Policy Statement – Texas CJI Cloud Service Providers

Guidance Dated 03/22/2018

The Texas Department of Public Safety (DPS), as CJIS Systems Agency (CSA) for the state of Texas, has implemented a modified Signatory Page to be made a part of any Security Addendum involving sub-contract services or support for cloud solutions.

Of concern is the need to ensure that Law Enforcement agencies are alerted prior to the introduction of any possible third party involvement as it relates to cloud services. Knowledge of where an agencies data is being stored and who may have possible access to the data is critical to information security.

Items to consider include whether CJI data may be considered under encryption prior to being submitted and whether the data will remain encrypted “at rest” until returned to the LE agency. Typically if this involves any form of processing outside of the secure LE physical control then it would be considered unencrypted for a time at which point the vendor and any one with either physical, logical or remote access is subject to the full requirements of the FBI CJIS policy – to include fingerprint based background and security awareness.

In the event an existing support vendor develops a cloud solution as part of enhancing services with an agency, an updated Security Addendum would be required between the agency and vendor(s) to accommodate for the addition of such services.

For services involving cloud solutions we encourage agencies to reach out with any questions or concerns as it may relate to meeting FBI CJIS compliance.