MANUAL

Power to Ontario.
On Demand.

Market Manual 6

Participant Technical Reference Manual

Issue 29.0

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 29.0
Reason for Issue	Issued for Baseline 29.0. To include new RTUs to the certified list of devices in section 4.1.2
	Revised for Baseline 30.0 in regard of need for Participants to. Include use of new Registration System and Windows 7 and IE 8.0 and 9.0
Effective Date	September 11, 2013

Document Change History

Issue	Reason for Issue	Date
For change history prior to Issue 10, see issue 17.0 of the PTRM.		
10.0	Issued for baseline 15.1 for changes related to the *IESO* Portal and Identity Management systems and access to the Cybertrust Entrust Authority Administration tool used for creation of version 7.1 certificates that are required for TRA users accessing the Portal.	June 15, 2006
11.0	Issued for Baseline 16.0. To Include new RTUs to the certified list of devices in section 4.1.2	September 13, 2006
12.0	Issued for Baseline 16.1	December 6, 2006
13.0	Issued for Baseline 17.0	March 7, 2007
14.0	Issued for Baseline 17.1	June 6, 2007
15.0	Issued for Baseline 18.0	September 12, 2007
16.0	Issued for Baseline 18.1	December 12, 2007
17.0	Issued for Baseline 19.0	March 5, 2008
18.0	Issued for Baseline 19.1	June 4, 2008
19.0	Revised for Baseline 20.0	September 10, 2008
20.0	Revised for Verizon Data Center Move date change from May to June 2009.	June 5, 2009
21.0	Revised for Baseline 21.0	December 9, 2009
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	September 11, 2013

	for deployment of new IESO Registration System and use of Windows 7 and IE 8.0.	

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
All sections	Modified term of *market participant* to more generic term *participant.*
All Sections	Removed references to Window 98 /NT 4.0, Internet Explorer 6.0 and added use of Windows 7 and Internet Explorer 8.0 and 9.0
Section 2	Added content to provide explanation of generic term *participant.*
Section 2	Removed PKI references
Section 2	Updated content of required java policy file for changes required by java update 1.6.0_29 and higher.
Section 2	Updated IESO trust model entities and identity management content to correspond to changes required with use of new online Registration System
Section 4.12.	Updated to include new RTUs to the certified list of devices

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, S ection 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 XP and Vista, and 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 Java 2 R untime Environment (see java.sun.com). At this time there are no known issues with the *IESO* Portal and the supported browsers.

21 For Windows XP, 7.0 and above It is recommended that the client workstation hardware conform to Microsoft's specifications found at: http://www.microsoft.com/windowsxp/pro/evaluation/sysreqs.mspx

However going forward the *IESO* recommends the following:

Processor

22 The minimum recommended processor is a 1 GHz 32 –Bit (X86) or 64-bit (x64) CPU

Memory

23 The minimum recommended system requirements are 1 GB of internal RAM.

Disk

24 The recommended available disk space is a minimum of 15 gigabytes on a 40 GB hard drive.

Interface Cards

25 A minimum 56Kb modem or faster cable modem or equivalent is strongly recommended if the *participant* is interfacing with the *IESO* over the public Internet.

26 Support for DirectX 9 graphics and 128 MB of graphics memory (minimum), WDDM driver, Pixel Shader 2.0 in hardware and 32 bits per pixel.

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

Monitor

28 The supported monitor must be SVGA with a resolution capability of 800 x 600 pixels or greater.

Printer

29 It is recommended that a printer with high resolution of at least 600 dpi and that supports multiple fonts be used.

Other Components

30 Additional components that should be included with your system are a compatible two-button mouse, keyboard, and 1.44 MB high-density floppy disk drive.

31 A Smartcard and reader are highly recommended options.

32 DVD-ROM drive

2.1.2 Software Requirements

Operating System

33 The recommended operating system is Windows XP SP2, Vista or Windows 7 as shown on the *IESO* Supported Client Platform web page at :

http://www.ieso.ca/imoweb/ti/ti_Supported-Client-Platform.asp .

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

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. G o 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

34 All *IESO* applications within the MPI are fully tested with the supported OS /Browser and JRE combinations.

35 128-bit encryption is standard with the Internet Explorer browser and this can be verified under the 'Help' menu and then the 'About Internet Explorer' menu selection. *IESO* secure web sites also have been configured to work with SSL 3.0 or higher which requires this level of encryption.

36 The viewing resolution must be 800 x 600 pixels or higher in view maximized mode.

37 Internet Explorer has been tested with the Notice of Disagreement (NOD) and Meter Trouble Reporting (MTR) applications. MTR and NOD will function as expected with the supported Microsoft OS, Internet Explorer combinations

38 The *IESO* Portal is accessible with Internet Explorer 7.x, 8.x, 9.x as well as Mozilla Firefox 2.x, 3.x or Safari 2.x & 3.x (on Windows XP, Windows Vista, and 7). 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.

Portal Outage Forms Browser configuration

39 The Portal On-line Outage Request Form has the following requirements:

40 Screen resolution of 1024 X 768 or higher

41 Internet Explorer version 7.0

42 Internet Explorer native XMLHTTP enabled

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

Firewall

44 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*.

Microsoft Internet Explorer Configuration for Portal

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

- IESO Energy Market Application Transmission Rights Auction
- MVWEB - participant metering data
- On-line Settlement Forms
- On-line Outage Forms (New)
- Various Collaboration initiatives (NERC CIP Technical Exceptions, SmartGrid Working Group, Enrolment etc., for document submission and retrieval etc.
- Access to the new Registration system

46 For the supported versions of Microsoft Internet Explorer to work properly with the Portal 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 7.0 has differences in configuration settings between Windows XP SP1 and SP2 and so does Internet Explorer 8.0 between Windows XP SP1 and SP2 and Vista and Windows 7. Internet Explorer 9.0 under Windows 7 is similar. These differences are documented by the *IESO* as required.

47 The browser settings are essentially the same for IE 7.0 and 8.0 and above with minor differences when using Windows XP–SP2, Vista and Windows 7. However under Vista, and Windows 7, Internet Explorer 7.0, 8.0 and 9.0 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 Vista and *Windows 7* and turn off Protected Mode for this zone only. *Vista, Windows 7 and above en*forces the opening of a new browser window every time the security zone changes

Internet Options - Advanced

48 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** XP shown)

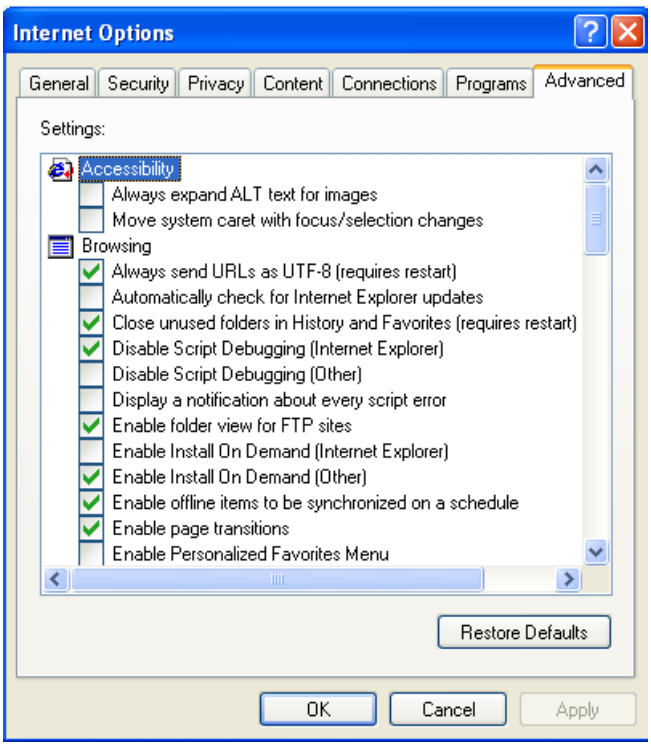


Figure 2-1: Internet Explorer, Internet Options - Advanced

3. Choose the following settings as shown in Table 2-1 for the appropriate Windows / IE combination and then click on the *'A*pply' button. Depending on the user's workstation soft*ware* 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 XP-SP2,Vista and *Windows 7*

Ad*vanc*ed Internet Option Parameter	**IE 7.0 – XP-SP2**	**IE 7.0 – Vista**	**IE 8.0 – Vista, Windows 7 and above**	**IE 9.0 – Windows 7 and above**
Accessibility Parameters – all				
Always expand ALT text for images	No stipulation	No stipulation	No stipulation	No stipulation
Move system caret with focus/selection changes	No stipulation	No stipulation	No stipulation	No stipulation
Reset text size to medium for new windows and tabs	No stipulation	No stipulation	No stipulation	No stipulation
Reset text size to medium while zooming	No stipulation	No stipulation	No stipulation	No stipulation
Reset Zoom level to 100% for new windows and tabs	No stipulation	No stipulation	No stipulation	No stipulation
Browsing Parameters				
Always send URLs	N/A	N/A	N/A	N/A
Automatically check for Internet Explorer updates				
Close unused folders in History and Favorites	No stipulation	No stipulation	No stipulation	No stipulation
Disable script debugging	N/A	N/A	N/A	N/A
Disable script debugging (Internet Explorer)	No stipulation	No stipulation	No stipulation	No stipulation
Disable script debugging (Other)	No stipulation	No stipulation	No stipulation	No stipulation
Display a notification about every script error	No stipulation	No stipulation	No stipulation	No stipulation
Enable folder view for FTP sites	N/A	N/A	N/A	N/A
Enable FTP folder view (outside of Internet Explorer)	✓	✓	✓	✓
Enable install on demand (Internet Explorer)	N/A	N/A	N/A	N/A
Enable install on demand (Other)	N/A	N/A	N/A	N/A
Enable offline items to be	N/A	N/A	N/A	N/A

Ad*vanc*ed Internet Option Parameter	**IE 7.0 – XP-SP2**	**IE 7.0 – Vista**	**IE 8.0 – Vista, Windows 7 and above**	**IE 9.0 – Windows 7 and above**
synchronized on a schedule				
Enable page transitions	No stipulation	No stipulation	No stipulation	No stipulation
Enable Personalized Favorites menu	No stipulation	No stipulation	No stipulation	No stipulation
Enable third-party browser extensions (requires restart)	✓	✓	✓	✓
Enable visual styles on buttons and controls in web pages	✓	✓	✓	✓
Force offscreen compositing even under Terminal Server (requires restart)				
Notify when downloads complete	No stipulation	No stipulation	No stipulation	No stipulation
Reuse windows when launching shortcuts	No stipulation	No stipulation	No stipulation	No stipulation
Show friendly HTTP error messages	✓	✓	✓	✓
Show friendly URLs	N/A	N/A	N/A	N/A
Show Go button in Address bar	N/A	N/A	N/A	N/A
Show Internet Explorer on the desktop	N/A	N/A	N/A	N/A
Underline links	Always	Always	Always	Always
Use inline AutoComplete	No stipulation	No stipulation	No stipulation	No stipulation
Use most recent order when switching tabs with Ctrl+Tab	No stipulation	No stipulation	No stipulation	No stipulation
Use Passive FTP (for firewall and DSL modem compatibility)	No stipulation	No stipulation	No stipulation	No stipulation
Use smooth scrolling	✓	✓	✓	✓
HTTP 1.1 Settings				
Use HTTP 1.1	✓	✓	✓	✓
Use HTTP 1.1 through	No	No	No	No stipulation

Ad*vanc*ed Internet Option Parameter	**IE 7.0 – XP-SP2**	**IE 7.0 – Vista**	**IE 8.0 – Vista, Windows 7 and above**	**IE 9.0 – Windows 7 and above**
proxy connections	stipulation	stipulation	stipulation	
International				
Always show encoded addresses	No stipulation	No stipulation	No stipulation	No stipulation
Send IDN Server Names	No stipulation	No stipulation	No stipulation	No stipulation
Send IDN server names for Intranet addresses	No stipulation	No stipulation	No stipulation	No stipulation
Send UTF-8 URLs	No stipulation	No stipulation	No stipulation	No stipulation
Show Information Bar for encoded addresses	No stipulation	No stipulation	No stipulation	No stipulation
Use UTF-8 for mailto links	No stipulation	No stipulation	No stipulation	No stipulation
Java(Sun)				
Use Java 2 v1.5.0_xx for <applet> ((requires restart) (If shown)				
Microsoft VM				
Java Console enabled	No stipulation	N/A	N/A	N/A
Java logging enabled	No stipulation	N/A	N/A	N/A
JIT compiler for virtual machine enabled	✓	N/A	N/A	N/A
Multimedia				
Don't display online media content in the media bar (if shown)	N/A	N/A	N/A	N/A
Always use ClearType for HTML	No stipulation	No stipulation	No stipulation	No stipulation
Enable automatic image resizing	✓			
Enable Image Toolbar (requires restart)	N/A	N/A	N/A	N/A
Play animations in web pages	No stipulation	No stipulation	No stipulation	No stipulation

Ad*vanc*ed Internet Option Parameter	**IE 7.0 – XP-SP2**	**IE 7.0 – Vista**	**IE 8.0 – Vista, Windows 7 and above**	**IE 9.0 – Windows 7 and above**
Play sounds in web pages	No stipulation	No stipulation	No stipulation	No stipulation
Play videos in web pages	N/A	N/A	N/A	N/A
Show image download placeholders	No stipulation	No stipulation	No stipulation	No stipulation
Show pictures	No stipulation	No stipulation	No stipulation	No stipulation
Show image dithering	No stipulation	No stipulation	No stipulation	No stipulation
Printing				
Print backgrounds colors and images	No stipulation	No stipulation	No stipulation	No stipulation
Search from the Address bar	No stipulation	No stipulation	No stipulation	No stipulation
Security				
Allow active content from CD to run on My Computer	No stipulation	No stipulation	No stipulation	No stipulation
Allow active content to run in files on My Computer	No stipulation	No stipulation	No stipulation	No stipulation
Allow software to run or install even if the signature is invalid	No stipulation	No stipulation	No stipulation	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	No stipulation
Empty Temporary Internet Files folder when browser is closed	No stipulation	No stipulation	No stipulation	No stipulation
Enable Integrated Windows Authentication (requires restart)	No stipulation	No stipulation	No stipulation	No stipulation
Enable Profile Assistant	N/A	N/A	N/A	N/A

Adv*anc*ed Internet Option Parameter	**IE 7.0 – XP-SP2**	**IE 7.0 – Vista**	**IE 8.0 – Vista, Windows 7 and above**	**IE 9.0 – Windows 7 and above**
Enable memory protection to help mitigate online attacks	N/A	No stipulation	No stipulation	No stipulation
Enable native XMLHTTP support	✓	✓	✓	✓
Phishing Filter	Turn on automatic website checking	Turn on automatic website checking	Turn on automatic website checking	Turn on automatic website checking
Use SSL 2.0				
Use SSL 3.0	✓	✓	✓	✓
Use TLS 1.0	No stipulation	No stipulation	No stipulation	No stipulation
Warn about invalid site certificates	✓	✓	✓	✓
Warn if changing between secure and not secure mode	✓	✓	✓	✓
Warn if forms submittal is being redirected	N/A	N/A	N/A	N/A
Warn if Post submittal is redirected to a zone that does not permit posts	✓	✓	✓	✓

Internet Explorer - Internet Options - Security

49 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 URLs for the Production and Sandbox environments into the Trusted Sites zone under IE Security or leave those URLs in the Internet zone by default for Windows XP. 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 Vista and 7 is important that the URLs be placed in the 'Trusted sites' zone as well as the *IESO* corporate site as discussed previously.

50 When the URL's are included in the 'Trusted Sites' zone for XP then it is recommended that the Security settings be configured as Medium-low instead of the default Low. This provides reasonable security but eliminates most prompts. For Vista and *Windows 7*, the default is medium and this can be left as is.

51 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

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

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

Select the **Security** tab. See Figure 2-2 and Figure 2-3. (IE / Windows XP shown). For Windows Vista and *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 Vista and *Windows 7* for the MPI web sites 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 2-3.

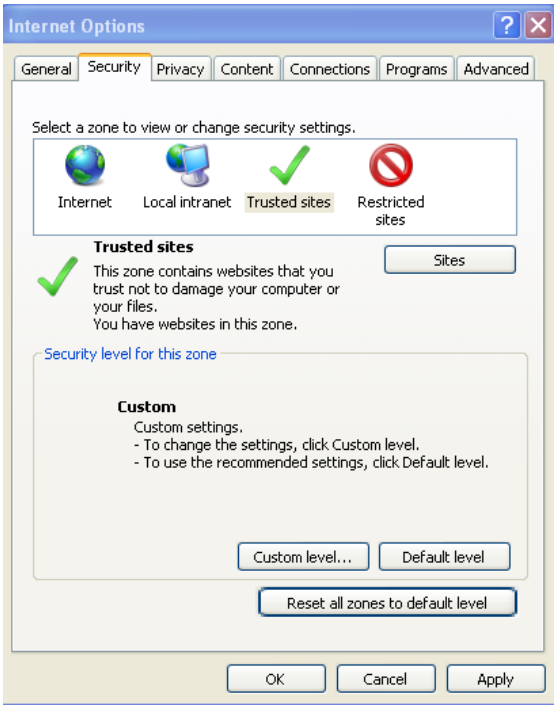


Figure 2-2: Internet Explorer 7.0, Internet Options - Security - Windows XP

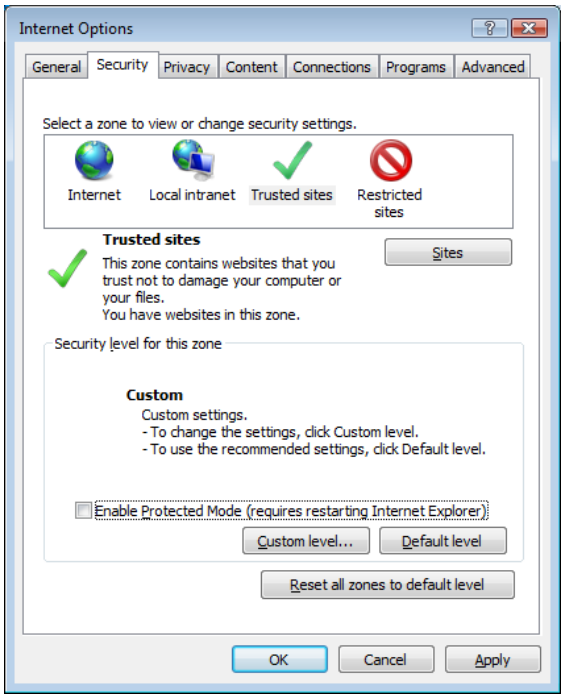


Figure 2-3: Internet Explorer 7.0/8.0/9.0, Internet Options - Security - Windows Vista and Windows 7

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 2-4. (IE / Windows 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.

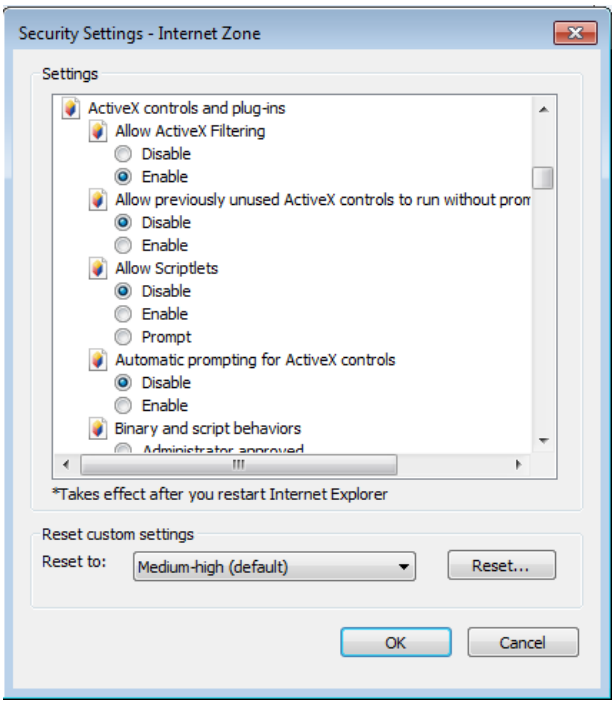


Figure 2-4: Internet Explorer 8.0/9.0, Internet Options - Custom Security Settings Window

Trusted Sites Security Settings

53 When including the *IESO* Portal 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 2.4 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 'Low' for XP and Medium for Vista and Windows 7. It is recommended to change this 'Medium-low' for XP and leave as default for Vista and 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 2-6 and 2-7.

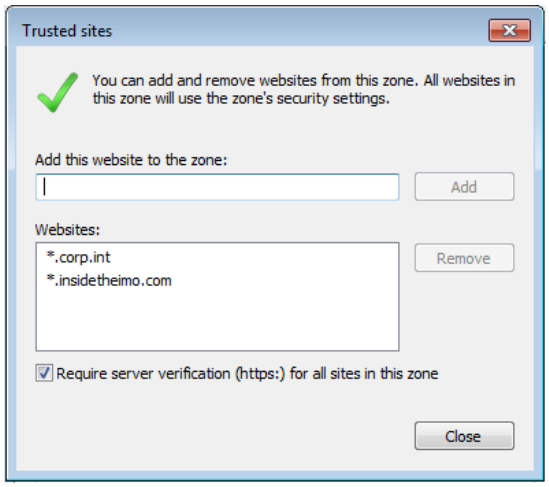


Figure 2-5: Internet Explorer 8.0/9.0, Internet Options - Trusted Sites Security – Windows 7

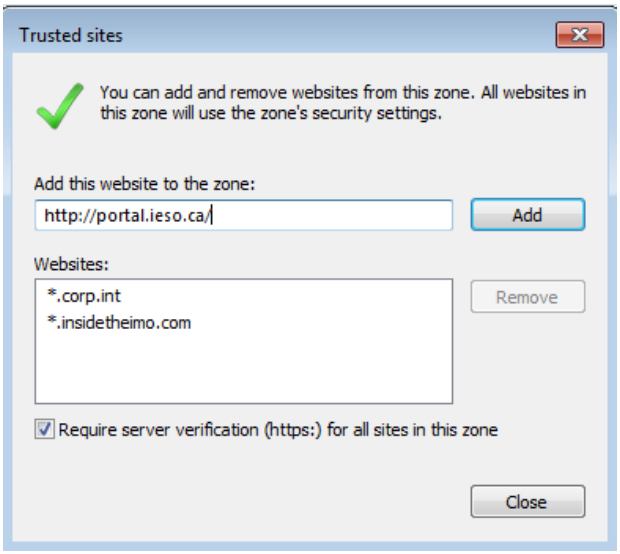


Figure 2-6: Internet Explorer 8.0/9.0, Trusted Sites Security - Web Sites Addition - Windows 7

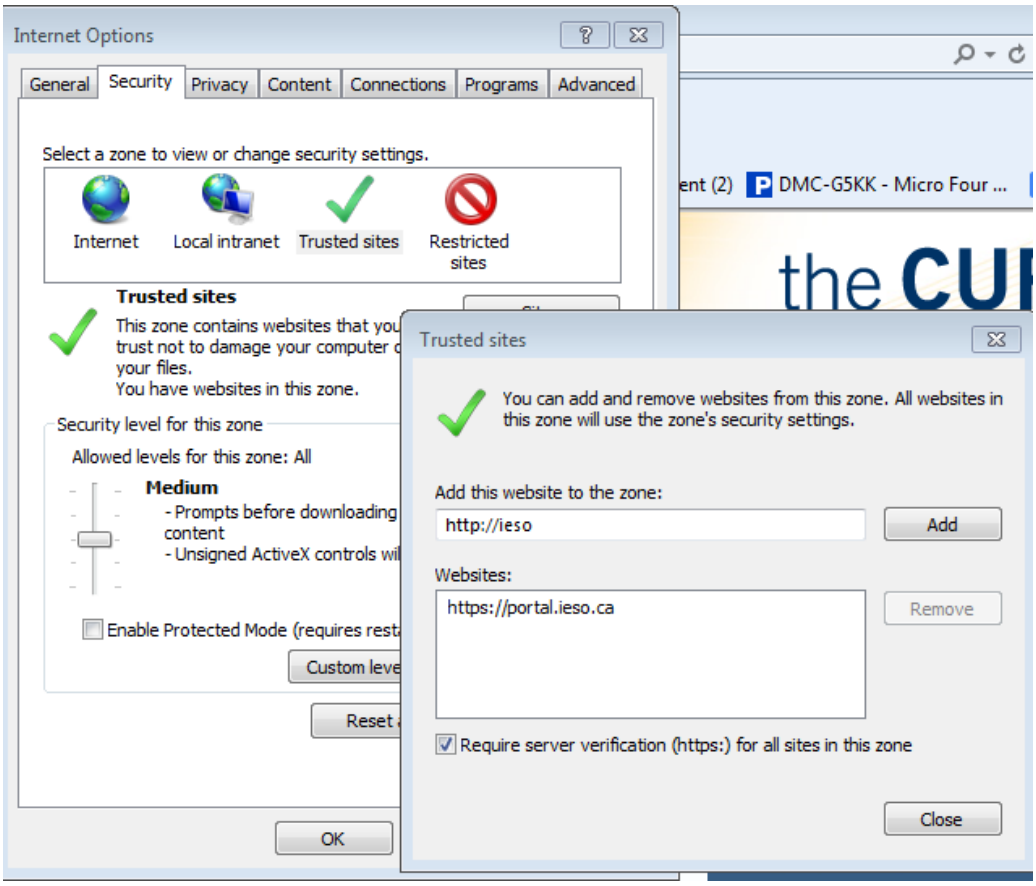


Figure 2-7: Internet Explorer 7.0/8.0, Trusted Sites Security - Web Sites Addition – Windows Vista and Windows 7

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.*

Table 2-2: IE Internet Options, Security Settings – Windows XP-SP2, Vista and *Windows 7*

Parameter	When IESO Portal URLs added to 'Trusted Sites' zone in XP-SP2 and IE 7.0	When IESO, Portal URLs added to 'Trusted Sites' zone in Vista and IE 7.0	When IESO, Portal URLs added to 'Trusted Sites' zone in Windows 7 and IE 8.0/9.0
General Security Level for zone	Medium	Medium	Medium
.NET Framework			
	No stipulation on all settings	No stipulation on all settings	No stipulation on all settings
.NET Framework-reliant components			
	No stipulation on all settings	No stipulation on all settings	No stipulation on all settings
Active X Controls and Plug-ins			
Allow Previously unused ActiveX controls to run without prompting	Enable	Enable	Enable
Allow Scriptlets	No stipulation	No stipulation	No stipulation
Automatic prompting for ActiveX controls	Enable	No stipulation	No stipulation
Binary and script behaviors	Enable	Enable	Enable
Display video and animation on a webpage that does not use external media player	No stipulation	No stipulation	No stipulation
Download Signed ActiveX Controls	Enable	Enable	Enable
Download Unsigned ActiveX Controls	Prompt	Prompt	Prompt
Initialize and script ActiveX controls not marked as safe	Disable (prompt acceptable)	Enable	Enable
Run ActiveX controls and plug-ins	Enable	Enable	Enable
Script ActiveX	Enable	Enable	Enable

Parameter	When IESO Portal URLs added to 'Trusted Sites' zone in XP-SP2 and IE 7.0	When IESO, Portal URLs added to 'Trusted Sites' zone in Vista and IE 7.0	When IESO, Portal URLs added to 'Trusted Sites' zone in Windows 7 and IE 8.0/9.0
controls marked as safe			
Downloads			
Automatic prompting for file downloads	Enable	Enable	Enable
File Download	Enable	Enable	Enable
Font Download	Enable	Enable	Enable
Microsoft VM			
Java Permissions	Medium Safety		
Java VM			
Java permissions	Medium safety	N/A	N/A
Miscellaneous			
Access data sources across domains	Prompt or Enable	Prompt or Enable	Prompt or Enable
Allow META REFRESH			
Allow scripting of Internet Explorer Web browser control	No stipulation	No stipulation	No stipulation
Allow script initiated windows without size or position constraints	No stipulation	No stipulation	No stipulation
Allow web pages to use restricted protocols for active content	No stipulation	No stipulation	No stipulation
Allow websites to open windows without addresses or status bars	No stipulation	No stipulation	No stipulation
Display mixed content	Enable	Enable	Enable
Don't prompt for client certificate selection when no certificates or only one certificate exists - (i.e. automatic	Enable	Enable	Enable

Parameter	When IESO Portal URLs added to 'Trusted Sites' zone in XP-SP2 and IE 7.0	When IESO, Portal URLs added to 'Trusted Sites' zone in Vista and IE 7.0	When IESO, Portal URLs added to 'Trusted Sites' zone in Windows 7 and IE 8.0/9.0
certificate presentation)			
Drag and drop or copy and past files	Enable	Enable	Enable
Include local directory path when uploading files to a server.	Enable	Enable	Enable
Installation of desktop items	Prompt	Prompt	Prompt
Launching applications and unsafe files	Prompt	Prompt	Prompt
Launching programs and files in an IFRAME	Prompt	Prompt	Prompt
Navigate sub-frames across different domains	Enable	Enable	Enable
Open files based on content, not file extension	Enable	Enable	Enable
Software channel permissions	Medium Safety	Medium Safety	Medium Safety
Submit non-encrypted form data	Enable	Enable	Enable
Use Phishing Filter	Enable	Enable	Enable
Use Pop-up blocker	No Stipulation	No Stipulation	No Stipulation
User data persistence	Enable	Enable	Enable
Web sites in less privileged web content zone can navigate into this zone	Enable	Enable	Enable
Scripting			
Active scripting	Enable	Enable	Enable
Allow paste operations via script	N/A	N/A	N/A

Parameter	When IESO Portal URLs added to 'Trusted Sites' zone in XP-SP2 and IE 7.0	When IESO, Portal URLs added to 'Trusted Sites' zone in Vista and IE 7.0	When IESO, Portal URLs added to 'Trusted Sites' zone in Windows 7 and IE 8.0/9.0
Allow programmatic clipboard access	Prompt	Prompt	Prompt
Allow status bar updates via script	Enable	Enable	Enable
Allow websites to prompt for information using scripted windows	Enable	Enable	Enable
Scripting of Java applets	Enable	Enable	Enable
User Authentication			
Logon			

Internet Explorer Pop-up Blocker with Windows XP-SP2 / Vista and Windows 7 and the Portal

54 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.

55 This functionality continues as is with Internet Explorer 7.0 under Windows XP and Vista and also Internet Explorer 8.0/9.0 under Windows 7. The directions included here apply to all the combinations of Windows XP and IE 7.0 and Windows Vista and IE 7.0, Windows 7 and IE 8.0/9.0.

Internet Explorer Turn Pop-up Blocker On or Off

56 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 2-8.

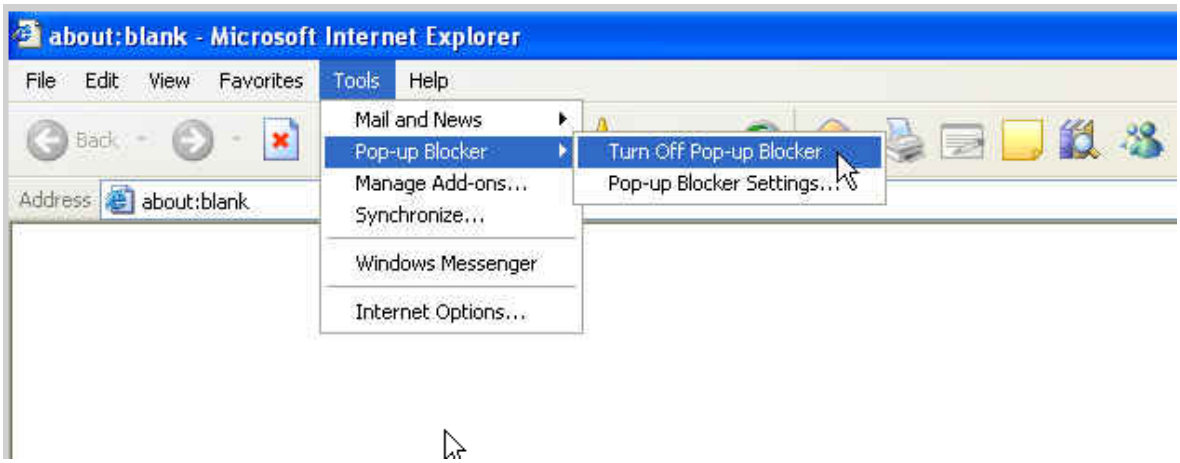


Figure 2-8: Internet Explorer, Enabling or Disabling Pop-up Blocker

Internet Explorer Configure Pop-up Blocker Settings

57 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 2-9.
3. The Pop-up Blocker Settings windows will activate See Figure 2-10
4. Select the desired Filter 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 filter level 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 2-11). This will allow the proper functioning of Energy Market Application and Portal, no matter what the filter level setting.

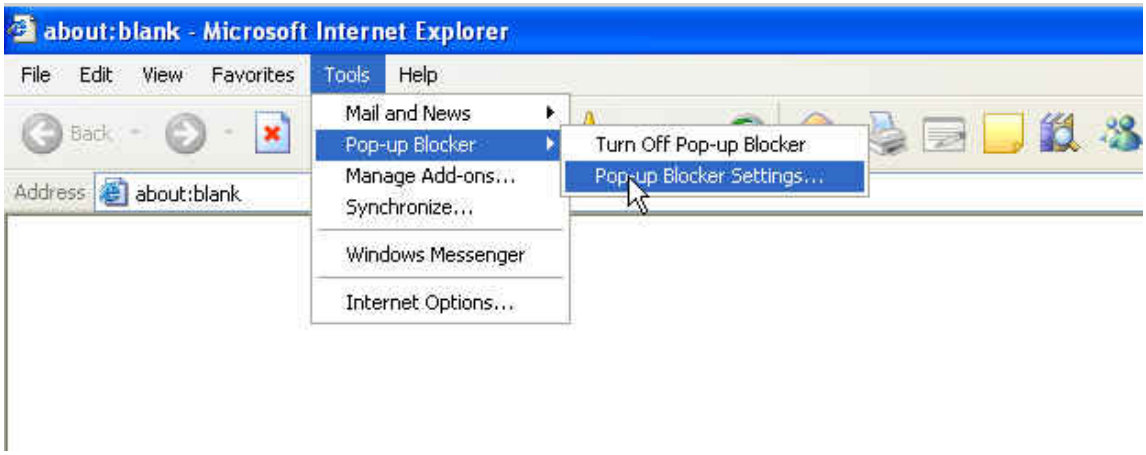


Figure 2-9: Internet Explorer, Activating Pop-up Blocker Settings

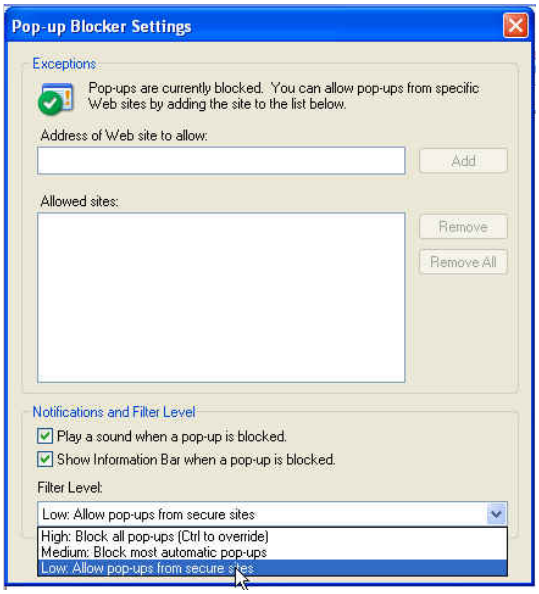


Figure 2-10: Pop-up Blocker Settings Window Filter Setting for Portal & Energy Market Application Use

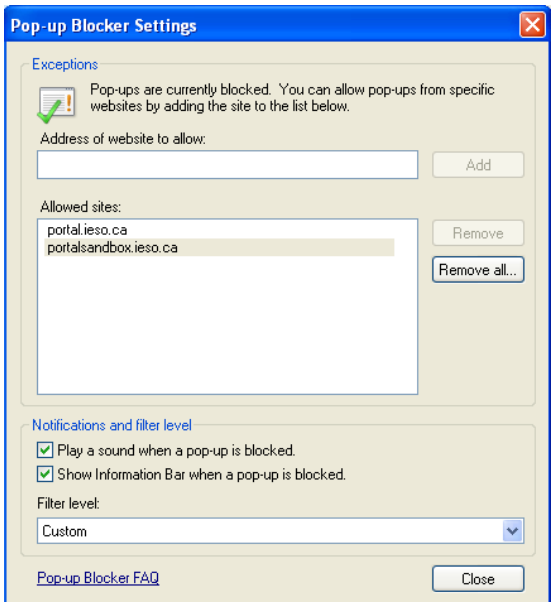


Figure 2-11: Addition of Portal URL to Allow Web Site List for Pop-ups

Sun Java Runtime Environment

58 Please refer to the *IESO* Supported Client Platform web page for the required Java runtime environment. Obtaining this software from the Oracle - Sun 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.

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

60 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.

61 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.

62 Ensure that 'Enable logging' is checked under Debugging in the Java control panel.

63 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 MPI or uses Internet Explorer.

64 Ensure that 'SSL 3.0' is checked under Security in the Java control panel and in Internet Option in IE. See Figure 2-12 below. Also, ensure that all other boxes under Security are checked except for 'Use SSL 2.0' and 'Use TLS 1.0' unless the user has other java applications that need these security protocols. 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.

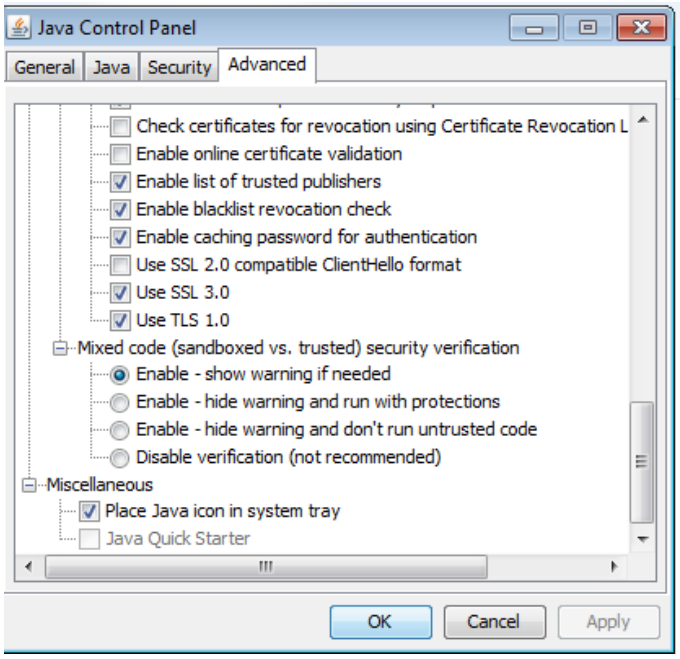


Figure 2-12: Java Control Panel Settings

IESO Java Policy File

65 A special *IESO* Java, policy file with the file name "**.java.policy"** (note the dot at the beginning of the filename) is required for successful *IESO* Energy Market Application processing on the workstation when using Internet Explorer as the browser for the Energy Market Application within the portal and is also required for uploading multiple files within the IESO Portal Collaboration communities. It has also been updated for java security needs required for release of Java 1.6.0_29 and above This is a simple text-format file available from the *IESO* Technical Interfaces page. It must be installed in each user's "C:\Documents and Settings*userID" (e.g.* C:\Documents and Settings\smithj*)* directory on the workstation where *userID* represents the login ID for the user. Users should not use the previous versions of the java policy file. Software downloads page The latest version of the .java.policy file for use with the Energy Market Application in the Portal is expected to have the following content for java permissions:

grant {
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.io.FilePermission "<<ALL FILES>>", "read, write";
permission java.io.FilePermission "C:\Documents and Settings\"user's domain name here"\My Documents", "read, write";
permission java.util.PropertyPermission "*", "read, write";
permission java.lang.RuntimePermission "queuePrintJob";
permission java.lang.RuntimePermission "stopThread";
permission java.lang.RuntimePermission "modifyThreadGroup";
permission java.lang.RuntimePermission "modifyThread";
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,resolve";
permission java.net.SocketPermission "142.9.6.121:443", "connect,resolve";
};

Without the java policy file with the above content in the home directory location for each user, the Energy Market Application applet java code will not function correctly. 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.

66 To download the file from the Technical Interfaces page the user can right mouse button click on the file's POL link on the web-site and choose to save to the required location as show in Figure 2-14. This will activate the typical Windows "Save As" window to allow the user to choose the directory location to save the file to.

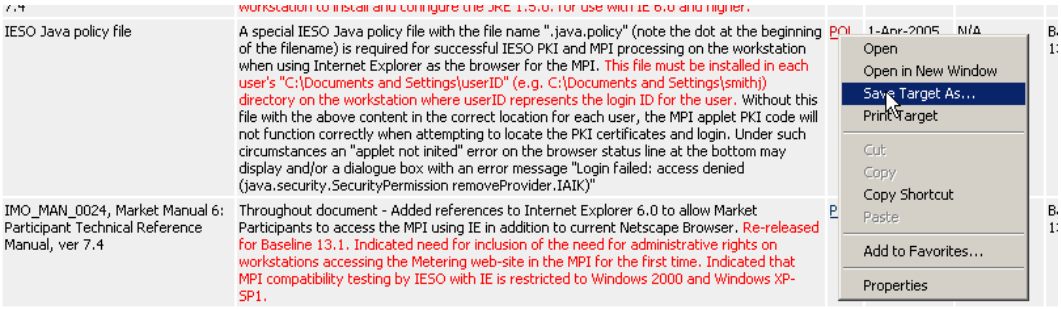


Figure 2-13: Right Mouse Button 'Save Target as ..." Function to Download Java Policy File

67 The file type 'policy' is not a normal registered file type and this is not required for successful download of the *IESO* '.java.policy' file. To download the file, the user must choose the 'Save as type' option "All Files" and choose the appropriate C:\Documents and Settings\UserID directory path. The file name must not be changed. See Figure 2-15. Once this has been done use of the Energy Market Application within the portal with IE should be successful.

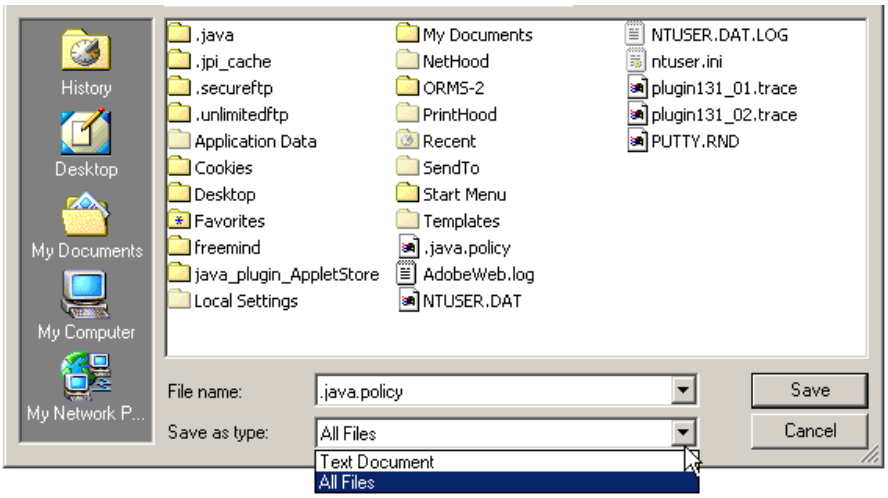


Figure 2-14: File type Selection to Download Java Policy File

68 Prior or after download, Windows XP, Vista and Windows 7 users (or administrators) may create a 'policy' document file type, extension to make the purpose of the file more explicit. To do so, after opening Windows Explorer (or any window), select the 'Tools' menu, then 'Folder Options…' and then the 'File Types' tab selection. See Figure 2-16 for the resultant window.

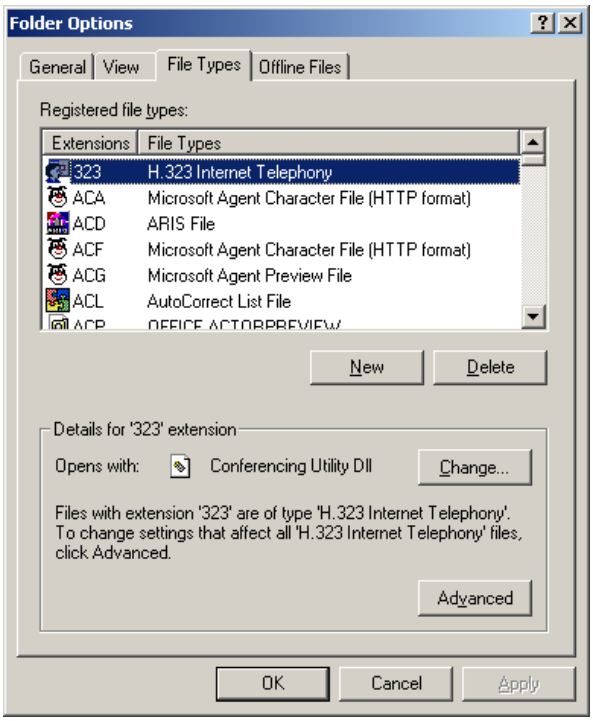


Figure 2-15: Folder Options, File Types Listing window

69 Click in the 'New' button to activate the 'Create New Extension' window as shown in Figure 2-17 and type in 'POLICY' in the file extension field and leave the Associated File Type as <New>. Click on the OK button.

Figure 2-16: Create New Extension Window

70 The Folder Options window will now typically indicate some details for the 'POLICY' extension and that files of the 'POLICY" extension are of type FT000001, (or FT000002 and so on if other customized file extensions have been created previously, Windows creates the numbered file types automatically). See Figure 2-18 for an example.

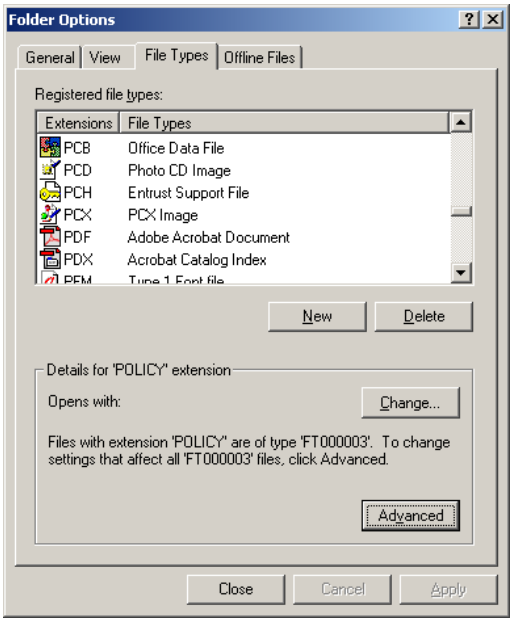


Figure 2-17: Folder Option Window with Detail on 'POLICY' extension shown.

Click on the 'Advanced' button in order to activate the 'Edit File Type' window as shown in Figure 2-19.

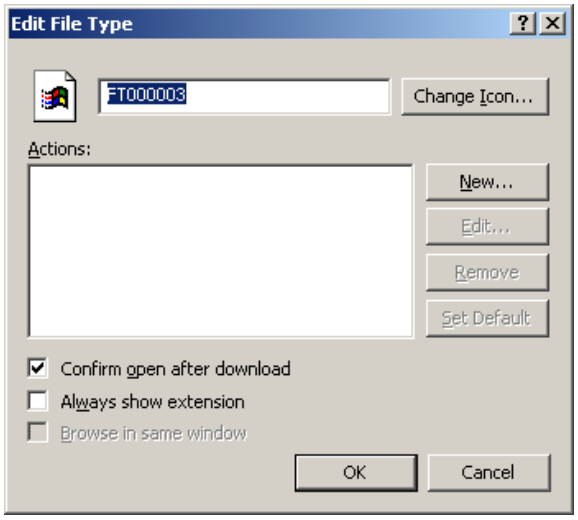


Figure 2-18: Edit File Type Extension Window

Replace the 'FT00001 entry (or FT000002..FT000003 etc.), with the term 'Java Policy File" for ease of identification of the file type and then click on the 'OK' button. Ensure that the correct file type for the 'POLICY' extension is being changed and not some other file type.

Correct file extension editing will let the user see that the '.java.policy' file is of the 'Java Policy File' type in folder windows.

Internet Connection

71 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 dial-up 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

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

73 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) or Frame Relay switched network. *Participants* who require high performance or reliability may wish to consider the PRIVATE or SHARED network alternatives.

74 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

75 The connectivity bandwidth should be at least 64Kbps but higher speeds are recommended to maintain optimal performance.

76 *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 the *IESO* Web site the *participant* will present an *IESO* authentication credentials to the *IESO* Portal). If the presented *IESO* authentication credential is valid, the user will be granted access to the Portal and authorized applications. *Participants* must register for *IESO* authentication credentials. .Registration will be performed as specified in the *Identity Management Operations Guide* (see Technical Interfaces page of *IESO*'s Web site).

77 Secure Sockets Layer (SSL) is used to encrypt the messages between the client system at the *participant* and the 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

78 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*.

79 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.

80 *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.

81 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.

82 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

83 Our telecom service provider has notified the IESO of the end of sales of Frame Relay services. An announcement was made at the Information Technology Standing Committee (ITSC) meeting on September 13, 2011. The IESO will start migrating the existing shared networks from Frame Relay to MPLS beginning in 2012 through 2013. Our telecom service provider will continue to maintain the IESO Frame Relay networks until all *participants* are migrated to MPLS. *Participants* who are currently on the Frame Relay networks will be contacted in advance of any scheduled changes.

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* who 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. For example: Browser based HTTP traffic (TCP/IP port 80) will be allocated its own Class of Service to enable it to be prioritized by the Quality of Service and queuing controls.

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. In cases where FTP is required by a *participant,* TCP Ports 20 and 21 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 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 accounts used for accessing the IESO Portal and secure Reports site will be subject to a number of security provisions. These include:

- Portal 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 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.
- 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 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 new 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* handle all *participant* internal management aspects of the Identity Management processes using the IESO Registration System 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 hav*e 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 SSO and Identity Management System

116 All Portal users login with a U serID account credential for all Portal hosted applications.

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.

118 All Portal 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 the Portal with this type of identity credential.

119 The *IESO Portal User Interface User's Guide* should be referenced for Portal login procedures.

2.3.5 Requirements for Browser Software Compatibility

Workstation Platform for Portal Browser Client

120 The browser client recommended by the *IESO* portal vendor (Oracle) and supported by the *IESO* is as shown on the "IESO Supported Client Platform" web page. Recommended by the Portal vendor but not supported by the *IESO* is: :

- Mozilla Firefox 1.0, 1.5 or 2.0.1
- Safari 2.0

Any of these will work. Not supported but compatible are:

- Mozilla Firefox 1.0 in combination with Sun JVM 1.4.2

Ports

121 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.

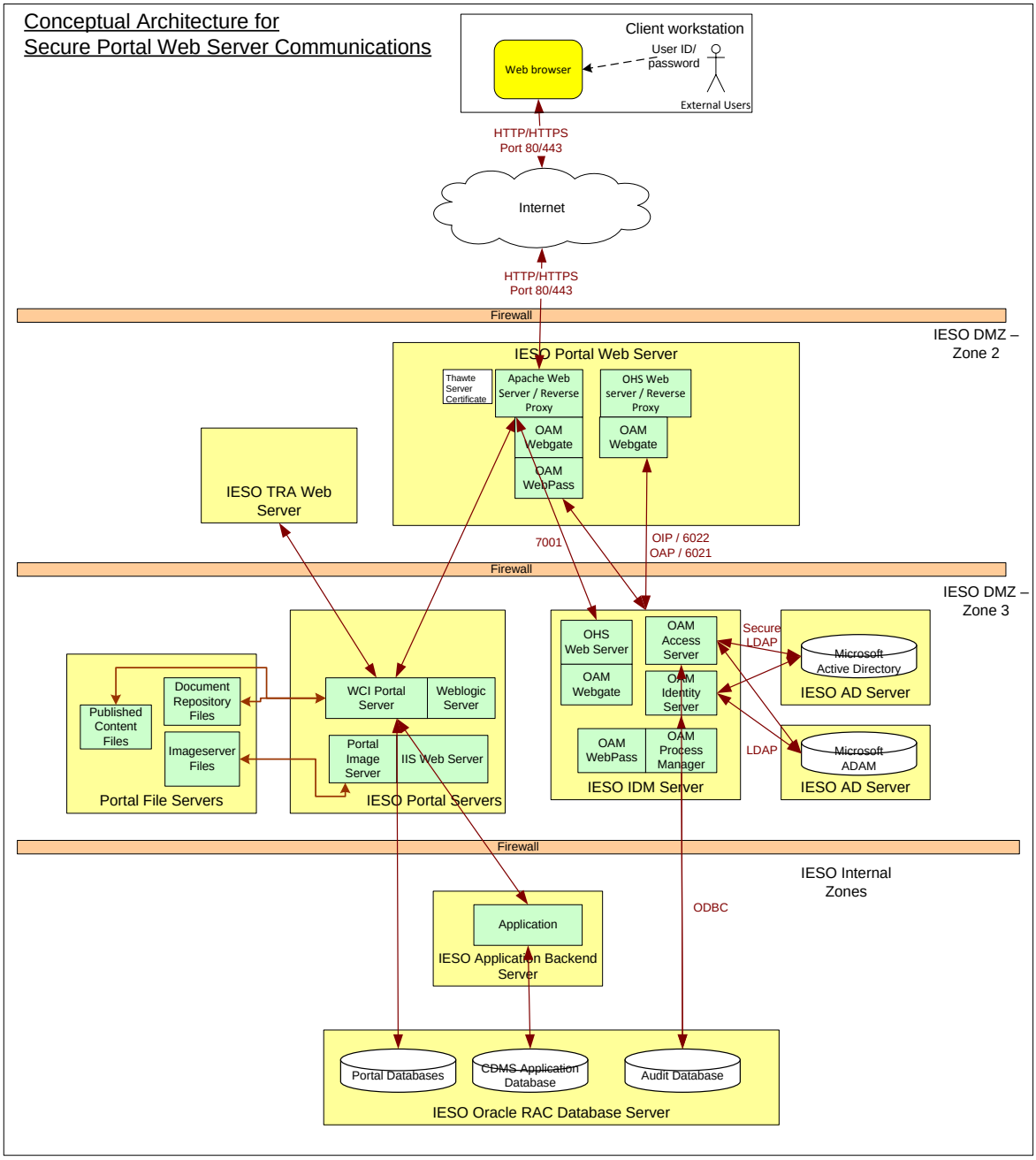


Figure 2-19*: IESO* Portal Co*nc*eptual Architecture

Other Documentation

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

– End *of Section* –

3. Dispatch Information

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

3.1 Dispatch Workstations

124 *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

125 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 XP, Vista and Windows 7 operating systems. Displays may be rendered incorrectly if a Windows Operating System is not used.

126 For Windows XP and above, it is recommended that the client workstation hardware conform to Microsoft's specifications found at:
http://www.microsoft.com/windowsxp/pro/evaluation/sysreqs.mspx

The following provides the minimum hardware requirements:

Processor

127 The minimum required processor speed is 300 M Hz PII or equivalent, however 500MHz, PIII or higher or equivalent is recommended.

Memory

128 The PC must have a minimum of 256 megabytes of internal RAM. For better performance however, 512 megabytes RAM and higher is recommended.

Hard Disk

129 The PC must have at least four gigabytes of available disk space.

Interface Cards

130 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

131 The supported monitor must be SVGA 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 1280 x 1024 pixels is however, recommended.

Sound Card

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

Printer

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

Other Components

134 Additional components that should be included with your PC are a compatible two-button mouse, keyboard, and 1.44 MB high-density floppy disk drive.

3.1.2 Software Requirements

Operating System

135 The PC should be operating with Windows XP, Vista or 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 7 or IE 8 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 use 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*.

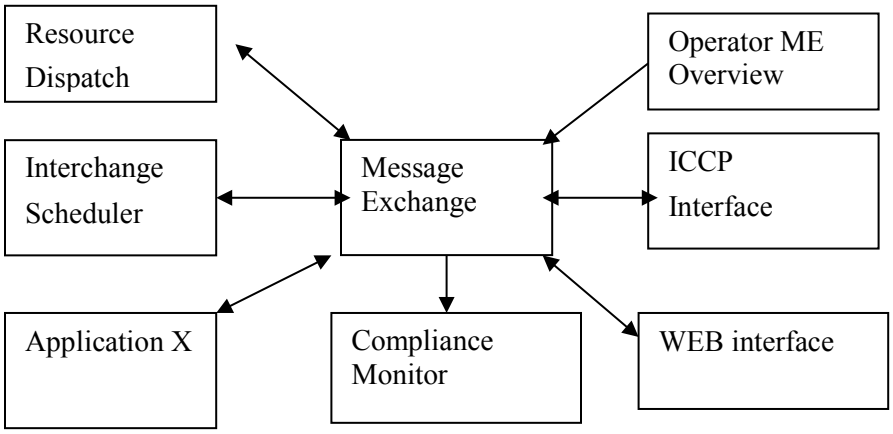


Figure 3-1: Message Exchange Interfaces

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 Our telecom service provider has notified the IESO of the end of sales of Frame Relay services. An announcement was made at the Information Technology Standing Committee (ITSC) meeting on September 13, 2011. The IESO will start migrating the existing real time networks from Frame Relay to MPLS beginning in 2012 through 2013. Our telecom service provider will continue to maintain the IESO Frame Relay networks until all *participants* are migrated to MPLS. *Participants* who are currently on the Frame Relay networks will be contacted in advance of any scheduled changes.

168 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.

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

170 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.

171 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. A dedicated dial-up telephone line connected to the DNP3 device to enable remote maintenance.

c. Space to house the customer premises equipment in a suitable environment (e.g. dry, clean, 0 – 40°C, free of Electro-Magnetic interference, etc.)

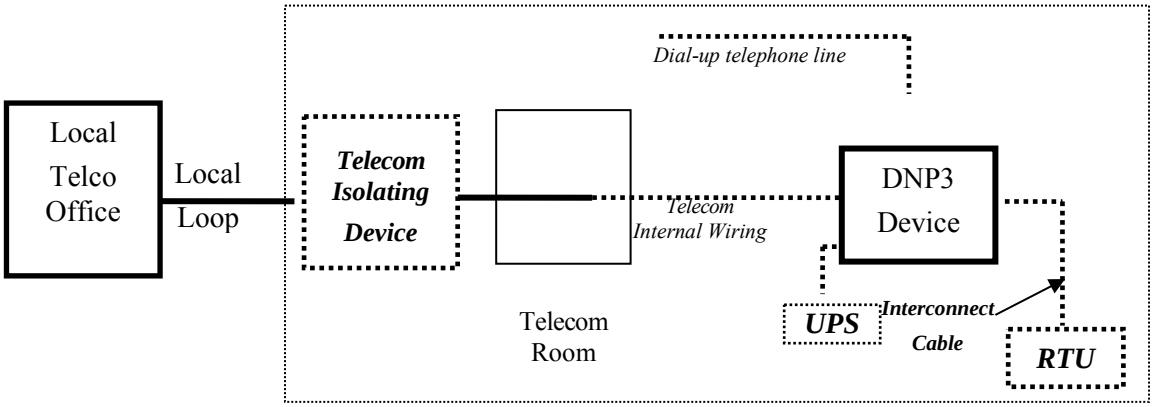
d. A suitable power source for the customer premises equipment (typically a reliable source of 120V ac, 60 Hz – usually from a UPS with a total load capacity of 500 Watts) with at least 8 hours of survivability after loss of commercial power.

e. Access for maintenance personnel as needed.

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

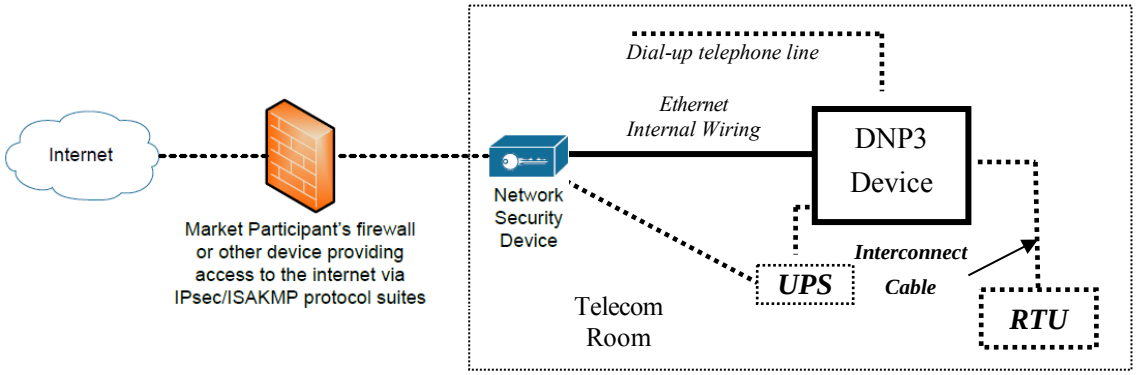
g. A point of contact (a person and telephone number) to enable the *IESO* to request repairs by the *participant* for telemetry failures.

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

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

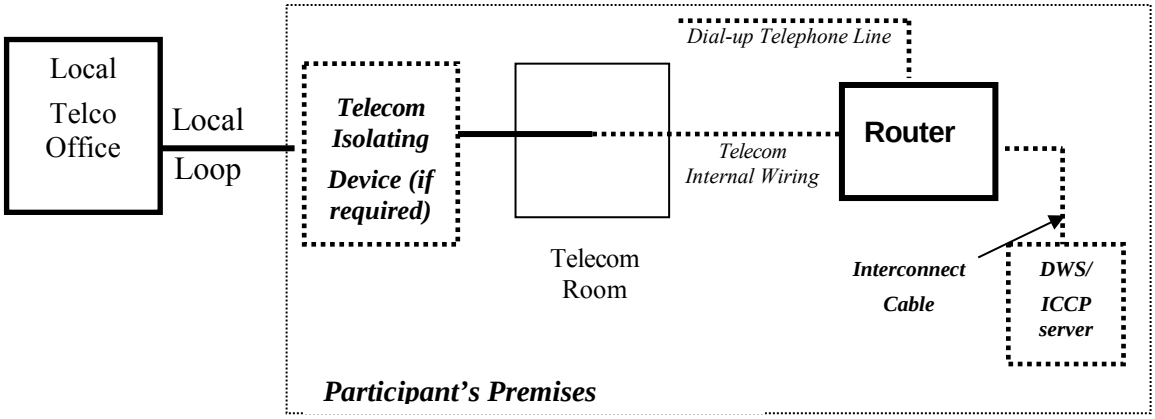
a. Access for the communications carrier to the *participant* site to install a local loop and other customer premises equipment.

b. A dedicated dial-up telephone line connected to the Router to enable remote maintenance.

c. 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.)

d. A suitable power source for the customer premises equipment, typically a reliable source of 120V ac, 60 Hz.

e. 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

173 Voice communications are broken into two categories:

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

174 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*.

175 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

176 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

177 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.

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

179 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.

180 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.

181 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

182 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

183 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

184 (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

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

186 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.

187 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.

188 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

189 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.

190 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.

191 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.

192 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.

193 The following RTU manufacturers using the DNP 3.0 protocol have been qualified for use by the *IESO*:

194 **Vendor Name:** GE Energy / GE Harris

195 **Device Name:** D20, D200, and D25 RTUs,

196 **Vendor Name:** Quindar

197 **Device Name:** XPPQ and Scout RTUs,

198 **Vendor Name:** PML

199 **Device Name:** 7330, 7500, 7600, 7700 and 8500

200 **Vendor Name: Cooper Power Systems (**Cybectec)

201 **Device Name:** SMP Gateway, SMP I/O

202 **Vendor Name:** Schneider Electric

203 **Device Name:** Quantum PLC System with a DNP3 Processor,

204 **Vendor Name:** Bow Networks

205 **Device Name:** Advantech Industrial PC Part # UNO-2160-IDA0

206 **Vendor Name:** Schweitzer Engineering Laboratories, Inc.

207 **Device Name:** SEL-3332 Intelligent Server.

208 **Vendor Name:** Telvent

209 **Device Name:** Sage 3030 Substation Automation Platform.

210 **Vendor Name:** Schweitzer Engineering Laboratories, Inc.

211 **Device Name:** SEL-3351, 3354 & 3530 System Computing Platform.

212 **Vendor Name:** ABB

213 **Device Name:** ABB RTU560

214 **Vendor Name:** Subnet Solutions Inc.

215 **Device Name**: SEL/SUBNET 1102

216 **Vendor Name :** Customized Energy Solutions.

217 **Device Name**: SecureNet-RT

218 **Vendor Name:** Nova Tech LLC

219 **Device Name**: Orion LX Data Concentrator

220 Further information on additional qualified devices or assistance on RTU set-up and configuration is available from the *IESO*.

221 The *IESO* may add qualified devices from other manufacturers. *Participants* should contact the *IESO* to get information on the current set of qualified devices.

222 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.

223 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.

224 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

225 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.

226 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.

227 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.

228 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

229 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

230 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*.

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

Analogue Points

232 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

233 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

234 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.

235 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

236 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*.

237 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.

238 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

239 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.

240 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.

241 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.

242 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.

243 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.

244 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.

245 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

246 *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.

247 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.

248 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.

249 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*.

250 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.

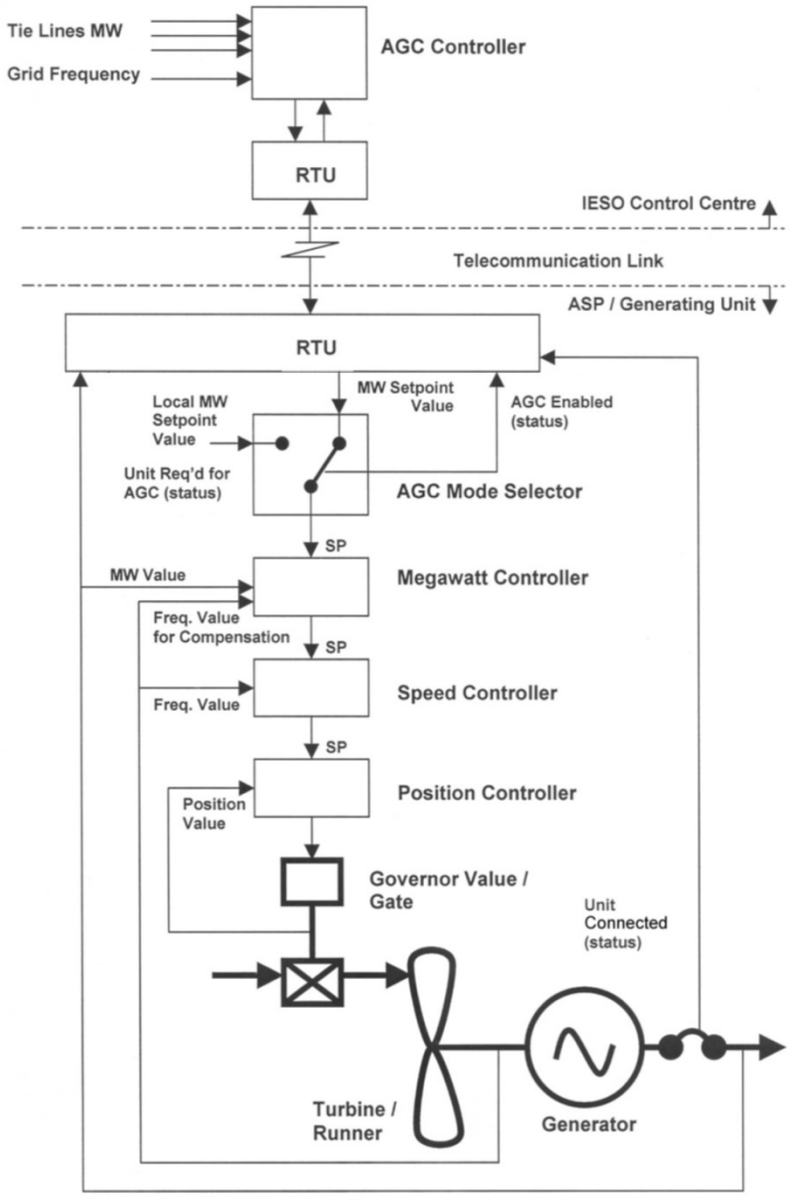


Figure 4- 1 Block Diagram of Typical AGC Control Arrangement for Generation units With Remote MW Setpoint Control Capability

251 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.

252 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.

253 Two models of RTU have been qualified for use by the *IESO* for *AGC*. These are GE models D20/200 and D25 RTUs.

5. Market Applications

5.1 Market Application Systems Information

5.1.1 Overview of Dataflow Systems

254 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*.

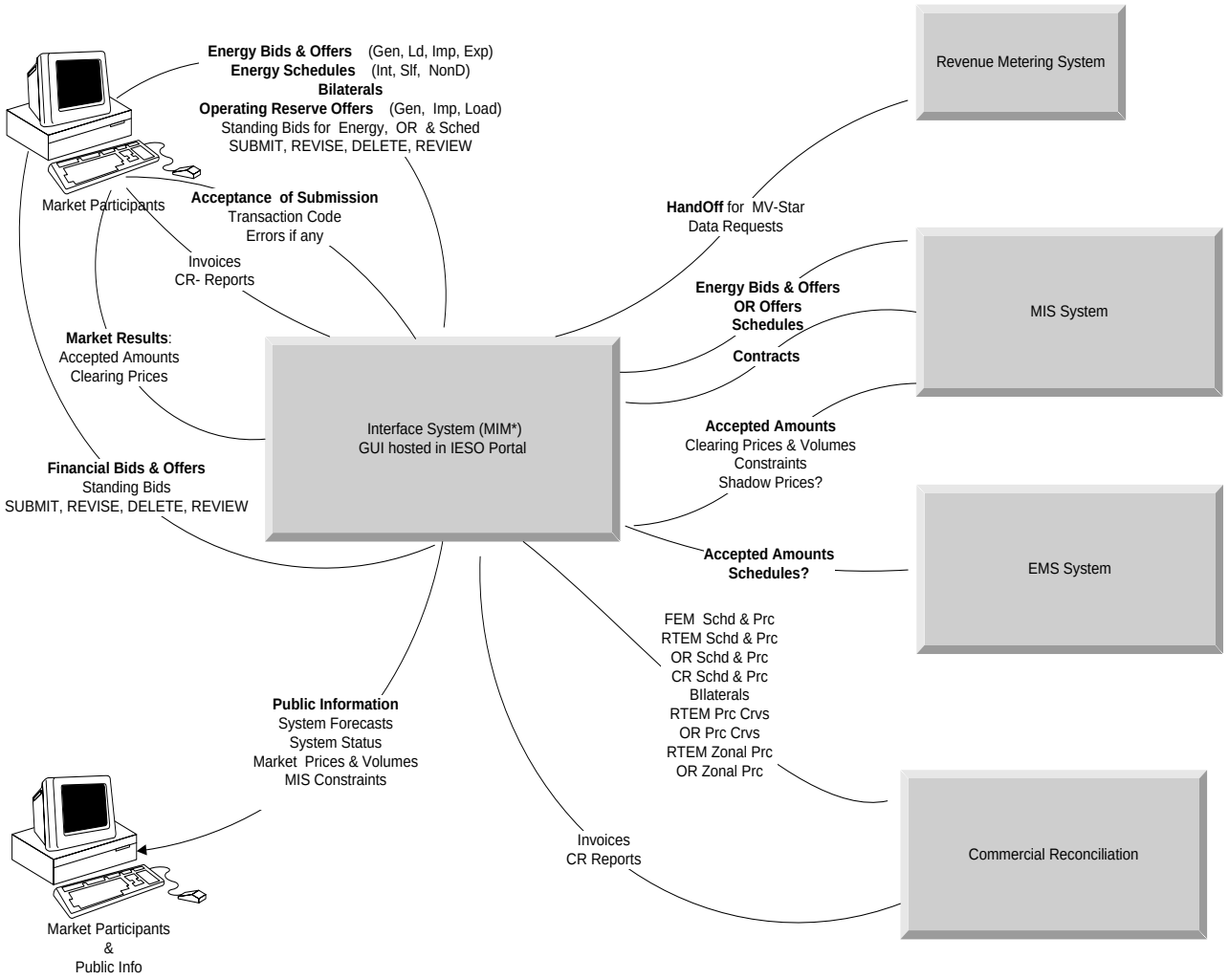


Figure 5-1: Overview of Dataflow from the MP to IESO systems

5.1.2 Energy Market Application

255 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

256 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.

257 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

258 A single transmission file may contain one or more *bids*. The entire file will be considered as o ne 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

259 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

260 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.

261 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.

262 *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

263 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.

264 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

265 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 IESO Reports web server.

266 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.

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

Settlement Statement Files

268 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.

269 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.

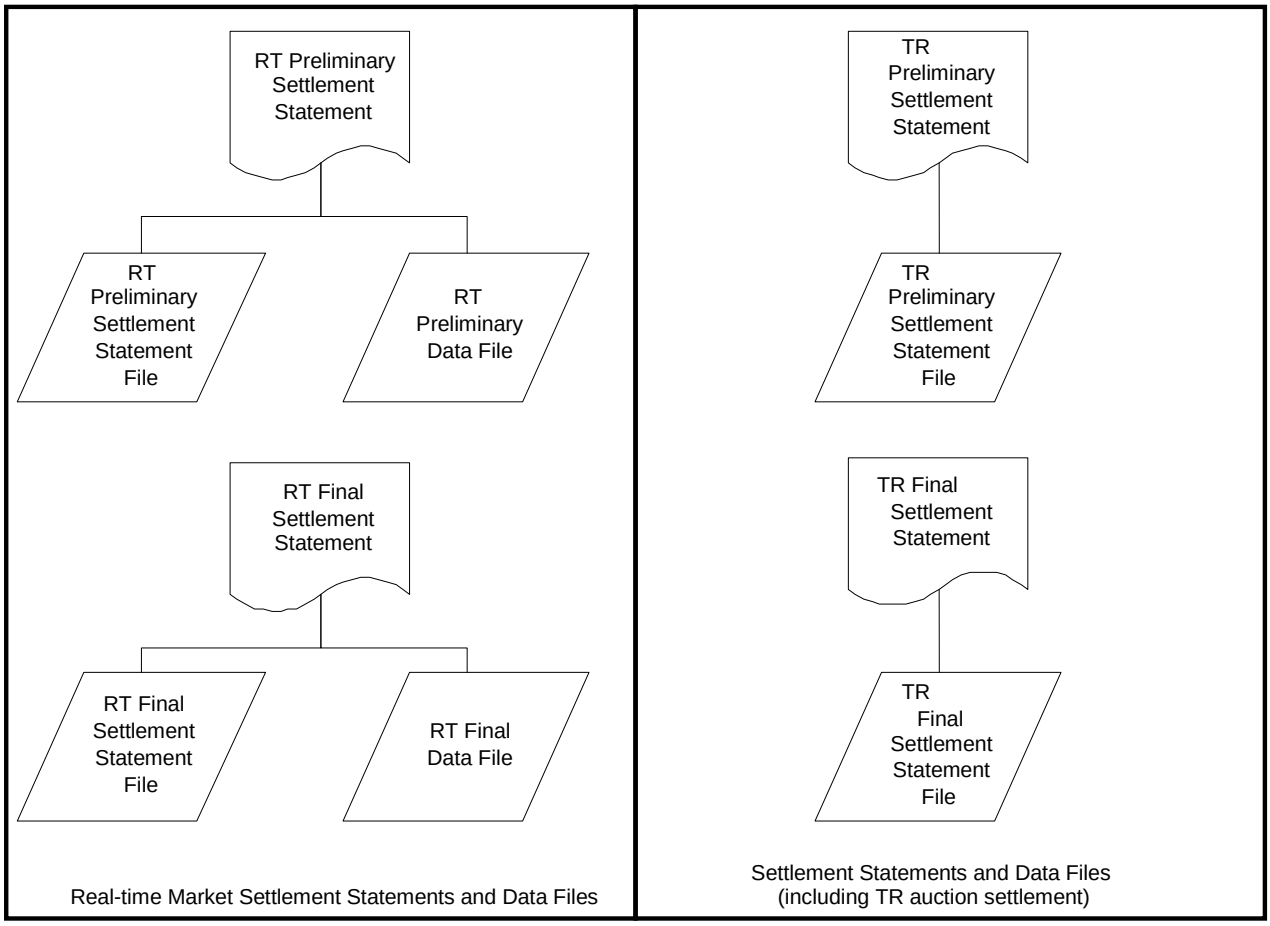


Figure 5-2: Schematic Overview for Settlement Statements and Data Files

270 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. A fter a predetermined *notice of disagreement* period, a final statement is generated.

271 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

272 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

273 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

274 Within the IESO Portal the On-line Outage Forms application will provide functionality to permit secure submission and historical search for outage data previously submitted via IESO Form 1360: Outage Request. Over time outage data submission functionality will be updated to meet current requirements

5.1.6 Energy Market Application Interfaces

275 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.

276 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.

277 The MIM Application Interface (API) code will allow *participants* to customize their interface to interact with the *IESO*. U sing 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

278 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.

279 Client-side certificates are required to access the MIM via the API. However as of summer 2011 a transition to UserID/Password identity credentials will be supported. To use the API, it is necessary to establish an SSL session with the MIM Web server. *Market partipants* 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.

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

- Minimum 128 MB of system memory;
- Intel based PC running Windows XP SP2, or higher;
- Java 2 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
- Client-side digital certificates and the software to establish a secure (e.g. SSL) session with the MIM server.

281 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.

5.1.7 Portal Metering Application

282 The IESO Web based Metering application securely available via the Portal allows *participants* to retrieve *participant* metering data by navigating to the Metering application page. The Metering page provides access to recorded quantities of interval meter data, available in tabular or graphical format. *Participants* can also:

- Download the data to their computers in a way that is easy to import into spreadsheet programs or other data systems.
- Generate reports using the data within the metering database.

- Grant other *participants* access to specific delivery points for a time period the *participant* defines.

5.1.8 Portal Transmission Rights Auction Application

283 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 IESO Compliance Tool Application

284 The web based IESO Compliance Tool (ICT) application allows participating *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 IESO Compliance Tool link and access it without logging in again. The IESO Compliance tool 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 Registration System Application

285 The web based IESO Registration system application 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 IESO Registration System link and access it although the will have to login as SSO is not set up with it. The IESO Registration System enables the *participant* to register who they are and register for enrolment in markets or programs and request system access for IESO systems.

5.2 Funds Administration

5.2.1 HTML and Text File Invoices

286 *Invoices* will be distributed to the *participants* via XML, HTML or text files hosted on the IESO 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*.

287 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

288 Emailing of *invoices* and statements will not be available as an option.

5.2.3 Fund Transfers

289 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.

290 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, can not 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: Forms

This appendix contains a list of the forms and agreements associated with Participant Technical Reference Manual. These are available on the *IESO* public Web site on the Market Entry Page. The forms and agreements included are as follows:

Form Name	Form Number

– End of Section –

Appendix B: 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 2 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

– **End of Document –**