Gas Network Innovation Competition Full Submission

Supplementary Answer Form

Project: _Real-Time Networks_____

Tick if this answer has been provided verbally: ☐

Project code	SGN_GN_03	Question Number	4
Question date	25/08/2015	Answer date	27/08/2015
Submission section question relates to	5.3		
Topic			
Question	The cloud computing provider is an American company based in San Francisco. Have the server locations and security implications been addressed?		
Notes on question			
Answer	Splunk Cloud (Cloud service) is a single-tenant service hosted in AWS (Amazon Web Services). Every customer has a dedicated environment provisioned in order to meet the strictest enterprise security requirements. Dedicated environments ensure that the data is never co-mingled with data from another customer and further assures that access to the data is strictly limited to provisioned users. Whilst AWS is an American company, with a worldwide network of locations, a contract with AWS can specify the location(s) where Customer Data can be processed within the AWS Network. This includes the EU (Dublin) Region, the EU (Frankfurt) Region, the US East (Northern Virginia) Region, the US West (Northern California) Region, the US West (Oregon) Region, the South America (Sao Paulo) Region, the Asia Pacific (Tokyo) Region, the Asia Pacific (Singapore) Region and the Asia Pacific (Sydney) Region. It is stated that "Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s)" The Splunk cloud service can be run within Europe, either from the Dublin or the Frankfurt datacentre. This results in management within EU data protection laws.		

	The cloud service uses industry standard secure socket layer (SSL) encryption for data in transit. Each forwarder, user session and archive is secured in this manner with no exceptions. Splunk offers data encryption at rest using advanced encryption standard (AES) 256-bit encryption. Customers can choose to run a hardware security module (HSM) under their own management while owning their own encryption keys, or have Splunk manage the HSM on their behalf.
Attachments	