



Recommendation 24.6

Tanya Koshy [Redacted]

Wed 9/9/2020 12:05 PM

[Redacted]

This message is from outside the City email system. Do not open links or attachments from untrusted sources.

Dear Acting Captain Altorfer,

Our office has completed its review of the materials related to Recommendation 24.6 that have been submitted to us as part of the collaborative reform process. After reviewing the package and information provided by SFPD, the California Department of Justice finds as follows:

Recommendation 24.6:

The SFPD should report twice a year to the Police Commission on the outcome of its audits of official electronic communications, including the number completed, the number and types of devices audited, the findings of the audit, and the personnel outcomes where biased language or other conduct violations are discovered.

Response to 24.6:

SFPD has exceeded the biannual report provided in the recommendation and instead requires quarterly reports to the Police Commission on its audits of official electronic communications. This requirement is codified in Internal Affairs Division Unit Order 18-02. Under Unit Order 18-02, IAD members prepare quarterly reports to the Commanding Officer of Risk Management, which includes the number and types of devices audited, total number of "hits" (i.e. number of times biased language used) found in the audit, the number of false positives or non-member generated "hits," any reportable findings, and the disciplinary outcomes for any investigations arising out of the audited information. The quarterly report is forwarded and reviewed up the chain of command. The Commander of Risk Management then presents the quarterly report to the Police Commission.

SFPD specifically audits its members' emails and cell phone text messages. The DOJ inquired about whether SFPD could audit individual terminal computer hard drives used by officers and staff. SFPD researched whether it had the capacity to do a random sampling of hard drives and determined that while it did have the capacity, it would be too expensive to implement. Specifically, SFPD's Acting Director of Technology estimated that the cost of the software needed to review the hard drives would amount to \$140,000 a year. SFPD determined that, in light of mandatory budget cuts, SFPD would not be able to audit computer hard drives at this time.

SFPD has expanded the list of words it searches for in its audits. The California Department of Justice has reviewed this list and determined that it included contemporary bias-based words.

Since SFPD has implemented this audit process, its audits have uncovered two incidents of members using words on the bias-based word list. SFPD has filed disciplinary charges against the three members involved and the Police Commission has issued penalties to them.

Based on the all of the above, the California Department of Justice finds SFPD in substantial compliance with this recommendation.

Please let us know if you have any questions or would like to discuss these further. Thank you.

Tanya

Tanya S. Koshy (she/her)
Deputy Attorney General
Civil Rights Enforcement Section





California Department of Justice
1515 Clay Street, Suite 2100
Oakland, CA 94612



CONFIDENTIALITY NOTICE: This communication with its contents may contain confidential and/or legally privileged information. It is solely for the use of the intended recipient(s). Unauthorized interception, review, use or disclosure is prohibited and may violate applicable laws including the Electronic Communications Privacy Act. If you are not the intended recipient, please contact the sender and destroy all copies of the communication.





Collaborative Reform Completion Memorandum

Finding # 24: The SFPD did not conduct a comprehensive audit of official electronic communications, including department-issued emails, communications on mobile data terminals, and text messages on department-issued phones following the texting incidents.

Recommendation # 24.6 The SFPD should report twice a year to the Police Commission on the outcome of these audits, including the number completed, the number and types of devices audited, findings of the audit, and the personnel outcomes where biased language or other conduct violations are discovered.

Response Date: 08/05/2020

Executive Summary:

Unit Order 18-02 "Internal Affairs Audit Procedure," was created to establish the protocol and procedure for the auditing of Department electronic devices for possible bias by members of the department.

The procedure for reporting the findings of the audit is described in the "Reporting" section of the Unit Order. Internal Affairs Division (IAD) investigators are assigned to conduct the audits of department electronic devices. The Unit Order mandates that the Commanding Officer of Risk Management reports the findings of the audits to the Police Commission on a quarterly basis.

The report shall contain the following information (based on the amount of time between reports):

- The total number of "hits" per type of audit
- The number of false positive or non-member generated "hits"
- Any reportable findings obtained from the audit
- The disciplinary outcomes for any investigations initiated by audited information

The Unit Order also established that electronic and hard copies of the bias reports are maintained by the Officer in Charge (OIC) of IAD.

In addition to the audit reports being maintained by the OIC of IAD, records of disciplinary hearings resulting from use of prohibited bias-words on Department electronic devices and technology are available on the Police Commission website so the public can see that the use of bias-words is being addressed by the Department.

To date, two incidents of bias-word use have been discovered via the audits and all of the members involved have been disciplined.

At the request of the CAL DOJ, the bias-word list has been expanded to include contemporary words reporting bias.



Collaborative Reform Completion Memorandum

It has been determined that expanding the audits to include random audits of Department hard-drives is cost-prohibitive at this time due to mandatory budget cuts.

Compliance Measures:

1) Policy to report bias outcomes twice yearly to Police Commission.

On 07/22/2019 Hillard Heintz (HH) noted that this compliance measure had been met.

Unit Order 18-02 established that the outcome of the bias audits be reported to the Police Commission four times yearly. (see **Attachment 1: Unit order 18-02 Internal Affairs Audit Procedure**)

2) Audit report to include:

- **Number of audits**
- **Number and types of devices audited**
- **Findings of audit**
- **Personnel outcomes if/when violations are discovered**

On 07/22/2019 Hillard Heintz (HH) noted that this compliance measure required additional information. On May 19, 2020, SFPD members

held a telephone conference with

CAL DOJ

During that conference, SFPD members asked for further clarification on compliance measure 2 and the three items listed in the "Requested Documents" section that were needed to reach substantial compliance.

A) Evidence that audits of other department electronics and technology is included in the bias report to the Police Commission.

SFPD asked specifically what types of electronic equipment/technology was contemplated when making this request, since the Department audits text messages to and from Department cell phones, emails to and from Department computers, and all inquiries made in the Level II (CLETS) program. In addition, the Department and the City and County of San Francisco have several Firewalls that filter and block members from accessing and downloading prohibited sites and content.

recommended that the Department conduct random audits on Department computer hard drives to search for bias word usage. Commander said the Department would look into whether auditing computer hard drives was possible, and if it proved to be so, she would provide the information to Chief Scott for a decision.



Collaborative Reform Completion Memorandum

-
-
- The Department protects its computers from members downloading prohibited material by using Palo Alto Networks next generation boundary protection devices that prevent prohibited downloads as well as Fire Eye HX endpoint client software on all computers.
- Members are prevented from accessing prohibited websites because all traffic to and from the Internet passes through SFPD Firewalls that filter/block prohibited sites and content. As a second layer of protection, that traffic also passes through the City's Department of Technology (DT) Firewalls, which also filter/block prohibited sites and content.

B) Evidence that the bias word list has been expanded to include contemporary words reflecting bias, including words directed at Muslims, religions, LGBTQ, and other societal classes.



Collaborative Reform Completion Memorandum

Members of SFPD asked for clarification surrounding this request as SFPD understood that members of the CAL DOJ team had seen the bias word list and were satisfied with the list. _____ confirmed that members of the CAL DOJ team had seen the bias word list and were satisfied with the list.

C) Evidence of remedial action resulting from the Technology Division discovery of bias-word usage.

Members of the SFPD asked for clarification regarding the seemingly conflicting comments in the RFI of: "There is no evidence of the bias word audit having discovered any incidents of usage by members," and "it had been reported to the HH Team that use of bias words has been discovered on other department communications." Members of SFPD explained that to date, there have been two incidents involving three members where bias words from the list were used, and both incidents were discovered using the current protocol for auditing the Department's communication systems. These incidents have been reported to the Commission and the remedial action for each case is posted on the Commission's website.

To date, the audit has discovered two incidents involving three members where words included on the bias word list have been used. The SFPD filed disciplinary charges against each member, and the outcome of each case is available on the Police Commission website in an anonymized format for the public to view.

The two incidents include:

- 1) IAD-2017-0283/MCD-2017-0283 (involved two members):
 - One member was charged with using Racial Epithets was disciplined with a 30-day suspension with mandatory re-training. (see Attachment #7: 4th quarter 2018 report of Discipline posted on Police Commission webpage).
 - One member was charged with Neglect of Duty and was disciplined with an admonishment and retraining (see Attachment #8: February 2018 IAD Sustained Complaints report on the Police Commission webpage)
- 2) MCD-2019-0122:
 - The member was charged with Neglect of Duty and Conduct Unbecoming a Member and was disciplined with a written warning and retraining (see Attachment #9: October 2019 IAD



Collaborative Reform Completion Memorandum

Sustained Complaints report posted on the Police Commission webpage).

3) Evidence of ongoing review and audit

On 07/22/2019 Hillard Heintz (HH) noted that this compliance measure had been met.

The first way the Department provides evidence that its review and audit of Department electronic devices for possible bias is ongoing is by reporting its findings to the Police Commission quarterly in public session.

The second way the Department provides evidence that the audit is ongoing is by being transparent with the results to the public. By reporting the findings to the Police Commission in public session, the reports are public record. Copies of the findings report can be found on the Police Commission's website sfgov.org/policecommission/. This level of transparency allows the public to monitor the process and to ensure the audits are continuous and ongoing as required. (see Attachment #10: sfgov.org/policecommission/)

A third way the Department provides evidence is by preserving the records of the findings with the Officer in Charge of IAD. The Unit Order established the procedure for maintaining the audit data:

The underlying audit data will be maintained electronically and all reports shall have a hard copy safeguarded in the OIC of the Internal Affairs Administrative Division office. All audited data not determined to be in violation of Department policy will be held for safekeeping by the IA investigators in charge of auditing unless directed by the Commanding Officer of Risk Management to discard it.

4) Evidence of supportive and remedial action if deficiencies are found.

On 07/22/2019 Hillard Heintz (HH) noted that this compliance measure had been met.

To locate possible deficiencies in the audit, the bias word list is reviewed and updated by IAD continually.

The bias word list shall be reviewed quarterly along with the bias audits. Bias terms shall be uniform across all audit platforms. Terms deemed problematic, impractical, or subject to overwhelming false positives to auditing can be removed with approval of the OIC of IAD and the Commanding Officer of Risk Management. If IAD investigators find that new bias words are being utilized by members or the populace at large, the IAD investigators shall add them to the bias list by notifying the Technology Division Director, CLETS Administrator, and the Commanding Officer of Risk Management.

The remedial action of updating the audit's data base is evidence that the Department reevaluates the audit process and takes action for improvement (see Attachment #11: Memorandum requests to update Bias audit list).



Collaborative Reform Completion Memorandum

To date, there have been two incidents involving three members discovered by the audit. Per Unit Order 18-02, when those three members were found to be communicating outside the guidelines set by the Department, IAD initiated an investigation into those members regarding the improper use of Department equipment. The incidents were reported to the Police Commission and the remedial action for each case is posted on the Commission's website.

DGO 2.04 – Complaints Against Officers was updated, effective 05/15/2019, and lists procedure and Department policy in regard to complaints of possible misconduct of officers. (see **Attachment #12: DGO 2.04 – Complaints Against Officers**)

Attachments:

- Attachment #1: Unit Order 18-02 (1)
- Attachment #2: calendar invite from Ms. Beninati to members of the SFPD
- Attachment #3: emails between Sgt. Chandra Medina and director Sanson-Mosier
- Attachment #4: emails between Mr. Price and Ms. Kilshaw
- Attachment #5: salary range for classification 1043-Is Engineer, Senior
- Attachment #6: notes from Chief Scott to Commander Ewins
- Attachment #7: 4th Quarter 2018 Report of Discipline listing case #IAD-2017-0283 posted on Police Commission website
- Attachment #8: February 2018 IAD Sustained Complaints report listing case MCD-2017-0283 posted on Police Commission website
- Attachment #9: October 2019 IAD Sustained Complaints report listing case MCD - 2019-0122
- Attachment #10: screenshots of sfgov.org/policecommison/ web page
- Attachment #11: Memorandum requests to update Bias audit list (3)
- Attachment #12: DGO 2.04 – Complaints against Officers (1)