LOS ANGELES POLICE DEPARTMENT

Date: July 8, 2010

To: Chair, Information Technology and Government Affairs Committee

From: LAPD, Commanding Officer, Information Technology Bureau

Subject: **SUPPLEMENTAL REPORT TO THE CITY ADMINISTRATIVE OFFICER SECOND STATUS REPORT ON THE IMPLEMENTATION OF THE GOOGLE E-MAIL AND COLLABORATION SYSTEM (C.F. 09-1714)**

BACKGROUND

The City of Los Angeles, Information Technology Agency has contracted with Google to implement its Google Apps offering that Google has created to serve organizations who wish to outsource the management of various information technology (IT) services such as email, electronic calendaring and document preparation. While such outsourcing may represent savings in hardware purchases and maintenance, and software administration, it also poses certain security concerns, as the customer's data is stored and administered by the vendor (Google), rather than the customer (the City or the LAPD).

To cater to the heightened needs of a government customer, including law enforcement, Google proposed the creation of a new service to be tailored to the needs of government, called Google Apps For Government (GAFG) or the "Gov Cloud." GAFG was to be different from Google Apps offerings provided to other Google customers, in that it was conceived to meet the elevated security requirements for storing law enforcement-related data, primarily defined by the California Department of Justice (Cal-DOJ).

In order to access information within a variety of justice systems, Cal-DOJ imposes certain requirements and policies on how a subscriber agency, such as the LAPD, stores and administers its law enforcement-related data. Cal-DOJ requirements are pertinent to email services used by law enforcement-related agencies as those email services are capable of transmitting justice information from state and federal systems such as Criminal Justice Information System (CJIS), NLETS/CLETS (National Law Enforcement Telecommunication System/California Law Enforcement Telecommunication System), and the Criminal Offender Records Information (CORI) system. Each of these systems imposes its own security requirements upon any law enforcement entity accessing such information. For the City, these include the LAPD, Office of the City Attorney, Office of Public Safety of the Department of General Services, and the Department of Recreation and Parks (Park Rangers).

To ensure that its subscriber agencies are adhering to the security policy of these state and federal systems, periodic audits are performed by Cal-DOJ, as well as the FBI, to ensure that appropriate security controls are in place within each agency. If agencies are found to be out of compliance, access to these justice systems can be terminated until the agency meets Cal-DOJ's or the FBI's security requirements.

Through a review of relevant policy, and several discussions with Cal-DOJ, the security requirements were defined as follows:

- Data encryption;
- Segregation of City data from other data maintained by Google;
- Data storage only within the continental United States;
- Background checks for all Google employees with access to LAPD data; and
- Direct access to Google's data centers by auditors from the City, DOJ or FBI.

On June 21, 2010, Google made version 1.5 of GAFG available. Version 1.5 includes the following features:

(1) GAFG servers store the City's Gmail and Google Calendar data. (Note: Data for other Google Apps the City uses (e.g., Google Docs, Google Sites and Google Video) are not stored on GAFG servers, nor restricted to the continental US, and, as such, the LAPD has elected to turn off this functionality).
(2) Within Google datacenters, GAFG servers are physically segregated and locked in separate cages from that of other Google Apps customers.
(3) Data stored at rest on GAFG servers is encrypted, using cryptographic standards accepted by the US Government (through the National Institute of Standards and Technology). Encryption keys to decrypt the data are created and managed by Google.
(4) Google datacenters storing City data, or the cages within them where GAFG servers will be stored, may be inspected by the City, DOJ or FBI auditors.
(5) Two designated Google employees, with the skill, access and authority to put LAPD data back together, should the need arise, have passed the LAPD background check.

OUTSTANDING SECURITY ISSUES

1. eDiscovery

The Google eDiscovery application, which will allow City departments to easily respond to discovery requests, search email in response to administrative investigations, etc. and will contain several years of LAPD data, will not be contained within the GAFG offering. Instead, this data will reside on servers Google purchased as part of its purchase of a third party company, Postini, which are not physically segregated from other Google customers, and will not be subject to GAFG security measures. This is of significant concern to the LAPD, as the eDiscovery application was viewed as a primary benefit of moving to Google for email services.

Google has indicated that it will work with the LAPD to determine its requirements for responding to discovery requests and administrative investigations, and will look to develop an

alternative solution. On July 6, 2010, Google/CSC met with the LAPD to begin this effort. As soon as Google proposes a solution, the LAPD will evaluate the proposal to ensure it meets investigative requirements. The LAPD cannot go live with Google until an appropriate solution is in place.

2. Audit Tool

While two Google employees, with the skill, access and authority to put LAPD data back together, should the need arise, have completed an LAPD background check, there is no physical security on the GAFG servers to prevent any other Google employee on the server administration team from performing such a task. This limitation is imposed via Google written policy, only.

As a result, Cal-DOJ asked that LAPD system administrators have the ability to audit the system to determine: (1) who from Google has accessed LAPD data; (2) what data the employee accessed; and (3) why the employee accessed the data. Per Google representatives, this function is not available to the LAPD today, and Google will need to build an audit utility to allow LAPD to perform this auditing function. Google has given an estimated completion date of December 31, 2011for the audit utility.

As an interim measure, Google has proposed that it produce quarterly audit logs to show the LAPD which Google employees have accessed LAPD data. This proposal was presented to Cal-DOJ representatives on July 1, 2010. Cal-DOJ indicated that this solution could suffice in the interim, given that the LAPD and Google can show a plan for improvement of this process, via the development of the audit utility. However, Cal-DOJ cannot formally certify such a solution or guarantee a compliance finding should the DOJ or FBI conduct an audit. Cal-DOJ suggested that Google provide a detailed walk-through of how this interim solution will work, to include how the LAPD can be assured that the audit logs produced by Google are pristine, and have not been altered by Google employees. Google is in the process of documenting this information. Upon receipt, the LAPD will share the information with Cal-DOJ for its assessment, before going live on Google.

OUTSTANDING PERFORMANCE ISSUES

1. Delayed Delivery of Email

There are currently 50 LAPD employees piloting the Gmail solution. These users have consistently experienced delays in receiving email, up to several hours. Given that the LAPD is a 24/7 operation, which relies upon email/blackberry notifications for public safety related incidents across the City, these delays are not acceptable. While it was originally thought that such delays were a result of the LAPD being on two email solutions concurrently (Groupwise and Gmail), this theory might not explain why even Gmail to Gmail communications are delayed. Google and CSC have committed to finding a resolution to this issue, and troubleshooting efforts are ongoing.

2. Email Status Not Available

The LAPD has a need to know when a particular email has been delivered, opened/read, and deleted. This requirement is directly related to the "eDiscovery" item discussed above in that, often, LAPD administrative investigations require information pertaining to when an email was delivered, opened, and/or deleted. Although the City has set this functionality as a "high priority" for development, Google has indicated that it cannot deliver this functionality, due to limitations set by Google's current architecture. ITA has indicated that it will look for an alternate solution to satisfy this requirement. Also, as discussed above, Google is looking to resolve this issue for the LAPD via an alternate solution to eDiscovery.

3. BCC Indication Not Available

Gmail does not currently distinguish between a "CC" or BCC" recipient. As a result, an email recipient cannot be confident as to whether they were copied, or blind copied on an email. Although the City has set this functionality as a "high priority" for development, Google has indicated that it cannot deliver this functionality, due to limitations set by Google's current architecture. Google has suggested a "workaround" approach that can be set by each individual user; however, it cannot be set globally for all users. The LAPD remains concerned that this workaround will have to be set for each of its 13,000 employees individually. Google/CSC have committed to reviewing an alternative approach that might allow this workaround to be set globally for all users.

CONCLUSION

As the LAPD was unable to migrate to Google by June 30, 2010, for the reasons discussed above, it must maintain its current email solution into FY 2010/2011. Novell has agreed to allow the City to renew its Groupwise licensing on a quarterly basis at a minimum, at approximately $60,000 per quarter for all LAPD employees. As the funding typically allocated for Groupwise funding was not allocated to the LAPD for FY 2010/2011, and was instead allocated to ITA for Gmail funding, LAPD expects that ITA will process the licensing purchase for the quarter July 1 – September 30, 2010, and any subsequent quarters, until the outstanding Google issues are resolved and the LAPD can migrate to GAFG.

At this time, a definitive timeline for LAPD migration cannot be provided. The LAPD expects that it can proceed with its migration to GAFG when all workarounds/interim/alternative approaches discussed above are delivered by Google, tested by the LAPD, and are proven to comply with LAPD operational requirements.