INDEPENDENT MARKET OPERATOR

Notice of SHA256 certificate upgrade

16 April 2015

WEMS and the Gas Bulletin Board are currently using SHA-1 SSL certificates, using 128-bit encryption algorithms. These certificates will be upgraded to SHA-2 (256-bit) SSL certificates.

What will be affected?

The SSL certificates are used to secure the connection to WEMS and the Gas Bulletin Board over https.

Why are the certificates being upgraded?

We are upgrading the SSL certificates because:

- SHA-1 certificates are no longer considered strong enough to offer sufficient protection to encrypted traffic:
    - Why Google is Hurrying the Web to Kill SHA-1: https://konklone.com/post/why-google-is-hurrying-the-web-to-kill-sha-1
- Some browsers have already started to show warnings (and eventually errors) for sites that do not use 256-bit SSL certificates. As of today, 16 April 2015, Google Chrome has started showing an error icon to flag that they do not consider security to be sufficient (this reflects a tightening of security policy, as opposed to a weakening of the security that is currently in place).
- Microsoft and Google have both announced SHA1 deprecation policies:
    - Microsoft SHA1 Deprecation Policy: http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx
    - Google – Gradually sunsetting SHA-1: http://googleonlinesecurity.blogspot.com.au/2014/09/gradually-sunsetting-sha-1.html

Who will be affected?

SSL security is in place for WEMS and the Gas Bulletin Board. The majority of users will be unaffected by this change.

Users of Microsoft Internet Explorer 8 who are running Windows XP will need to ensure that Windows XP Service Pack 3 has been applied.

Rollout schedule

The following rollout schedule is planned:

Service	URL	SHA-2 Rollout Date
WEMS - Market Trial	https://wems-mkt.imowa.com.au/	16 April 2015
Gas Bulletin Board - Trial	https://gbb-trial.imowa.com.au/	16 April 2015
WEMS	https://wems.imowa.com.au/	30 April 2015
Gas Bulletin Board	https://gbb.imowa.com.au/	30 April 2015

We recommend that users of WEMS and the Gas Bulletin Board conduct testing in the trial environments to verify that they will be unaffected by the certificate upgrade. Verification should be as simple as checking that the pages can be loaded correctly using the supported operating system and browser.

Please contact the IMO if you encounter any difficulty with the certificates in the trial environment, or if the planned timeframes will cause a problem.