




CLOSED CASE SUMMARY

ISSUED DATE: AUGUST 25, 2023

FROM: DIRECTOR GINO BETTS 
OFFICE OF POLICE ACCOUNTABILITY

CASE NUMBER:

Allegations of Misconduct & Director’s Findings

Named Employee #1

Allegation(s):		Director’s Findings
# 1	12.050 - Criminal Justice Information Systems 2. Inquiries Through ACCESS, or Any Other Criminal Justice Record System, Are Only to Be Made for Legitimate Law Enforcement Purposes	Sustained
# 2	12.050 - Criminal Justice Information Systems 6. All Employees Shall Adhere to WASIS and NCIC Policies	Sustained
# 3	5.002 - Responsibilities of Employees Concerning Alleged Policy Violations 6. Employees Will Report Alleged Violations	Sustained

Imposed Discipline

Written Reprimand

This Closed Case Summary (CCS) represents the opinion of the OPA Director regarding the misconduct alleged and therefore sections are written in the first person.

EXECUTIVE SUMMARY:

The Complainant alleged that Named Employee #1 (NE#1) made an unauthorized ACCESS computer system search.

ADMINISTRATIVE NOTE:

On June 27, 2023, the Office of Inspector General (OIG) certified OPA’s investigation as thorough, timely, and objective.

SUMMARY OF INVESTIGATION:

On February 27, 2023, the Complainant—a Bothel Police Department captain— emailed an OPA complaint. The complaint stated that a Seattle Police Department (SPD) sergeant potentially violated their ACCESS, a statewide computer system that draws criminal justice information from local, state, and federal databases, privilege. OPA spoke with the Complainant, who directed OPA to Botel Officer #1 (BO#1)—who reported the potential violation to the Complainant. BO#1 only knew NE#1 as “Bill.” BO#1 told OPA that on February 25, 2023, around noon, Community Member #1 (CM#1)— “Bill’s” wife—approached him with a backpack containing a firearm. CM#1 told BO#1 that she



and NE#1's son, Community Member #2 (CM#2), was suicidal and asked BO#1 to safeguard the firearm until a safe place was identified.

The next day, BO#1 said that NE#1 came to retrieve the weapons. BO#1 said that NE#1 told him that he suspected CM#2 had another firearm in the house, so he ran CM#2's name in ACCESS and learned CM#2 had another firearm registered at NE#1's home. NE#1 stated that he located and secured that weapon. BO#1 confronted NE#1 about using ACCESS for personal use, and NE#1 agreed to self-report his action to SPD.

OPA opened an investigation. A remote log check showed that on February 25, 2023, NE#1 was logged as in-service, was not assigned calls, and did not use his mobile data terminal to run computer checks. However, searches on computers inside SPD facilities do not appear on remote log searches.

On March 6, 2023, OPA contacted SPD's ACCESS liaison to confirm whether CM#2's name was run on February 25th and whether NE#1 self-reported the violation. The next day, SPD's ACCESS liaison confirmed that NE#1 ran CM#2's name in ACCESS on February 25th, that the search violated ACCESS rules, and that the violation was not reported to SPD's data center.

On June 2, 2023, OPA interviewed NE#1. NE#1 acknowledged knowing that using ACCESS for personal use was forbidden. NE#1 also acknowledged being trained on the rules before being granted ACCESS privileges. NE#1 told OPA that on February 25th, he searched a family member's name on ACCESS and that the search was unrelated to an SPD investigation.

Further, NE#1 said that on February 22nd, he saw CM#2 at a coffee shop instead of work, where he was scheduled to be. NE#1 said CM#2 confided in Community Member #3 (CM#3)—a pastor and family friend. CM#3 told NE#1 that CM#2 was in a dark place and had suicidal thoughts. NE#1 said that on February 25th, while at work, CM#1 called and told him that CM#2 had access to a firearm.¹ NE#1 was also told that CM#2 paced in circles in their driveway, "yelling about nonsense," including from his job, the economy, and his relationships. NE#1 said he searched CM#2 in ACCESS solely to learn whether a firearm was registered to him and unchecked the other boxes. After verifying that CM#2 had another firearm registered to him, NE#1 instructed CM#1 to take the backpack containing the previously recovered firearm to BO#1, their neighbor. NE#1 said he retrieved the firearm from BO#1 the following day and told BO#1 about the situation. NE#1 said that when he received OPA's five-day notice, he believed there was no longer a need to self-report. NE#1 also denied telling BO#1 that he would self-report violated ACCESS rules.

ANALYSIS AND CONCLUSIONS:

Named Employee #1 - Allegation #1

12.050 - Criminal Justice Information Systems 2. Inquiries through ACCESS or any other criminal justice record system are only to be made for legitimate law enforcement purposes.

The Complainant alleged that NE#1 searched a criminal justice record system for a non-law enforcement purpose.

¹ NE#1 said he confiscated a firearm from CM#2 in late 2022.



ACCESS inquiries made for personal use, inappropriate use, or dissemination of the information can result in internal discipline and penalties under federal and state law. SPD Policy 12.050-POL-2.

Here, NE#1 admittedly searched CM#2's information in ACCESS for non-law enforcement purposes. Although NE#1 had a legitimate concern that prompted the search, it nevertheless, as SPD's ACCESS liaison confirmed, violated ACCESS' rules. Specifically, "The Department of Justice Criminal Justice Information System (CJIS) restricts the use of all criminal-related databases to official investigations when conducted while working for a criminal justice organization." SPD Policy 12.050-POL-6(3). Where CM#2 was not the subject of an SPD investigation, NE#1's search was unauthorized. The Washington State Patrol ACCESS manual also lists "running criminal history on family or friends," as unauthorized non-criminal justice purposes. Washington State Patrol ACCESS Manual Chapter 1 Section 5. Moreover, he confirmed with OPA that he told BO#1 that he might be suspended for the search, evidencing that NE#1 knew it was prohibited.

Accordingly, OPA recommends this allegation be Sustained.

Recommended Finding: **Sustained**

Named Employee #1 - Allegation #2

12.050 - Criminal Justice Information Systems 6. All employees shall adhere to WASIS and NCIC policies.

The Complainant alleged that NE#1 violated Washington State Identification System (WASIS) and National Crime Information Center Interstate (NCIC) policies.

Employees must adhere to WASIS and NCIC policies, including not sharing inquiry results with anyone outside the department (except a prosecutor) and only making inquiries for official criminal backgrounding investigations. SPD Policy 12.050-POL-6.

Here, NE#1 shared with CM#1 and BO#1 that his ACCESS inquiry showed that CM#2 had another registered gun. That action and those noted at Named Employee #1 – Allegation #1 violated this policy.

Accordingly, OPA recommends this allegation be Sustained.

Recommended Finding: **Sustained**

Named Employee #1 - Allegation #3

5.002 - Responsibilities of Employees Concerning Alleged Policy Violation 6. Employees will report alleged violations.

Employees will report any alleged minor policy violation to a supervisor and any serious violation to a supervisor or directly to OPA. SPD Policy 5.002-POL-6.



Here, NE#1's violation occurred on February 25th. BO#1 told OPA that he confronted NE#1 on February 26th about the potential policy violation, and NE#1 agreed to self-report it. On February 27th, the Complainant made an OPA complaint about NE#1's possible violation. After efforts to identify the named employee, OPA sent NE#1 a 5-day notice on March 21st. Although NE#1 denied telling BO#1 he would self-report the potential violation, he admittedly told BO#1 it could result in a suspension. That indicated that NE#1 knew the search was potentially, at minimum, a minor policy violation requiring reporting to a supervisor. NE#1 told OPA that he did not believe self-reporting was necessary after he received OPA's five-day notice. Still, he did not receive that notice until 25 days after his potential misconduct.

Accordingly, OPA recommends this allegation be Sustained.

Recommended Finding: **Sustained**