Cloud Computing FAQ

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FGBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

1. Q) What is cloud computing?

A) Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The "cloud" spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

Cloud computing comes in many forms, but the general idea is that your data (and sometimes your software) runs at a facility which is shared by other clients of the cloud provider. How much data and software are stored at these facilities depends on your usage. Some cloud providers will charge based on the space being utilized, and some provide a flat fee for the use of their equipment and facilities. The bottom line with cloud computing is that the data and/or software are not physically located within your data center.

2. Q) Are all cloud solutions the same?

A) No they are not. There are public cloud providers and private cloud providers. Each cloud provider may offer various options, such as an "education" cloud, a "public" cloud, and a "government" cloud. Private cloud providers are companies that offer cloud services on a smaller scale, and to a selected group of customers. Some cloud providers will offer Infrastructure as a Service (IaaS) which is renting space on a provider's equipment where you can configure your own virtual computing environment. Other providers will offer Software as a Service (SaaS) which allows you to use an already working software application in a cloud environment.

When storing performing transactions with, or simply storing, criminal justice information in the cloud, you must remember that all CJIS Security Policy rules must be complied with as if those computers and that data were in use at your facility.

3. Q) Where is my data really stored?

A) When contracting with a cloud provider, your data can be stored in multiple locations or just one location depending on your provider. For example, Micorsoft's Government cloud is in two cities in the U.S. and your data could be stored in both places. The limitation for you when considering a cloud solution is to remember that all criminal justice information must not be transmitted or stored outside of the United States.

4. Q) How do I ensure my data is safe in the cloud?

A) The best way to ensure your data is safe in the cloud is to do your due diligence in vetting the cloud provider. The CJIS Security Policy was put in place to give the agency an opportunity to mitigate risks to a compromise of criminal justice data. It is perfectly acceptable to question a cloud provider as to how they will meet the requirements set forth in the CJIS Security Policy as it pertains to the solution you're looking for. Of course, the best way to make sure your data is safe in the cloud is to make sure that your software encrypts the data at rest and in flight with a FIPS 140-2 compliant encryption routine.

5. Q) Which cloud solutions are CJIS certified in Illinois?

A) None. Illinois, the FBI, and other states do not certify nor recommend any particular cloud provider. Illinois will work with agencies to ensure software solutions and implementations meet CJIS Security Policy requirements, but each solution is vetted on its own merits and not as a software provider as a whole. For example, if Agency A purchases a space on the Amazon cloud, and Agency B does the same thing, it doesn't mean both uses will meet CJIS Security Requirements. Once a Cloud Provider is vetted out through one agency in Illinois, the CJIS Information Security Officer will accept certain aspects of that vetting process for another agency; however, each implementation should be fully vetted prior to purchasing cloud services.

6. Q) We purchased Office 365 Government Cloud for our email, does this mean I can email Criminal Justice Information over the internet?

A) It has been the trend of most software vendors to move over to a cloud solution for their software products. Microsoft has done this with Office 365 and Exchange (their email suite), making it much more cost effective for an agency to purchase cloud email capabilities rather than purchasing their own MS Exchange server. However, this does not mean criminal justice information is secure in Microsoft's cloud email. Agencies must still encrypt any criminal justice information prior to sending that information via email through the internet.

7. Q) Do I need to perform a fingerprint background check on the cloud employees?

A) So now you've purchased, for example, a Microsoft Office 365 cloud solution, but the CJIS Security Policy says that if a private vendor is storing my data then I need to perform a fingerprint background

check on each employee at the facility, and Microsoft has over 200 employees. The Illinois State Police have adopted a policy that if a vendor has had their fingerprint background checks completed by another Illinois State Agency then the CJIS Information Security Officer will accept those background checks performed by one department as have been completed by the second department. There is no need for multiple agencies to conduct the same background check on the same vendor's employees. However, each department has the right to conduct those background checks on their own, should they so choose. Also, if your data is encrypted while moving through, and being stored, at the cloud facility then the need for fingerprint background checks is not necessary. If you're unsure whether or not your cloud provider has been background checked in Illinois, please contact the CISO at leadsiso@isp.state.il.us.