitments, Demand Response MPPS Action applications have been added to permit submissions and reporting for the new Demand Response Auction.

261 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.

5.1.10 IESO Confidential Report Site

262 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

263 *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*.

264 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

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

5.2.3 Fund Transfers

266 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.

267 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

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)
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* (www.dnp.org)
Java Runtime Environment	Non-*IESO* (http://www.oracle.com/technetwork/java/archive-139210.html)
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
Energy Market Application User Interface User's Guide	IMO_GDE_0003
IESO Developer's Toolkit (IDK), Implementation Manual	IMO_MAN_0023
Web Based Message Exchange – Market Participant's Guide	IMP_MAN_0031
IESO Reports API Guide	N/A

– **End of Document –**