Minneapolis
City of Lakes

MPD DVS Systems Access and Breach Investigations Audit

City of Minneapolis

Internal Audit Department

May 17, 2021

Table of Contents

Executive Summary

In response to a court order from Civil Case No. 13-3562 issued on September 3, 2020, the City of Minneapolis (the "City") Internal Audit department conducted an audit of the Minneapolis Police Department's (MPD's) use of the Minnesota Driver's and Vehicle Services (DVS) database. The objective of this audit was established in the court order, namely, to examine the Internal Affairs Division ("Internal Affairs") investigative process as it relates to allegations of violations of the Driver's Privacy Protection Act (DPPA) and MPD's established controls for the use of the DVS system. Appropriate controls for accessing the DVS system reduces the likelihood of DPPA violations, detects misuse, and corrects violations by holding the party that misused the system accountable.

The audit scope and approach, testing results, and conclusion are discussed below, followed by a description of Internal Affairs processes in the background section and a detailed description of observations and management's action plans in the final section.

Audit Scope and Approach

The scope of this engagement covered Internal Affairs investigations from January 1, 2018 to April 1, 2021. It also covered current controls that reduce the likelihood of misuse and detect potential violations. To assess Internal Affairs investigations, Internal Audit performed the following:

- Reviewed policies and procedures for investigating Internal Affairs complaints, including any specific documentation for cases involving DPPA violation allegations;
- Requested a sample of DPPA violation cases and reviewed whether investigations followed documented processes;
- Attempted to compare sample of DPPA violation investigations to non-DPPA investigations for consistency; and
- Requested a comparative sample of DPPA investigations to determine whether investigations involving female complainants differed from those not involving female complainants.

To assess DVS Access Controls, Internal Audit performed the following:

- Reviewed policies and procedures describing access and use of DVS databases;
- Reviewed training provided to employees regarding DVS databases;
- Reviewed permissions and access procedures to determine whether only valid users can access DVS databases; and
- Reviewed procedures for detecting improper use of DVS databases.

Results

As a result of this audit, one issue was identified. The issue was remediated before the conclusion of the report. The detail is listed below:

1. The process the Minneapolis Police Department (MPD) Business Technology Unit (BTU) uses to determine the legitimacy of DVS queries they receive from the Bureau of Criminal Apprehension (BCA) is not documented. (MOD)

Table 1 below contains the overall evaluation of the severity of the risk and the potential impact on operations. There are many areas of risk to consider including financial, operational, compliance, and reputational when determining the relative risk rating. Issues are rated as High, Moderate, or Low.

Table 1

High	Moderate	Low
	The process the Minneapolis Police Department (MPD) Business Technology Unit (BTU) uses to determine the legitimacy of DVS queries they receive from the Bureau of Criminal Apprehension (BCA) is not documented.	

- **High Risk:** Some key controls do not exist or are not effective resulting in impaired control environment; high risk improvement opportunities require immediate corrective action
- **Moderate Risk:** Adequate control environment in most areas; moderate risk improvement opportunities identified which require corrective action
- **Low Risk**: Satisfactory overall control environment; small number of lower risk improvement opportunities identified which do not require a management action plan

The detail of this observation is included within the *Observation and Management's Action Plan* section of this report, beginning on page 8.

Conclusion

Overall, the MPD's internal controls related to DVS access and DPPA investigations are satisfactory. Internal Affairs no longer investigates DPPA allegations; civilians from the Department of Civil Rights – Office of Police Conduct Review investigate these cases, as evidenced by case documents. Only one instance of an investigation related to a potential DVS access violation occurred between 2018 and 2021, and that case was transferred to the Office of Police Conduct Review.

Further, MPD regularly trains all officers on the appropriate use of the DVS system and indicates that misuse will result in termination. The MPD Business Technology Unit regularly checks that all users are valid employees and removes accounts when employees separate from the City. Users can only access the system using a valid City account, and accounts can be quickly deactivated by removing active directory access.

Internal Audit would like to note one observation outside of the scope of this audit. Detective controls locate potential occurrences of control failures, allowing the entity to investigate and remediate when necessary. In this instance, detective controls would alert authorities when searches deviate from expected norms. The MPD does not have access to user search logs for its employees; that is maintained by the BCA. The BCA employs a limited system for detecting potential misuse, but that system is unlikely to detect improper searches unless they involve specific individuals (celebrities, politicians, public figures). While MPD has no control over this BCA function, it is worth noting that it would not necessarily detect the type of searches that led to the original lawsuit.

Internal Audit would like to thank the Minneapolis Police Department, the Business Technology Unit, and the Internal Affairs Division for their cooperation and time during this engagement.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Team for this Engagement

Ryan Patrick, CIA – Internal Audit Director
Huguette Essoh Latte, CIA – Internal Audit Manager
Comlan Alede – Internal Auditor
Travis Kamm – Internal Auditor

Minneapolis Police Department Primary Contacts

Commander Thomas Wheeler, Internal Affairs Unit
Commander Travis Glampe, Business Technology Unit
Commander Travis Glampe, Business Technology Unit

Lieutenant Jeff Rugel, Business Technology Unit
Lesli Norman, Business Technology Unit

City Attorney Primary Contact

Brian Carter, City Attorney

Office of Internal Audit

Phone: (612) 673-5938
Email: InternalAuditDepartment@minneapolismn.gov
Website: http://www.ci.minneapolis.mn.us/audit

Background

Program Goals and Objectives

The Minneapolis Police Department's Internal Affairs Division (IAD) investigates allegations of police misconduct. The IAD includes a commander who supervises a lieutenant. The lieutenant supervises a compliment of sergeants who conduct investigations. IAD also employs civilians in administrative and technical roles.

The IAD seeks to neutrally investigate allegations of police misconduct with the ultimate outcome decided by the Chief of Police. The Chief may issue discipline based on the information presented in the investigation.

Leadership and Organizational Structures

The Chief of Police appoints the Deputy Chief of Professional Standards, who oversees IAD, and the Internal Affairs Commander. The Commander oversees the lieutenant, sergeants, and administrative staff of the unit.

Background and Overview

The IAD, along with the Office of Police Conduct Review, investigates allegations of police misconduct. This audit considers investigations of potential violations of the Driver's Privacy Protection Act (DPPA), 18 U.S. Code § 2721[1], which defines the situations in which information stored in the Driver and Motor Vehicle Services database can be accessed. Section (a) prohibits disclosure of information by a State department of motor vehicles, with the relevant exception in § (b)(1), which allows access for a government agency "in carrying out its functions." Hence, Minneapolis police officers can access the information so long as they are doing so in the course of law enforcement business.

If information is accessed by Minneapolis police officers not for a law enforcement purpose, they could be in violation of the DPPA and Minneapolis Police Department policy. For example, if officers used their access to the DVS system to look up personal information of celebrities or coworkers, not in the course of business, they would have improperly accessed protected information. Internal Affairs may then be tasked with investigating the alleged violation.

This audit arises from a lawsuit filed against the City of Minneapolis, in which plaintiff alleged improper uses of the DVS system to access her personal information. In a court order, Judge Donovan Frank noted "inconsistencies in past investigations"[2] of the alleged DPPA violations and ordered this audit.

[1] Details can be found here

[2] See order filed by Judge Donovan Frank, 13-cv-03562-DWF-TNL

Observations and Management Action Plans

ISSUE #1

There is no documented process for responding to BCA inquiries regarding DVS queries. (MOD)

Observation

The process the Minneapolis Police Department (MPD) Business Technology Unit (BTU) uses to determine the legitimacy of DVS queries they receive from the Bureau of Criminal Apprehension (BCA) is not documented. The BCA sends a notification to MPD command staff when a DVS query meets certain conditions. The BCA requests that MPD look into the query to determine whether it had a legitimate business purpose. Staff from the MPD BTU do an initial search to determine whether a report or explanation for the search exists. If there is no reason for the search, the instance is forwarded for a misconduct investigation.

Several risks arise when processes are not formally documented. First, if the BTU were to change staff, a new employee may not have adequate documentation to rely on for training, which can cause inconsistency and untimely responses to BCA inquiries. Second, a lack of process documentation does not provide criteria for conducting a proper reponse to a BCA inquiry. The BTU explained the process, but without supporting process documentation, there is no benchmark to ensure that staff follow a consistent process for each and every inquiry. Management cannot evaluate whether the process continues to meet business needs and is consistent with best practices. Third, without a documented process, staff outside of the BTU may not be aware of the current practice, and errors may occur if they attempt to respond to the inquiry.

Recommendation and Management Action Plan

Management agreed to develop a formal Standard Operating Procedure to address the audit observation. This was completed on April 30, 2021.

Target remediation date: April 30, 2021
Responsible party: Lt. Jeff Rugel