## Recommendation 24.5

Gabriel Martinez [redacted]
Tue 8/18/2020 10:46 PM
**To:** McGuire, Catherine (POL) [redacted] Scott, William (POL) [redacted] Altorfer, Eric (POL) [redacted]



Dear Lt. Altorfer,

Our office has completed its review of the materials related to Recommendation 24.5 that have been submitted to us as part of the collaborative reform process. This package focused on SFPD establishing policies and practices for signing off on SFPD's electronic communications policy and ensuring officers receive a notification of the policy when using department systems. After reviewing the package and information provided by the Department, the California Department of Justice finds as follows:

Recommendation 24.5: The SFPD should require all members to acknowledge appropriate use standards for electronic communications. This should be a signed acknowledgement, retained in the personnel file of the member, and department personnel should receive an alert reminding them of appropriate use whenever they sign onto SFPD systems.

Response to 24.5: On March 21, 2019, SFPD published Department Bulletin 19-051, SFPD Members' Expectation of Privacy - Use of Computers, Peripheral Equipment and Facilities. The Bulletin defines inappropriate uses of electronic devices, emphasizes that officers have no expectation of privacy on department devices, and notifies officers that all communications may be audited. The Bulletin updated Department General Order 10.08, Use of Computers and Peripheral Equipment, which also notifies officers that they do not have any expectation of privacy on department-issued devices.

On April 28, 2020, SFPD ran an audit of officers that had signed off on reviewing Bulletin 19-051 using the Human Resources Management System (HRMS). HRMS sign-offs are retained in each officer's personnel file. The audit showed that 98.19% of officers had signed off on the bulletin (officers on leave and certain extenuating circumstances prevented 100% compliance). If an officer has not signed off, they are subject to progressive discipline beginning with a notification to the officer's supervisor that they are out of compliance. For continued non-compliance, officers may be subject to discipline for failure to follow Department General Order 2.01, General Rules of Conduct, which includes obeying all written directives.

Additionally, SFPD implemented a program of pop-up acknowledgements before an officer can log in to a department device. The acknowledgement outlines prohibited uses of devices, notifies the user that there is no expectation of privacy on the device, and states that communications may be monitored without notice. On January 18, 2017, SFPD published Department Bulletin 17-011, Pop-up Network Acceptable Use Statement on Workstations, with the acknowledgement. On September 3, 2019, SFPD published its report on audits to ensure that the pop-up notifications appear on all department devices. After initially finding that 234 smartphones had applications that prevented the pop-up notifications from appearing, during the course of the inspection all but 14 smartphones (at the time of publication) were fixed and were receiving the pop-up notification. SFPD has since followed up to address the remaining smartphones.

Finally, on April 24, 2020, SFPD published Department Bulletin 20-01, User Acceptance Agreement on Department Devices, that establishes protocols for the Technology Unit to ensure all officers receive the pop-up notification when logging in to a department device.

Based upon all of the above, the California Department of Justice finds that SFPD is in substantial compliance with this recommendation. Please let us know if you have any questions or would like to discuss these further. Thank you.

# 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. The advice in the memo (found in appendix K on page 380) sent on May 5, 2016, has not been completed by the SFPD. The recommended audit is to ensure organizational integrity regarding the potential for bias in departmental electronic communications.

**Recommendation # 24.5** – The SFPD should require all members to acknowledge appropriate use standards for electronic communications. This should be a signed acknowledgement, retained in the personnel file of the member, and department personnel should receive an alert reminding them of appropriate use whenever they sign onto SFPD Systems.

**RFI Response Date: July 2, 2020**

## Executive Summary:

To verify substantial compliance on recommendation 24.5 of the Collaborative Reform Initiative (CRI), the San Francisco Police Department (SFPD) made several changes over the past few years. These changes include policy and procedure updates and ongoing audits to ensure that all members are acknowledging appropriate use standards for electronic communications.

One such policy update is SFPD Department Bulletin 19-051, which was issued to modernize and expand the rules surrounding use of department owned electronic devices. This department bulletin is attached and titled "SFPD Members' Expectation of Privacy, Use of Computers, Peripheral Equipment and Facilities ". Department Bulletin 19-051 was distributed to all members. This new department bulletin updated Department General Order #10.08. (See Attachment #1; DB 19-051 & Attachment #2; DGO 10.08).

To ensure that members are compliant in acknowledging department bulletins the SFPD also developed a new procedure for signing off on all department bulletins. This new process requires employees to sign department bulletins electronically in the Human Resource Management System (HRMS). Members were given information and instructions on this process by the issuance of Department Bulletin #19-156, titled "Mandatory Sign-off of Department Issued Documents in HRMS, Human Resource Management System." (See Attachment #3: DB 19-156).

The updated procedure for electronic acknowledgement/sign-off of department bulletins in HRMS provides immediate access to each members document signing history. Member signatures are retained on the computer in HRMS as a permanent record in the member's

electronic personnel file. Attachment #4 provides a sample of a member's document signing history. (See Attachment #4; HRMS Personnel File for Document Sign-off)

The storage of sign-off records in HRMS assists supervisors in verifying member compliance. An audit report is generated monthly in HRMS for members who are not in compliance with the electronic document sign-off procedure. The results of such audits are sent to the Officer in Charge (OIC), at the relevant unit. The OIC is responsible for member compliance and recommending disciplinary action for non-compliance. When members are not in compliance, the first step is email contact by training coordinators at their unit. For a sample of this email contact, see Attachment #5: Non-compliance emails. Additionally, an audit of Department Bulletin #19-051 shows that out of 2,870 members, 2,818 are in compliance, which is a 98% success rate for sign-off on this particular document. An audit of Department Bulletin #19-156 shows that out of 2,900 members, 2,827 members completed sign-off for a similar 97.5% compliance rate. (See Attachment #6: Audit of member acknowledgment for Department Bulletin 19-051 and Department Bulletin #19-156.

If a member does not sign to acknowledge written orders, and the supervisor does not enforce the signing policy, then both would be subject to disciplinary action in violation of DGO 2.01, Section 10, Failure to obey all written orders, policies, and procedures of the department. (See Attachment #7: DGO 2.01, Section 10)

A new pop-up alert and disclaimer was implemented by the SFPD and circulated to all communication devices connected to the SFPD Network, such as department issued computers and cellphones. SFPD Department Bulletin #17-011, titled "Pop-up Network Acceptable Use Statement on Workstations" was distributed to all members. This bulletin informed all members that they must acknowledge the alert, which discusses appropriate computer use policy, before being allowed to use their department computer/cellphone. (See Attachment #8: Department Bulletin #17-011 & Attachment #9; Pop-up alert images from department owned computers & cellphones).

The aforementioned pop-up alert references the following policy/law within the text of the alert: Attachment #10: Department Bulletin #16-089 and Attachment #11: California Penal Code 502; The crime of unauthorized computer access.

An inspection was initiated by the SFPD Staff Inspections Unit (SIU) to ensure that the aforementioned pop-up alert disclaimer was in fact being circulated to all department owned electronic communication devices. This inspection utilized random sampling of department devices at various district stations. The inspection found that 2 department cellphones within this random sample were not displaying the pop-up disclaimer. In response to this deficiency, a department-wide inspection revealed that 234 department cellphones were not displaying the pop-up alert disclaimer, which IT determined was related to an unwanted application. (See Attachment #12: SIU Electronic Communications Inspection).

Members were contacted and instructed on application removal in order to bring their devices into compliance. For officers not responding to this communication, the OIC at each unit

associated with non-compliant cell phones was contacted. Each OIC engaged in compliance efforts with members and completed a memorandum detailing their progress. (See Attachment #13: App removal instructions & Attachment #14: SFPD Cellphone Compliance Memos)

As a remedial action, an SFPD Unit Order was issued for the SFPD Technology Division. This Unit Order established protocols to ensure ongoing review of all electronic devices for implementation of the pop-up alert prior to deployment into the field. (See Attachment #15: Technology Division Unit Order for User Acceptance Agreement on Department Devices).

Finally, an updated audit by the SFPD SIU, conducted on May 05, 2020, revealed that there are only 14 department cellphones remaining that are not displaying the pop up alert. (See Attachment #16: SIU audit of remaining non-compliant cell phones).

**Compliance Measures:**

**Please Note:** Recommendation 24.5 was returned for further information (RFI). Per the Hillard Heintze Review Recommendation, Compliance Measures 1 and 2 have been met, whereas Compliance Measures 3 and 4 were not met. This RFI response includes updated information for all 4 Compliance Measures, as well as newly requested information for Compliance Measures 3 and 4 in order to fully answer this entire recommendation.

1) **Establish policy regarding appropriate use standards for electronic communications.**

   Pursuant to the Hillard Heintze File Review response from 6/11/2019 for Recommendation for 24.5, Compliance Measure #1 has already met substantial compliance. The below is inclusive of the prior submission from 6/11/2019, with updated information.

   In order to verify substantial compliance for CRI recommendation 24.5, the SFPD updated department policy related to appropriate use of electronic communication devises. This policy, which includes the use of department issued computers and cell phones, was updated and expanded in Attachment #1; SFPD Department Bulletin #19-051, issued on 03/21/2019 and distributed to all members. This bulletin is an update to Attachment #2; Department General Order #10.08 and serves to modernize and expand the policy surrounding the use of department owned electronic devices. This bulletin reminds members that department computers, cell phones, and other electronic devices owned by the SFPD are for official use only and, with said use, there is no expectation of privacy. Department General Orders (DGOs), such as DGO 10.08, are SFPD's overall policy and procedure manual. DGO #10.08 provides overall policy for SFPD members related use of computers and peripheral equipment.

Additionally, in order to further ensure appropriate use standards for electronic communication, the SFPD developed a pop-up alert message. This pop-up alert was created for use with all SFPD electronic devices, including department computers and cellphones connected to the SFPD Network. Attachment # 8; SFPD Department Bulletin #17-011, titled "Pop-up Network Acceptable Use Statement on Workstations", was distributed to all members. DB 17-011 described the pop-up alert and notified members of their requirement to acknowledge the acceptable use policy each time they utilize SFPD equipment. This text of the alert reminds members of appropriate use standards and also reminds them that there is no expectation of privacy when signing onto SFPD owned electronic devices. The pop-up alert is displayed every time an SFPD member signs into an SFPD Computer System, and the member must acknowledge the pop-up statement before being allowed to use any department computer or department cellphone.

As part of the Hillard Heintze File Review Recommendation (RFI) for Rec. 24.5, we were asked to provide a "screen shot" showing the pop-up alert in use. Samples of this pop-up alert are included in Attachment #9; Pop-up alert images from department owned computers & cellphones.

The text of the pop-up alert, which appears on department computers and cellphones, references the following 3 documents.

- Department Bulletin #16-089; Department Email Policy and Procedures. This bulletin reminds members of the policy surrounding department email, including proper use and rights to privacy. (See Attachment #10: DB 16-089)
- Department General Order 10.08: Describes overall policy for SFPD members related use of computers and peripheral equipment. (See Attachment #2: DGO 10.08)
- California Penal Code 502; This is a statute that defines the crime of unauthorized computer access. (See Attachment #11: CA Penal Code 502)

**2) Require signature of all employees and retained in personnel file.**

Pursuant to the Hillard Heintze File Review response from 6/11/2019 for Recommendation for 24.5, Compliance Measure #2 has already met substantial compliance. The below is inclusive of the prior submission from 6/11/2019, with updated information.

In order to maintain better personnel records pertaining to acknowledgment of department policy, the SFPD developed a new procedure for sign-off on department related materials in the Human Resource Management System (HRMS). The new sign-off process is electronic, and provides easy access to new and updated policies and procedures, such as Department Bulletins. Attachment #3: SFPD Department Bulletin #19-156, titled "Mandatory Sign-off of Department Issued Documents in HRMS, Human Resource Management System", was distributed to all members. DB #19-156 provides

members with information and instructions pertaining to this electronic sign-off process. After a member signs a document, a sign-off report is electronically retained in HRMS as a permanent record for each member's personnel file (See Attachment #4; HRMS Personnel File for Document Sign-off). Per SFPD policy, members are required to electronically review and sign for all documents in HRMS within 30 days of the document issue date.

In response to the Hillard Heintze File Review Recommendation (RFI) for Rec. 24.5, the SFPD was asked if the department considers pop-up alert acknowledgment to be a sufficient substitute to placing a signed acknowledgment in the member's personnel file. The SFPD does not believe that the pop-up alert alone is enough to satisfy acknowledgment of appropriate use standards. For that reason, the SFPD issued Attachment #8: Department Bulletin #17-011; Pop-up Network Acceptable Use Statement on Workstations, which was signed by members. This signed acknowledgment is stored in the Human Resource Management System for each member's electronic personnel file.

**3) Evidence of ongoing review and audit.**

The storage of sign-off records in HRMS assists supervisors in verifying member compliance. Since records are now electronically retained, compliance related information is easily accessible for ongoing review and audits. An audit report is generated monthly in HRMS to determine if members are in compliance with the electronic document sign-off procedure. Training Coordinators review the audit for members in their training group to ensure compliance of the posted documents. The Training Coordinators then remind members via email of any documents pending sign-off. This reminder is sent to members via email and the member's supervisor is copied on any email related to non-compliance status. A sample of this sort of email for gaining compliance is included in Attachment #5: Non-compliance emails. In addition to the unit level audit, the SFPD Training Division conducts random compliance audits and forward non-compliance reports through the chain of command to the respective Bureau Chiefs for compliance. The results of such audits are sent to the Officer in Charge (OIC), at the affected member's unit for review and to gain member compliance. This process is described in Attachment #3: SFPD Department Bulletin 19-156; Mandatory Sign-off of Department Issued Documents in HRMS.

Note that at any given time, various members of the SFPD may be off from work, and therefore unable to comply with the sign-off policy, specifically related to the 30-day time constraint. Examples of reasons employees may be off from work include, but are not limited to, the following: vacation, family leave, maternity leave, military deployment, disciplinary leave, medical disability, separation from the department, etc. The aforementioned examples of member related leave allot for difficulty in 100% compliance, as employees are delayed in signing. Such is the case in Attachment #6: Audit Report of Department Bulletin #19-051, which shows that out of 2,870 members, 2,818 are in compliance, which is a 98% success rate for sign-off on this particular

document. Similarly, and also included within Attachment #6, is the Audit of Department Bulletin #19-156. This audit shows that out of 2,900 members, 2,827 members completed sign-off for a 97.5% compliance rate. The SFPD has seen a significant improvement in compliance tracking ability and member compliance since the implementation of the electronic sign-off procedures.

As part of the Hillard Heintze File Review Recommendation (RFI) for Rec. 24.5, the SFPD was asked to develop an audit process that identifies if the pop-up network works as intended. In response to this, the SFPD Staff Inspection Unit (SIU) conducted a review and audit of the pop-up alert disclaimer. This inspection was in order to ensure that SFPD personnel are continuing to receive an alert reminding them of appropriate use on all department computers and cellphones. The SIU began this review process on September 3rd of 2019, by performing an inspection, which consisted of a random sampling of desktop computers and smartphones from various district stations. From these random samples, the SIU determined that all SFPD computers that were examined properly displayed the pop-up disclaimer. However, the SIU found that 2 department cellphones in this random sample failed to display the disclaimer. Further review of all department cellphones revealed that a total of 234 in-service cellphones were not properly displaying the pop-up disclaimer. The IT division determined that this was due to an unwanted application called "AirWatch", which was residing in the listed 234 cellphones. This application prevented the smartphones from receiving the disclaimer wirelessly from the SFPD network.

Hillard Heintze also requested, as part of the RFI, that the SFPD Identify the technology & cell phone audit process. The details of this process are described above and the full review and audit inspection process is included in Attachment #12, "SIU Electronic Communications "Disclaimer" Inspection." Furthermore, to satisfy this RFI request, the SFPD completed a Unit Order which established protocols to ensure that all electronic devices issued to members of the SFPD have implementation of a pop-up dialog prior to any device being deployed into the field. The full unit order is included in Attachment #15: Technology Division Unit Order for the User Acceptance Agreement on Department Devices).

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

The SFPD requires all members to acknowledge and sign-off on all department related documents. These signed acknowledgements are retained in the personnel file of the member. When the SFPD determines that a member is out of compliance pertaining to sign-off and acknowledgment of department policy, the following supportive and remedial actions are taken. As a supportive action, the member is first reminded via email by their training coordinator, and the OIC is copied on this email. Following this supportive action, as a remedial action, the OIC is required to follow up with the member to ensure compliance. Further remedial action results in the OIC recommending disciplinary action for non-compliance. If a member does not sign to

acknowledge written orders, and the supervisor does not enforce the signing policy, then both would be subject to disciplinary action in violation of (Attachment #2) DGO 2.01, Section 10, Failure to obey all written orders, policies, and procedures of the department.

In response to the Hillard Heintze RFI for Rec. 24.5, the SFPD was asked to identify what action was taken regarding 285 employees who were not compliant with signing off on Department Bulletin #19-051. Attachment #6, which includes both Audit reports for SFPD Department Bulletin #19-051 from June 2019 and April 2020, shows that the number of non-compliant members went from 285 (9.5%) in June of 2019 to just 32 members by April of 2020 (1.1%). This dramatic decrease is due to the aforementioned disciplinary procedure related to non-compliance. Members were notified by their OIC and the described remedial actions were taken to gain appropriate compliance, as described in Attachment #3: SFPD Department Bulletin # 19-156; Mandatory Sign-off of Department Issued Documents in HRMS. The remaining 1.1% of the SFPD who have yet to sign DB #19-051 may be off from work, and therefore unable to comply with the 30-day sign-off policy. As described above, various examples of leave including vacation, family leave, maternity leave, military deployment, medical disability, and other forms of separation from the department can account for the inability to reach 100% compliance.

During the course of SFPD SIU pop-up alert inspection, members have received supportive action from the department in order to re-establish the appropriate use reminders on the affected cellphones. Members have been contacted by the SIU for assistance in removing the unwanted application. The members were provided with "Step by Step" application removal instructions, as described in Attachment #13: App. removal instructions, which were created by IT and distributed via email. Additionally, as a supportive action, all members have access to assistance 24 hours a day, 7 days a week, from the IT division via the SFPD IT Help Desk.

The SFPD conducted remedial action related to the cellphone pop-up alert issue in two different ways. The first action was in the form of direct contact with members in possession of non-compliant phones via the member's OIC. After contacting the member, the OIC submitted a memorandum through the chain of command describing corrective measures and compliance gained by each member. Two of the discussed memorandums are included in this file as an example of the remedial action taken in Attachment #14: SFPD Cellphone Compliance Memos. The second form of remedial action was completed by issuing a Unit Order to the SFPD Technology Division on 4/24/2020. This unit order established protocols to ensure that all electronic devices issued to members of the SFPD have implementation of a pop-up dialog prior to any device being deployed into the field. The full unit order is included in Attachment #15: Technology Division Unit Order for the User Acceptance Agreement on Department Devices).

# Collaborative Reform Completion Memorandum

The SFPD has achieved great success in identifying and correcting deficiencies related to the pop-up alerts for appropriate use on SFPD Systems. The remedial actions that the SFPD has taken have also been largely successful. Currently (as of 05/05/2020) the SIU has determined that there are only 14 cellphones remaining, which continue to possess the unwanted application. Of those 14 cellphones, 6 are issued to officers on medical leave, which means that just 8 in-service cellphones are non-compliant. In essence, with only 8 department cellphones remaining from the original 234, this audit and remedial action created a 96.6% compliance increase. See the summary of this compliance increase in Attachment #16: SIU audit of remaining non-compliant cellphones.

In conclusion, the SFPD SIU Monitoring Team will continue their inspections and audits related to appropriate use on all department computers and cellphones. The SIU Monitoring Team will also complete monthly audits and continue compliance efforts for the remaining 14 cellphones with pop-up alert deficiencies. Thirty days following the SFPD Chief of Police's approval of Attachment #12: Electronic Communications "Disclaimer" Inspection, the SIU's Monitoring Team will conduct a follow-up to ensure that any out-of-compliance members are in full compliance. The SIU's Monitoring Team will then generate and attach an addendum documenting a full compliance finding.