OIR Group Report on Email Audits: Burbank Police Department

December 2016

Prepared by: Michael Gennaco
Stephen Connolly

323-821-0586
www.oirgroup.com
7142 Trask Avenue | Playa del Rey, CA 90293

OIR Group Report on BPD Email Audits

I. Introduction

Pursuant to our ongoing relationship with the City of Burbank as auditors of the Police Department, we became involved earlier this year with the City's response to the BPD email controversy. Our annual Audit Report to the City for 2016 includes our evaluation of that matter.

Along with an assessment of the relevant history and resolution of the 2014 case involving a former BPD executive, the Report offers several recommendations relating to email audits on a "going-forward" basis. The recommendations were first shared with BPD executives in July, and the Department has already accepted and implemented them. One of them reads as follows:

- *OIR Group recommends that all BPD command staff (Captains and above) be subjected to an annual email audit to be conducted by an auditing group outside BPD's chain of command.*

The City Manager requested that we perform such an audit as part of our oversight of the Department. Accordingly, the City and BPD moved ahead with enlisting OIR Group's involvement in two ways:

- monitoring the Department's own internal audit of different rank classifications and non-sworn employees; and
- conducting an independent direct audit of Command Staff emails.

II. Methodology

Our monitoring function of the Department's own auditing efforts followed the same protocol that we employ for the other subject matter of our reports. We received a copy of the completed audit package, assessed it for the thoroughness and legitimacy of the Department's process and conclusions, and spoke with BPD executives about our findings and recommendations. Those are summarized below.

For our own audit of the executive email accounts, the City provided OIR Group with Command Staff downloaded emails for a random one month period, segregated by individual and by the categories of "Sent" and "Received." Our understanding is that these came directly from the

City's server and reflected all material that passed through the accounts – even if they had been deleted. The accounts were for the Chief, Deputy Chief, three Captains, and the highest-ranking civilian administrator. Combined, there were approximately 2,100 "Sent" emails and approximately 10,000 "Received" emails in these accounts.

To review them, we focused on the "Subject" line of each email and were able to eliminate the vast majority of them from further scrutiny in relatively efficient fashion. This was particularly true for the "Received" category. These were more voluminous, but also more repetitious, since multiple command staff members frequently received the same correspondence. More importantly, these were less significant from the perspective of potential wrongful behavior, to the extent that people have limited control over what others send.

Accordingly, we devoted the majority of our time to scrutinizing the "Sent" emails. We gave careful assessment to approximately 80 percent of these emails, and the remainder were either automatically generated (such as "Read" notifications or calendar acceptances) or part of a chain of correspondence; the latter were subsequently repeated and therefore otherwise viewable.

We also opened and reviewed approximately 15% of the "Received" emails. We looked at multiple random samples from each account, and looked for "Subject" lines that did not clearly describe the contents or obviously connect them to a business purpose. Of course, many of the same emails appeared multiple times across the accounts: an update sent by a captain to the rest of the command staff, for example, not only would have been part of his own "Sent" file, but also would be represented 5 different times among the 10,000 "Received" emails for the audit period.

In short, while we cannot attest to the definitive contents of every single email, or speak to activity that occurred outside the auditing period, our methods were more than consistent with basic auditing practices that rely on representative samples.

III. Results

Overwhelmingly, the emails reflected an appropriate level of professionalism and adherence to City and BPD policy. The relevant language from BPD's email policy reads as follows:

"Sending derogatory, defamatory, obscene, distasteful, vulgar, sexually suggestive or harassing or any other inappropriate messages on the email system is prohibited and may result in discipline. The email system is provided for official police business purposes only."

There were very limited exceptions. For the most part, these involved emails that were benign in their subject matter but seemingly not directly related to the sender's professional responsibilities. Examples include the following:

- 3 "forwards" of internet articles unrelated to work (by different senders)
- A brief reply to a received email relating to a classic car that was for sale
- An email to a family member regarding an interview request from an out-of-state media representative (topic unknown)
- Sightseeing photos from a vacation

To the extent these deviated from policy at all, they were extremely minimal in both number and severity. It should also be noted, for example, that the same executive who emailed two vacation pictures with his iPhone was responding consistently and thoughtfully to a variety of Department emails throughout his time "off." We also recognize that hyper-enforcement brings issues of its own, from the chilling of productive exchanges to an ironic incentive toward inefficiency.[1]

It is only because these emails were not apparently "work-related" that they deviated from the letter of BPD's policy. However, these technical violations do not warrant further formal action, both because of their very limited number (no individual person had more than two or three during the month period) and their innocuous content. In fact, as discussed below, an amendment of policy that preserves relevant Department interests while conforming to the realities of employee practice, may well be worth considering.

One other exchange of note related to a picture of a remote controlled robot with an explosive device that was captioned "Employee of the Month" for the Dallas Police Department. This was an apparent reference to the recent incident in which five Dallas officers were fatally shot before the suspect himself was killed by an explosive device tethered to a robot. The original email was sent without comment to a command staff member by a non BPD employee. The command staff member then responded in an innocuous but lighthearted fashion.

In its worst light, this could arguably be interpreted as the trivialization of a serious incident, and therefore "inappropriate" within the meaning of the policy. Others, though, could reasonably see it quite differently, and it clearly does not implicate any of the obvious problem areas of racial, ethnic, religious, sexual or gender-based content. Unless a message is clearly and definitively out of bounds, one must be careful about formally sanctioning discourse. Accordingly, no formal action seems warranted. At the same time, it seems more prudent to

[1] For example, if someone receives a "non-business" email in his or her City account, and then feels compelled to go to a personal email in order to reply, that ends up taking longer and being more of a distraction from work than simply allowing a quick response in the first place.

steer clear of debatable content in the first place when possible. The better course might have been for the BPD command staff member simply not to respond to the content of the initial email, as this individual has subsequently acknowledged.

IV. Review of BPD 2016 Internal Email Audits

We were provided with the results of the two audits (one for sergeants and lieutenants, and another for all other personnel, both sworn and civilian) that were conducted internally per past Department practice. In both audits, a percentage of total employees was randomly selected; per an OIR recommendation, employees whose accounts had previously generated issues were also included. Across the two audits, the accounts of 39 Department members were reviewed. The sample size and other methodology were reasonable and appropriate to the task: a thorough but efficient general survey of compliance with email policy and preferred practice.

As with the command staff in our own project, these audits found overwhelmingly that the emails were in compliance with policy. Several employees had no issues, while several others had only *received* emails that fell outside of policy because they were non-work related. Many of these were advertisements and/or spam. There were also multiple instances of personal or "non-work" emails being sent; again, however, the content of these was benign, the numbers were small, and the violations of policy were technical only. Finally, a few employees appeared to have linked their personal email accounts to the BPD system, resulting in additional traffic and potential vulnerabilities to the system.

A couple of the "received" emails seemed to warrant further scrutiny in terms of the appropriateness of the content. At our request, we received further information from BPD about these emails and learned that the emails were not forwarded or responded to, and were not indicative of a pattern of receiving such emails. In a couple of other instances, work emails were written with language that fell short of professionalism.

We consulted with the Department about our impressions, and agree with BPD's proposed action items. These include:

- A bulletin for all employees that describes the audit, explains the findings, and features appropriate reminders about policy and practice.
- Instructions to employees to "unlink" their personal email accounts to the BPD server.
- Verbal counseling to employees whose emails raised issues indicating lack of professionalism.

V. Recommendations

As detailed above, while the vast majority of emails reviewed by us of Command Staff were work related and clearly within current BPD policy, a minute few were innocuous but apparently non-work related and potentially in violation of the extremely rigid current policy. As further noted above, our results largely conform to what BPD found in its most recent audit of its employees (and previous audits). The vast majority of identified issues stem not from the content or volume of personal emails, but from the exacting standards of current policy language. The blanket prohibition of *any* personal use of the email server may create "infractions" of a sort that are not worthwhile preoccupations for the Department – and can lesson an agency's appetite for voluntary self-auditing.

Said another way, the Department (and the City) have a special interest in ensuring that its employees do not send derogatory, demeaning, racist, or otherwise inappropriate emails over its servers. Moreover, BPD has an interest in ensuring that employees are not consuming significant chunks of work time sending and receiving personal emails on their email accounts. However, in our view, it also makes sense to refine BPD and City policy and recognize an exception for limited and content-appropriate personal correspondence. Such an approach comports more closely to modern work realities, and continued audits will help ensure that abuses do not occur.

Recommendation: BPD and the City should consider modifying its current email use policy to allow for "de minimis" use of the servers for innocuous personal exchanges.