INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Guiding Principles on
Cloud Computing in Law Enforcement

Cloud computing technologies offer substantial potential benefits to law enforcement and government agencies. Cost savings, rapid deployment of critical resources, off-site storage and disaster recovery, and dynamic provisioning of new and additional resources when needed are among the tangible benefits that cloud computing potentially offers to law enforcement agencies of all sizes. Recognizing the sensitivity of law enforcement information, and the special responsibilities that law enforcement has to ensure the accuracy, reliability, security, and availability of data within their control, however, demonstrates some of the challenges that agencies face in evaluating the potential use of this new computing paradigm.

To meet the dynamic operational needs, while maintaining the security of systems and data, law enforcement agencies using or contemplating the use of cloud computing services should ensure that their planning and implementation of cloud solutions satisfactorily address the following key principles. These principles may be embodied in contractual agreements with a cloud service provider or in service level agreements (SLAs), as appropriate.

1) **FBI CJIS Security Policy Compliance – Services provided by a cloud service provider must comply with the requirements of the Criminal Justice Information Services (CJIS) Security Policy (current version 5.1, dated July 13, 2012), as it may be amended.** To the extent that a law enforcement agency puts Criminal Justice Information in the cloud, the cloud provider should warrant that it has the technological and operational capabilities to meet and/or exceed the requirements of the current FBI CJIS Security Policies, and that it will make every reasonable effort to maintain compliance with these policies moving forward. The provider must acknowledge that the FBI CJIS Security Policy places restrictions and limitations on the access, use, storage, and dissemination of Criminal Justice Information and comply by those restrictions and limitations.

2) **Data Ownership – Law enforcement agencies should ensure that they retain ownership of all data.** Data includes all text, numerical data, database records, media files, demographic information, search history, geo-location information, meta data, or any other data and information that law enforcement users or contractors provide to a cloud service provider, or to which the cloud service provider otherwise gains access as a direct or indirect product of the cloud services provided to the law enforcement agency. The cloud provider must provide timely and appropriate notification to the law enforcement agency that owns the data of any legal process made against the cloud provider in regards to that data. No data should be released to any third party without a) proper and timely notification made to the data owner, and b) receipt of the affirmative authorization for release of said data by a duly authorized representative of the data owner, or c) receipt of an official order authorizing release of said data by a duly authorized court with jurisdiction over the data, and then only after adjudication of any legal proceedings challenging release of the data by the data owner. In all instances, the law enforcement data owner must be notified immediately of any completed unauthorized access to their data and of any unlawful or significant attempted access to their data.

3) **Impermissibility of data mining – Law enforcement agencies should ensure that the cloud service provider does not mine or otherwise process or analyze data for any purpose not explicitly authorized by the law enforcement agency.** The cloud service provider should not be permitted to data mine or otherwise process or analyze law enforcement data for purposes not explicitly authorized in the agreement with the law enforcement agency. The cloud provider should not capture, maintain, scan, index, share with third parties, or conduct any other form of data analysis or processing of law enforcement data for such purposes as advertising, product improvement, or other commercial purposes. The cloud provider may process or analyze data as necessary for ongoing and routine performance monitoring to ensure continuity of service and/or to project future dynamic provisioning requirements. The cloud provider may also process information that is made public by the law enforcement agency, either as a matter of policy or as required by law. Any agreement with a cloud service provider must take precedence over and replace any generally applicable privacy, data access or use, or similar policy of the provider which might otherwise permit data mining for purposes not explicitly authorized in the agreement.

4) **Auditing – Upon request, or at regularly scheduled intervals mutually agreed, the cloud service provider should conduct, or allow the law enforcement agency to conduct audits of the cloud service provider's performance, use, access, and compliance with the terms of any agreement.** Audits can be completed internally, by the cloud service provider under conditions and provisions mutually agreed, by outside contractors under conditions and provisions mutually agreed, or by agents of the contracting law enforcement agency at such intervals as are deemed necessary and mutually agreed.

5) **Portability and interoperability – The cloud service provider should ensure that law enforcement data maintained by the providers is portable to other systems and interoperable with other operating systems to an extent that does not compromise the security and integrity of the data.** A law enforcement agency must be able to share and/or transfer law enforcement data with other information systems and resources. Data and applications provided by a service provider should be capable of exchanging data with other

information systems and resources, and should, in-so-far as possible, be capable of exchanging data in agreed non-proprietary standards.

6) **Integrity – The cloud service provider must maintain the physical or logical integrity of law enforcement data.** The cloud service provider must maintain the integrity of law enforcement data through physical or logical separation between the cloud storage and services provided to law enforcement agencies and cloud storage and services, if any, provided to other customers. Law enforcement data may not be commingled with data in the provider's consumer cloud services, or modified in any way that compromises the integrity of the data. If the system is designed to house evidentiary material, then the cloud service provider must maintain records of access to law enforcement data sufficient to allow the law enforcement agency to establish a clear and precise chain of custody for data of evidentiary value. To the extent required by the law enforcement agency for select categories of data, the cloud provider should notify the law enforcement agency if and when it changes the physical location in which the data is stored.

7) **Survivability – The terms of any agreement with cloud service providers should recognize potential changes in business structure, operations, and/or organization of the cloud service provider, and ensure continuity of operations and the security, confidentiality, integrity, access and utility of data.** In the corporate world, mergers, acquisitions, and corporate restructuring are fairly common. Law enforcement agencies must be confident that the terms of any agreement with cloud service providers will include specific provisions to ensure continuity of operations and the continued security, confidentiality, integrity, access, and utility of all data subject to the agreement, irrespective of the commercial viability of the service provider or changes in operations, ownership, structure, technical infrastructure, and/or geographic location.

8) **Confidentiality – The cloud service provider should ensure the confidentiality of law enforcement data it maintains on behalf of a law enforcement agency.** The provider will take all necessary physical, technical, administrative, and procedural steps to protect the confidentiality of law enforcement data. These steps may include physical security measures, access permission requirements, cybersecurity requirements, criminal history background security checks on employees and contractors with access to systems and data, and geographical location limitations. The confidentiality of law enforcement data may be further ensured by customer-held key encryption of the data using encryption processes. The cloud provider should provide a Certificate of Proof of Cybersecurity issued or approved by a duly authorized organization with appropriate credentials to verify the technical and operational capabilities and practices of the cloud provider. The cloud provider should provide timely and appropriate documentation that verifies that it currently maintains Cybersecurity liability insurance in an amount appropriate to the level of risk associated with managing and supporting the law enforcement agency, and agree that it will maintain said insurance throughout the course of its contracts with the law enforcement agency.

9) **Availability, Reliability, and Performance – The cloud service provider must ensure that law enforcement data will be available to the law enforcement agency when it is required within agreed performance metrics.** The degree to which the cloud service provider is required to ensure availability and the performance of data and services, and the reliability of its operations will be dependent on the criticality of the service provided. For

some services (such as the retrieval of archived data or email), lower levels of availability and performance may be acceptable, but for more critical services, such as Computer-Aided Dispatch, reliability at a "5-nines" level (e.g. 99.999% available) may be required.

10) **Cost – Law enforcement agencies should focus cloud acquisition decisions on the Total Cost of Ownership model.** Cloud service purchases may use a different model for acquisition than the traditional server-based information technology solutions. Cloud services may have lower initial capital costs and permit budgetary certainty over a term of years by incorporating fixed annual operation and maintenance costs. By contrast, server system purchases typically involved larger initial capital costs and more variable annual operating and maintenance expenses. Lifetime costs of both systems will include perpetual compliance with FBI CJIS Security policies and requirements. The cost-benefit analysis of a cloud transition can only be calculated by looking at the lifetime value of the two comparable options under a Total Cost of Ownership model.

The IACP is in the process of developing model policies for cloud computing by law enforcement agencies, and these model policies are expected to be released at the International Association of Chiefs of Police Annual Conference in October 2013. In the interim, law enforcement agencies interested in implementing these principles into their current or contemplated cloud service engagements may wish to consider incorporating the following sample contractual language in their contracts or service level agreements.

Sample Contractual Language

Definitions

1) For purposes of this Agreement the phrase "Law Enforcement Data" means all text, numerical data, database records, media files, demographic information, search history, geo-location information, or any other data that law enforcement users or contractors provide to [CLOUD SERVICE PROVIDER], or to which [CLOUD SERVICE PROVIDER] otherwise gains access as a direct result of the cloud services provided to the law enforcement agency.

2) For purposes of this Agreement, the phrase "data mining or other processing" means the capturing, maintaining, scanning, indexing, sharing with third parties, or any other form of data analysis or processing of Law Enforcement Data provided to [CLOUD SERVICE PROVIDER] by [LAW ENFORCMENT CUSTOMER] pursuant to this Agreement. "Data mining or other processing" includes, but is not limited to, permitting access to Law Enforcement Data to which [CLOUD SERVICE PROVIDER] gains access as a direct result of related services provided by [CLOUD SERVICE PROVIDER] which are not otherwise services covered by the terms of this Agreement.

CJIS Compliance

3) This agreement incorporates by reference the requirements of the Criminal Justice Information Services (CJIS) Security Policy (current version 5.1, dated July 13, 2012) issued by the Federal Bureau of Investigation, Criminal Justice Information Services Division, as in force as of the date of this Agreement and as may, from time to time hereafter, be amended. [CLOUD SERVICE PROVIDER] warrants that it has the technological capability to handle Criminal Justice Information (CJI), as that term is defined by the FBI CJIS Security Policy, in the manner required by the CJIS Security Policy. [CLOUD SERVICE PROVIDER] expressly acknowledges that the CJIS Security Policy places restrictions and limitations on the access to, use of, and dissemination of CJI and hereby warrants that its system abides by those restrictions and limitations.

Data Ownership

4) [LAW ENFORCEMENT CUSTOMER] retains full ownership of all Law Enforcement Data provided to [CLOUD SERVICE PROVIDER] or to which [CLOUD SERVICE PROVIDER] otherwise gains access by operation of this Agreement. Upon expiration or termination of [LAW ENFORCEMENT CUSTOMER'S] use of the [CLOUD SERVICE], [LAW ENFORCEMENT CUSTOMER] may extract Law Enforcement Data (and if [LAW ENFORCEMENT CUSTOMER] cannot so extract, then [CLOUD SERVICE PROVIDER] shall extract on [LAW ENFORCEMENT CUSTOMER'S] behalf), and [CLOUD SERVICE PROVIDER] will delete Law Enforcement Data, in accordance with this agreement.

Data Mining

5) For the purposes of this Agreement the phrase "unauthorized use of Law Enforcement Data" means the data mining or other processing of Law Enforcement Data for unrelated

commercial purposes, advertising or advertising-related purposes, or for any other purpose not explicitly authorized by [LAW ENFORCEMENT CUSTOMER] in this Agreement.

6) [CLOUD SERVICE PROVIDER] will take all reasonably feasible, physical, technical, administrative, and procedural measures to ensure that no unauthorized use of Law Enforcement Data occurs. [CLOUD SERVICE PROVIER] warrants that all active and latent technical capabilities to conduct data mining or other processing that would constitute an unauthorized use of Law Enforcement Data have been either removed from its software package or disabled entirely.

7) Notwithstanding any provision of this Agreement, or any other agreement between the parties, or any published policy of [CLOUD SERVICE PROVIDER], the terms of this subsection take precedence over and replace any generally applicable privacy, data access or use, or similar policy of [CLOUD SERVICE PROVIDER], which the parties understand and hereby agree have no application to the processing of Law Enforcement Data.

8) [CLOUD SERVICE PROVIDER] agrees and understands that implementation of this subsection may require it to modify or disable certain aspects of the software solution it proposes to provide to [LAW ENFORCEMENT CUSTOMER]. [CLOUD SERVICE PROVIDER] warrants that it has the technical capacity to implement the technical changes required to conform to the requirements of this subsection. In particular, [CLOUD SERVICE PROVIDER] warrants that it can either disable completely or modify its software solution such that the applications services provided to [LAW ENFORCEMENT CUSTOMER] under this Agreement do not permit the unauthorized use of Law Enforcement Data by other applications services provided by [CLOUD SERVICE PROVIDER] which are interoperable with the applications services provided under this Agreement.

Audit

9) [CLOUD SERVICE PROVIDER] will, upon the request of [LAW ENFORCEMENT CUSTOMER], provide either: (a) a reasonable ability to inspect [CLOUD SERVICE PROVIDER]'s handling of [LAW ENFORCEMENT CUSTOMER]'s data; or (b) the report of an expert, independent, third party, verifying compliance with the provisions of this Agreement.

Portability and Interoperability

10) [CLOUD SERVICE PROVIDER] will maintain Law Enforcement Data provided to it by [LAW ENFORCMENT CUSTOMER] in a format that, to the maximum extent practicable, permits the export of Law Enforcement Data and the interoperable use of Law Enforcement Data by other cloud service providers, to an extent that does not compromise the security and integrity of the data. To the extent practicable cloud applications and Law Enforcement Data databases shall be maintained be in universally recognized formats.

Integrity

11) [CLOUD SERVICE PROVIDER] will maintain physical or logical separation between the cloud services provided to [LAW ENFORCEMENT CUSTOMER] and the consumer cloud

services, if any, that it provides to other customers. [CLOUD SERVICE PROVIDER] will further ensure that there is no commingling of Law Enforcement Data with data in [CLOUD SERVICE PROVIDER]'s consumer cloud services or with data resulting from any data processing activities conducted by [CLOUD SERVICE PROVIDER] as part of its consumer services. If the system is designed to house evidentiary material, then the [CLOUD SERVICE PROVIDER] shall maintain records of access to Law Enforcement Data sufficient to allow [LAW ENFORCEMENT CUSTOMER] to establish a chain of custody for data of evidentiary value.

General Provisions

12) The terms of this Agreement shall be binding on [CLOUD SERVICE PROVIDER] and its legal successors and assignees.

13) [CLOUD SERVICE PROVIDER] expressly agrees that its failure to fully comply with any provision of this Agreement will result in irreparable harm to [LAW ENFORCEMENT CUSTOMER] and that [CLOUD SERVICE PROVIDER] shall be solely liable for all reasonably foreseeable results of such failures, including, but not limited to, unauthorized access to, or misuse of, Law Enforcement Data, and that such failure shall be cause for immediate termination of this Agreement, return of all Law Enforcement Data to [LAW ENFORCMENT CUSTOMER], and [LAW ENFORCEMENT CUSTOMER]'s immediate exercise of any lawful remedies.