



CLOSED CASE SUMMARY

ISSUED DATE: JUNE 18, 2019

CASE NUMBER: 2019OPA-0097

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	Not Sustained (Management Action)

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:

It was alleged that multiple SPD officers may have improperly accessed the NICS database.

ANALYSIS AND CONCLUSIONS:

Named Employee #1 - Allegations #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

OPA was forwarded an email from the chain of command indicating that an officer may have improperly accessed the National Instant Criminal Background Check System (NICS) database. OPA was informed that the officer was attempting to determine if she should pursue an Extreme Risk Protection Order (ERPO) and, as part of that review, learned contradictory information concerning whether or not the subject was lawfully permitted to own and possess firearms. In order to obtain conclusive information concerning this question, the officer ran a “free form” search of the NICS database. As a result of that search, the officer learned that there was an “ineligible to possess” entry for the subject that had been generated by the Redmond Police Department (RPD). The officer contacted RPD and was, in turn, referred to an employee of the Clyde Hill Police Department (CHPD), who had knowledge concerning the significance of the entry. The CHPD employee told the officer that she should not be using the NICS database to conduct this type of search. The CHPD employee sent the officer a link to NICS training materials, which explained who was permitted to search the NICS database and for what purpose. The officer reported this information and her actions to her supervisor. The supervisor directed his unit to stop using the NICS database for ERPO related searches; however, the supervisor noted that officers had been using the database for this purpose for the last 18 months. The supervisor confirmed with SPD’s public disclosure unit that the NICS database should not be used for ERPO related searches. Lastly, the supervisor reported all of the above to his chain of command, as well as to the Department’s Legal Counsel. The Department then notified Washington State Patrol of this matter.



SPD Policy 12.050-POL-2 states that inquiries through criminal justice systems, including NICS, “are only to be made for legitimate law enforcement purposes.” As detailed by the chain of command’s thorough review, while performed in good faith, the inquiries conducted by the Department in the context of ERPOs were technically inconsistent with the permitted usage of the NICS database. As set forth in the Washington State Patrol ACCESS Operations Manual, the use of NICS is only authorized for the transfer of a firearm, for the issuance/renewal of a concealed pistol license, and for the disposition of a firearm from evidence. The use of the database in this case did not conform one of these appropriate categories.

The above being said, SPD promptly identified this issue, took steps to end the practice of using the NICS database for ERPO-related searches, and self-reported to WSP. OPA finds that there was no intentional misconduct on the part of the Department or any individual officer. For these reasons, OPA recommends that this allegation be Not Sustained and issues the below Management Action Recommendation.

- **Management Action Recommendation:** OPA recommends that the Department reiterate to all officers the restrictions on the use of the NICS database and take affirmative steps, through additional training or revisions to the applicable policies, to ensure that the database is not improperly accessed in the future. To the extent that this has already been done, no further action needs to be taken by the Department.

Recommended Finding: **Not Sustained (Management Action)**