# Notification of Changed SSL Version

**Date: April 2015**

## Introduction

As a HLA/HLMT customer/agent, we want to remind you of an upcoming change regarding supported encryption protocols for internet browsers that access HLA/HLMT applications and services.

On 15 October 2014, Google researchers published details on the security vulnerability (CVE-2014-3566) that affects the Secure Socket Layer (SSL) version 3.0 (SSLv3) encryption protocol. This vulnerability may allow attackers to extract data from secure connections.

## Details of Change & Recommendation

In order for seamless access to our applications, customers/agents must ensure their browsers use Transport Layer Security (TLS) encryption, version 1.0 or higher.

Customers are encouraged to update their browser to the latest versions and remove SSL version 3.0 from their Integrations across all environments.

For reference purposes only, see the following:

1. Microsoft Internet Explorer Users

2. Mozilla Firefox Users

3. Google Chrome Users

Users who attempt access on or after 29th March 2015 using a browser that does not support TLS 1.0 or higher, will have interruption while accessing to our applications.