**CALIFORNIA DEPARTMENT OF TECHNOLOGY**

September 9, 2015

Honorable Rudy Salas Jr.
Chair, Committee on Accountability
and Administrative Review
1020 N Street, Room 357
Sacramento, CA 95814

Re: Response to CalCloud Computing and Information Technology Procurement Hearing

Dear Assemblymember Salas:

Following the March 11, 2015 hearing in the Assembly Committee on Accountability and Administrative Review, you requested that the California Department of Technology (CDT) provide an update by September 15, 2015 regarding the implementation of CalCloud. Accordingly, we are pleased to provide the following information in response to your request.

1. An update on the State Entities' CalCloud and commercial cloud participation, with a listing of how state entities are using CalCloud and commercial cloud solutions. Please describe new CalCloud products and services along with information about vendor participants.

   CalCloud has a suite of service offerings including Infrastructure as a Service (IaaS), Vendor Hosted Subscription Services (VHSS), and supporting services. These service offerings are offered to customer agencies through the Office of Technology Services' catalogue of technology services. CalCloud is available to government agencies, local government and public education entities within the State of California.

   CalCloud is a technology services model that features a reliable and secure set of pooled/shared computing resources and a cost model wherein customers pay only for services consumed. CalCloud provides customers a self-service portal for on-demand access to a shared pool of computing resources, allowing customers to rapidly setup and decommission computing infrastructure on an as-needed basis. The value of a shared pool of resources like computing capacity, data storage, network connectivity and disaster recovery services is that it results in cost, energy and operational efficiencies for government agencies.

**Description of Cloud Services**

One of the featured CalCloud services is IaaS. IaaS provides computing infrastructure (servers, storage and connectivity) as a service rather than as a capital investment. IaaS is an on premise cloud environment that ensures that the computing environment is shared only between government entities (no intermingling with commercial organizations or with private individuals or other customers of commercial cloud vendors). Unlike commercial cloud providers, our IaaS service ensures that all data collected or transacted by those government agency customers is stored and housed on premise in a secure state government facility. The Department Technology worked with the following companies (through a competitive bid) to stand up our secure government IaaS service offering: IBM, AT&T, Cisco, Citrix, Fortnet, Intel, McAfee, Microsoft, NetApp, Red Hat, and VMWare.

Currently, twenty-three state and local government agencies are customers of CalCloud IaaS environment. Another thirteen departments have plans to migrate to CalCloud IaaS in the coming few months. Customers utilize CalCloud IaaS for production, test and development environments. Below are examples of customer agencies using CalCloud IaaS:

| Agency | System |
|---|---|
| State Controller's Office | Mainframe Reporting Application |
| Department of Health Care Service's | CalLISA |
| Department of Food and Agriculture | Pierces Disease website |
| Department of Motor Vehicles | LoadRunner Performance Tool |
| Governor's Office of Business & Economic Dev | CA Business Portal |
| Emergency Medical Services Authority | EMT Certification application |

CalCloud also includes VHSS. These are a portfolio of software and platform services hosted and managed by cloud providers. A VHSS service is a commercial off-the-shelf software or platform product provided through a CDT-managed contract agreement with approved vendors. VHSS allows state entities to quickly leverage commonly used products in a secure manner. It also leverages the state's buying power and ensures that contracts with such providers incorporate the state's model terms and conditions for cloud services.

Customers can subscribe to these services through CDT for service categories such as project and portfolio management, customer relationship management and case management. The current VHSS portfolio consists of BMC's Remedy on Demand, Computer Associates' Clarity on Demand, and the SalesForce.com suite of products. There are fifteen departments leveraging these VHSS products and four additional departments planning to subscribe. Additional services will be added to the VHSS portfolio based on customer demand. CDT is planning a series of informational sessions for vendors interested in providing VHSS services through CalCloud. The first session will take place on September 21, 2015.

2. Information about how risk and liability are identified and addressed in vendor contracts related to cloud technologies.

The Department of Technology's contracts for clouds services contain specific requirements related to information security and service level agreements for performance. The Cloud Computing Services Special Provisions for Software as a Service and GSPD-401IT address specific requirements as follows:

CalCloud IaaS must meet the security requirements per the State Administrative Manual (SAM) Sections 5300, including the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations and the Federal Risk and Authorization Management Program (FedRAMP) version 2 controls.

CalCloud IaaS was designed to be compliant with the required FedRAMP cloud service providers controls. CDT also contracted with a third party vendor, to perform vulnerability scans and continuous security monitoring of the CalCloud IaaS. CDT, in collaboration with IBM and AT&T, has developed a System Security Plan (SSP) in accordance with NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Information Technology Systems. Completion of this SSP, which describes how U.S. Federal information will be safeguarded, is a requirement of the FedRAMP program [Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, and Public Law 100-235, and the Computer Security Act of 1987] as well as by SAM 5305.1.

This SSP provides a detailed listing of the security controls per the FedRAMP guidelines for CalCloud and describes the controls in place in implementation to comply with the security requirements. Information security is an asset vital to our critical infrastructure, and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by CalCloud.

Additionally, the Federal Information Security Management Act (FISMA), FedRAMP, as well as SAM 5305, requires that a Plan of Action and Milestones (POAM), using the format guidance prescribed by OMB, be utilized as the primary mechanism for tracking all system security weaknesses and issues to resolution. The authorizing official (accreditor) must take ownership of these risks and ensure they are included in the weakness repository, and that the POAM for the system is updated, monitored, and progress reported quarterly through the FISMA coordinator.

From the POAM and other information, a Security Assessment Report (SAR) has been developed as also required by the FedRAMP standards. The SAR provides the Designated Approving Authority with a holistic view of risk regarding the system, and documents the security assessment activities that were performed on the system. This report provides the system's stakeholders with a summary of the management, operational, and technical controls used to protect the confidentiality, integrity, and availability of the system and the data it stores, transmits or processes.

3. The extent to which state entities are following the "Cloud First Policy". Also, please describe the exemption process and type of exemptions that have been sought and their outcomes.

Departments seeking to acquire or implement new technology systems are required to comply with Government Code (GC) 11545-11546 and Section 4983 of the SAM, which details the state's Cloud First Policy. The Cloud First Policy is incorporated into CDT's project approval process. As part of project approval, the Department of Technology works with the departments to evaluate and determine the appropriate technical solution to meet their business and operational needs. Through this assessment, the departments and CDT jointly assess the feasibility of leveraging cloud computing services. Department's seeking to use non cloud technologies or services to address business needs would address their proposed technology approach through this joint assessment.

To date, no agencies have sought exemption from complying with GC 11545-11546 or SAM 4983 Cloud First Policy.

If we can be of any further assistance to you, please don't hesitate to give me a call.

Sincerely,

CARLOS RAMOS
Director