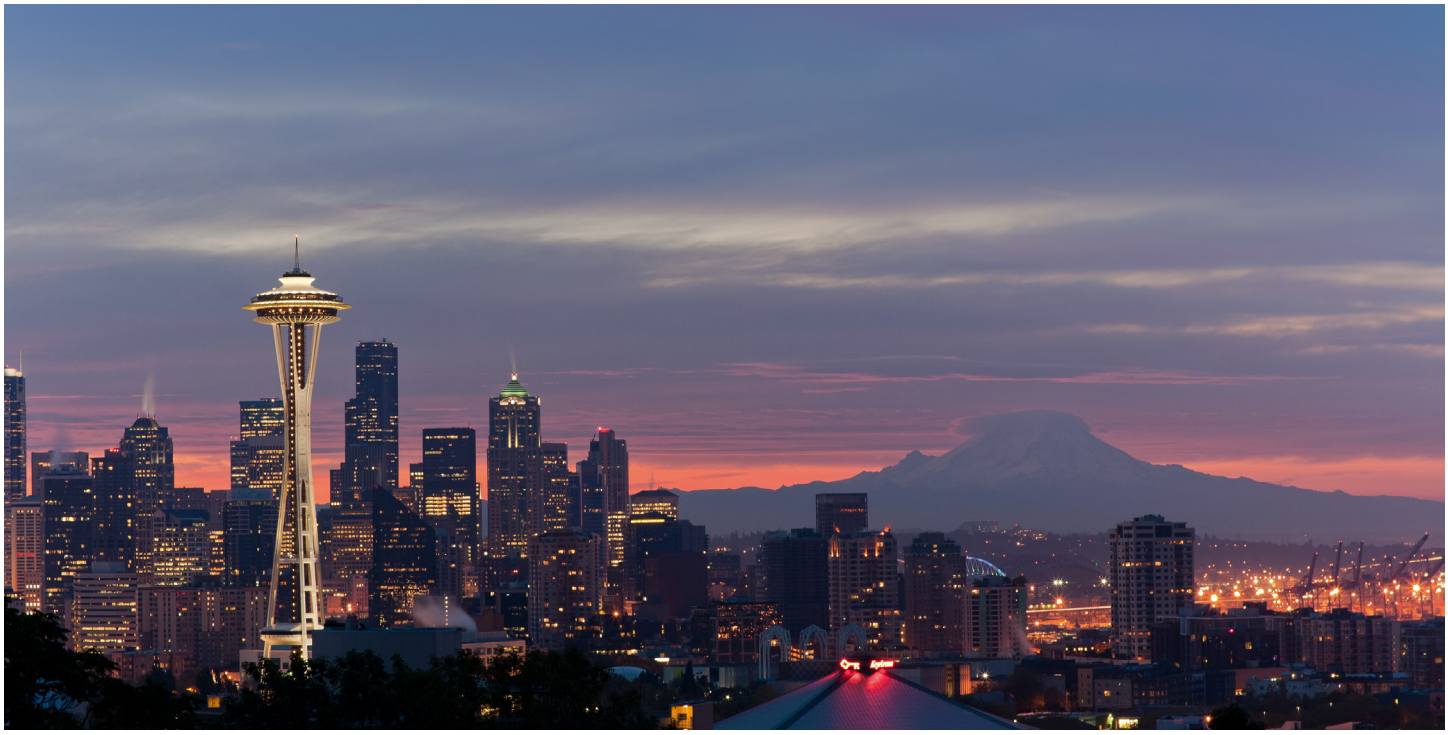
Seattle Office of Inspector General

Audit of SPD Compliance with Chapter 14.12 of Seattle Municipal Code, *Collection of Information for Law Enforcement Purposes*



Source: Dave Morrow, "Seattle Sunrise". Labeled for non-commercial reuse. www.DaveMorrowPhotography.com

The following report was produced by OIG in response to the audit requirements of Chapter 14.12 of Seattle Municipal Code.

Summary of Findings

OIG did not detect any violations of Chapter 14.12 of Seattle Municipal Code, *Collection of Information for Law Enforcement Purposes*. However, OIG identified several issues relating to the outdated language of the Chapter which prevent OIG from being able to determine whether SPD is in full compliance.

June 13, 2019

Table of Contents

Audit Selection

Chapter 14.12 of Seattle Municipal Code, *Collection of Information for Law Enforcement Purposes*, requires an audit every 180 days of Seattle Police Department (SPD) activity relating to the Chapter. Ordinance 125315, passed in 2017, assigned this responsibility to the Office of Inspector General (OIG). The first Inspector General was appointed in 2018. This is the first audit completed by OIG regarding Chapter 14.12.

Findings Summary

OIG did not detect any violations of Chapter 14.12 of Seattle Municipal Code, *Collection of Information for Law Enforcement Purposes*. However, OIG identified several issues relating to the outdated language of the Chapter which prevent OIG from being able to determine whether SPD is in full compliance:

- The Chapter was adopted in 1979 and does not address modern methods of distributing information, resulting in inconsistent practices by different units within SPD. The current wording of the Chapter is not specific enough for OIG to determine whether some of these practices are in violation of City code.
- OIG was unable to determine whether past authorizations issued by SPD complied with the Chapter, as SPD disposed of relevant records in compliance with Chapter records retention requirements.

While OIG did not find any specific issues involving unauthorized collection of information in a review of patrol reports, OIG identified gaps in SPD training and policies which may create risks for future compliance.

Finally, OIG determined that SPD records retention practices do not align with the retention requirements of the Chapter. OIG acknowledges that the limits set by the Chapter for retaining records could conflict with state records retention requirements and restrict the ability of SPD to comply with public records requests or investigate misconduct and crime.

Background

Origin

In 1979, the Seattle City Council unanimously passed Ordinance 10833, which specified how the Seattle Police Department could collect, receive, transmit, and use information about an individual's sexual orientation, as well as information about the political and religious affiliations of individuals and organizations. The ordinance became Chapter 14.12 of Seattle Municipal Code, Collection of Information for Law Enforcement Purposes. At the time of its passing, Ordinance 10833 was recognized as one of the first local ordinances to restrict the type of information collected by police departments.[1]

Chapter 14.12 was written well before the introduction of the first internet browser.

Chapter 14.12 has not been substantially altered since its creation, other than to extend certain deadlines and assign audit duties for confidential files. As discussed in the findings of this report, the age of the chapter creates confusion regarding the acceptable use of technology and information sharing tools that have been invented and become widely used since the Chapter was written. As a point of reference, the internet browser was introduced in 1990. OIG consulted with the City Attorney's Office on language in Chapter 14.12 that OIG found to be unclear, which has informed the writing of this audit and OIG recommendations for areas where Chapter 14.12 language could be clarified.

Information Protected by Chapter 14.12

This audit focuses on the type of information controlled by Chapter 14.12, which covers two distinct categories of information: private sexual information and restricted information. Throughout this report, OIG uses the term "protected information" to refer to both types of information covered by the Chapter. The two types of information are explained in more detail in Exhibit 1.

There are some exemptions from what is considered protected information. Generally, if someone discloses personal information to a law enforcement agency, that information may be collected and used. For example, a victim may disclose their sexual orientation to an officer when explaining why they think they were the target of a bias crime. Other categories of exempted information include personnel records, jail records regarding prisoners' religious preferences, and confidential communications between SPD personnel and a legal advisor representing SPD.[2]

---

1 Michael Sweeney, "Seattle Law Limits Police In Intelligence Gathering," Washington Post, July 3, 1979, https://www.washingtonpost.com/archive/politics/1979/07/03/seattle-law-limits-police-in-intelligence-gathering/916c9159-31da-4a1f-ab55-9804ba5efa19/

2 See Seattle Municipal Code Ch. 14.12, Subchapter II, "Scope – Exemptions and Exclusions" for a full list of exempted and excluded information categories.

Exhibit 1: Categories of Information Protected by Chapter 14.12

Two types of protected information

Private sexual information is defined as any information about an individual's sexual practices or orientation.

Restricted information includes information about the following items:
1) An individual's political or religious associations, activities, beliefs, or opinions

2) The political or religious activities, beliefs or opinions and the membership, mailing, subscription, or contributor lists of certain types of organizations, including political and religious organizations; or

3) An individual's membership or participation in such an organization, in a political or religious demonstration, or in a demonstration for community purposes.

Source: Seattle Municipal Code Ch. 14.12.030 (H) and (K).

Collection of Private Sexual Information

Private sexual information can be collected if it appears reasonably relevant to the investigation of certain types of unlawful activity[3] or to making the arrest of a subject or fugitive. No authorization is required for collecting private sexual information. An officer can make their own judgment as to whether the Chapter requirement is met.

Collecting restricted information requires a written authorization in most circumstances.

Collection of Restricted Information

Before SPD personnel can collect restricted information, they must first ensure three requirements are met, and then must obtain a written authorization. The three requirements are outlined in more detail in Exhibit 2, below, but are generalized as (1) reasonable suspicion, (2) relevancy, and (3) consistency with the rest of the Chapter.

3 The relevant activities include a reported or observed sex crime, an apparent felony where a motivation for the crime may be reasonably suspected to be sexual in origin, or a violation of the law that by its nature is commonly related to sexual activity. See Seattle Municipal Code, Chapter 14.12.130.

If an SPD officer believes all three requirements are met, the officer must still obtain a written authorization from a unit commander or higher-ranking officer prior to collecting the restricted information. There are exceptions for exigent situations, but the officer must either follow up with a written authorization or purge the information within five days.[4] The authorization must describe the information to be collected and explain why it is permissible under Chapter 14.12.

Written authorizations can only be extended by the Chief of Police.

Written authorizations must be approved by a unit commander or higher-ranking officer and are for a specified period. The authorization period can be extended by the Chief of Police, but for no longer than the expiration of the statute of limitations or the prosecution of a case.

SPD must notify the auditor (OIG) of each authorization.

Exhibit 2: Requirements Before an Authorization to Collect Restricted Information Can Be Granted

The following requirements must be met before SPD can grant an authorization to collect restricted information.

Reasonable suspicion There must be reasonable suspicion of <u>at least one</u> of the following:

- ☐ the subject of the information has committed a crime, is in the process of committing a crime, or will commit a crime in the future;
- ☐ the information will lead to the arrest of the subject; or
- ☐ the information will help evaluate the reliability of a witness or victim, or help in discovering their knowledge.

Relevancy The restricted information must appear relevant to the investigation of the unlawful activity, witness, or victim.

Consistency The collection of the restricted information must be consistent with the statement of purpose, policies, and other provisions of Chapter 14.12.

Source: Seattle Municipal Code Ch. 14.12.030 (H) and (K).

4 The exact requirement depends on whether the information is needed for criminal investigation purposes or for dignitary protection purposes. See Seattle Municipal Code, Section 14.12.150 and Section 14.12.210.

Oversight of Chapter 14.12

Chapter 14.12 requires an auditor to review police department files and records relating to Chapter-related activities at least every six months (180 days).[5] This review includes each authorization granted in the time period under review, along with relevant investigative files, as well as a random check of department files and a review of files containing information scheduled to be purged (deleted). The results of the audit are sent to the Mayor, City Council, City Attorney, and City Clerk, and filed as a public record.

Certain files are exempt from auditor review. These include personnel files, internal investigation files, and personal files of the Chief of Police. Additionally, the auditor is not allowed to review files that exclusively contain confidential criminal information regarding organized criminal activity or narcotics activity. Chapter 14.12 requires the Chief of Police to review those files and issue a summary report to the Mayor.

Finding 1: Chapter 14.12 does not address modern methods of collecting, sharing, and using information, leading to inconsistent practices by SPD.

SPD does not have a consistent approach to collecting protected information accessed via social media or offered to SPD by third parties.[6] Observed practices include retaining information without written authorization, seeking authorizations to retain the information, or declining to retain the information.

The current wording of the Chapter is not specific enough for OIG to determine compliance with the Chapter in relation to the following:

- Collecting protected information about named individuals from third parties;
- Seeking written authorization to collect protected information that has been made public by the subject of the information using social media or other platforms; and
- Forgoing collection of protected information under the belief that such collection is prohibited by the department.

Chapter 14.12 provides limited guidance on the collection of information that is publicly available, but not self-disclosed to SPD.

Before discussing the observed practices in detail, it is important to discuss the requirements of the Chapter to understand why it is difficult to adapt the Chapter to the present day. Chapter 14.12 was written at a time when a reasonable person could assume that SPD would have to intentionally search for protected information about an individual. Before the advent of the internet and social media, collecting protected information might have been impossible without conducting

5 Chapter 14.12 specifies that the Mayor shall appoint an auditor for this task. Until 2015, this work was performed by Professor David Boerner. Ordinance 125315, passed in 2017, assigned this function to OIG.
6 By social media, OIG refers to public posts on platforms such as Facebook, Twitter, and Instagram; in other words, information that could be accessed by any person, not just SPD personnel.

surveillance, interviewing known acquaintances, or infiltrating groups. Today, however individuals may make protected information known via a public tweet or Facebook post. Chapter 14.12 is silent on how SPD should handle these types of open sources of information.

Chapter 14.12 does allow SPD to collect and use protected information that individuals volunteer about themselves, without SPD needing to first obtain a written authorization. However, the examples included in the Chapter involve intentional declarations of the information to SPD, such as:

- "A general questionnaire completed by an applicant or witness using his or her own words"; and
- "The subject of the information supplies the information to known departmental personnel".

The Chapter does not include examples that would help SPD apply the Chapter to modern day situations.

The Chapter does not include examples that would cover current day situations, such as SPD collecting protected information that an individual has volunteered via a public Facebook post. Thus, it is unclear to OIG whether SPD doing so would be in compliance with the Chapter.

The Chapter also includes a section on "materials open to public inspection", which do not require written authorization for SPD to collect. Information in this section must be accessible to any person during business hours and must be "readily available". Categories in this section include information in a library, printed information from a criminal justice agency, and information about anticipated political or religious events. The Chapter was written before information was made publicly available in other forms, such as the Internet. For information about anticipated political or religious events, the Chapter specifies that the information must be necessary for the direction and control of traffic, to protect public health and safety, and to secure public liability insurance covering the city.

Thus, while Chapter 14.12 may allow SPD to collect information for an upcoming political rally without a written authorization, it is less clear if SPD needs a written authorization to access information via an open source, such as reviewing an individual's publicly available Twitter feed in relation to a bias crime investigation.

The guidance on protected information offered by third parties – for example, a witness offering protected information about the subject of a crime – also lacks clarity. The Chapter permits the collection of protected information without written authorization about a subject whose identity is unknown. However, if the subject's identity is known, the Chapter does not provide clear guidance on whether the officer needs written authorization to retain information provided by a witness in a statement, or if this scenario falls under one of the exceptions described above.

The lack of clarity around when a written authorization is needed has resulted in inconsistent collection of information within SPD.

OIG noted that SPD collected protected information without written authorization in a small percentage of reviewed case files, but it is not clear whether a written authorization would have been required.

As described in more detail in Finding 2, OIG reviewed 295 case files to determine if protected information was collected without written authorization by patrol officers. While OIG did not identify any cases that appeared to be explicit violations of Chapter 14.12, OIG identified seven cases (2%) in which it was unclear whether the Chapter would require written authorization to collect certain pieces of information included in the officer's report.

OIG did not identify any cases in which the reporting officer referenced obtaining a written authorization to collect protected information.

The clearest example involved an officer who was responding to a report of bias-related graffiti on a building occupied by a religious institution. The graffiti included a swastika, among other items. The responding officer went to the institution's website, noted the mission of the institution, and recorded it in the narrative of the report. This information was available on a public website, but not directly provided to SPD by the institution itself or a witness.[7]

The other six cases involved officers collecting unverified information from third parties about a suspect's political or religious affiliations. In one case, a victim showed the officer the website of a political organization the victim believed had posted fliers on their building as part of a bias crime. The officer recorded the name of the organization in the narrative and collected pictures of the organization's website for his report. Other examples include a victim stating that the suspect was Muslim, and a victim describing how a suspect self-identified both as Muslim and as a member of Al Qaeda.

All of the collected information appeared directly related to the crime under investigation.

The information collected by the SPD officers appears directly relevant to the specific crime in each of the seven noted cases. On multiple occasions, SPD personnel stated to OIG their belief that if information was related to a crime, no authorization was needed to collect the information. One SPD officer also offered the reasonable argument that if SPD did not collect key information, the prosecuting attorney would ask that SPD gather that information before proceeding with the case.

7 Chapter 14.12 protects certain types of information about some organizations, specifically "the political or religious activities, beliefs, or opinions and the membership, mailing, subscription, or contributor lists of a political or religious organization, an organization formed for the protection or advancement of civil rights or civil liberties, or an organization formed for community purposes to organizations as well as individuals." See Seattle Municipal Code Chapter 14.12.030.K.2.

If the information is considered restricted, Chapter 14.12 requires written authorization to collect the information.

However, OIG was unable to find an exception in Chapter 14.12 that would waive written authorizations if information was related to a crime. Rather, Chapter 14.12 on its face *requires* that the information be relevant to a crime as part of the criteria for granting a written authorization. It is possible that SPD personnel are confusing the requirements for collecting private sexual information (which requires no written authorization) with the requirements for collecting restricted information. As described in more detail in Finding 3, SPD policy does not explicitly instruct personnel to obtain a written authorization before collecting restricted information, which may be the source of the confusion.

SPD Intelligence Section personnel stated they collect written authorization when collecting open source protected information, but such authorization may not be required.

The SPD Intelligence Section was the only unit that OIG encountered who were familiar with the Chapter 14.12 written authorization process. Intelligence Section personnel stated repeatedly that they obtain written authorizations when collecting restricted information they discover on social media and other open sources. Personnel indicated that although Chapter 14.12 does not reference these types of information sources, they nevertheless obtained the authorizations out of an abundance of caution. Staff went so far as to say that they would obtain a written authorization even if they "accidentally" came across protected information while reviewing the social media of a group or organization. Once the Intelligence Section has obtained a written authorization and collected restricted information, personnel must then ensure the information is stored in a secure location and purged when the authorization expires and/or there is no court-related hold on the information.

As described in Finding 2, OIG was unable to review past authorizations obtained by the Intelligence Section due to the deletion of older records, which occurred in compliance with Chapter 14.12.290.B.

SPD personnel reported not collecting relevant information because of the belief that collecting the information was prohibited by the department.

The SPD bias crimes coordinator informed OIG that she believes she is unable to collect certain types of information regarding hate and bias crimes occurring in the Seattle area. She noted that it is not uncommon for her to receive information on bias incidents from members of the community through informal channels.

As an example, the bias crimes coordinator cited photos of "Nazi" banners hung off overpasses that she received as texts, or photos of fliers found around the University of Washington campus. She stated that she would like to log these incidents in a spreadsheet, but she believed she was unable to do so because they reflect information about a political organization's activities and are not associated with a specific crime or formal complaint.

Accordingly, the bias crimes coordinator reported to OIG that she is unable to fully address public inquiries as to whether the level of white supremacist activity in Seattle has increased or decreased during a certain time period. The Chapter was written prior to the adoption of bias crimes laws and contemporary public safety responses to the prevention and investigation of such crimes.

The Intelligence Section provided an additional example of the non-collection of information. Staff explained that any photos taken by SPD at protests are supposed to be deleted at the end of the day, after being reviewed by the scene commander. Additionally, per SPD Policy 16.090-POL 1, Recording with ICV and BWV, officers are not permitted to activate their body-worn video during demonstrations unless they have probable cause to believe that criminal activity is occurring or they are instructed to record by a supervisor. According to Intelligence Section staff, there have been cases where SPD discovered that an incident occurred or an individual made a complaint after relevant SPD photos are deleted and no body-worn footage is available. In these situations, staff reported that SPD must sometimes request photos and footage of incidents from the public or news media in order to fully investigate the incident.

Recommendation 1: The Chief of Police should work with the City Attorney's Office to develop a clear policy for whether written authorization is required prior to collecting protected information from open sources or third parties. If necessary, the City should amend the code to provide the required clarity.

Finding 2: OIG is unable to determine if past SPD authorizations to collect protected information were in compliance with Seattle Municipal Code Chapter 14.12, as relevant records have been purged in accordance with the Chapter.

OIG determined that the SPD Intelligence Section is the only unit that reported a record of past written authorizations to collect information protected by Chapter 14.12. OIG saw no indication that the Section is currently out of compliance with the Chapter. However, OIG is unable to affirm whether the SPD Intelligence Section complied with the requirements of the Chapter for past authorizations, as the Intelligence Section purges records relating to written authorizations when the authorization expires and there is no legal hold on the material. OIG noted that a review of Intelligence Section practices and record-keeping procedures, as well as multiple interviews with staff, indicate that the Intelligence Section is knowledgeable regarding the requirements of the Chapter.

The City did not engage an outside auditor for over three years, resulting in an extended period without an independent audit of Chapter 14.12.

Chapter 14.12 requires that the Mayor shall appoint an auditor to audit SPD's compliance with the Chapter. However, the last audit released prior to the current report was dated 12/8/2015, indicating that a substantial time period has elapsed without audit oversight.[8]

8 As stated previously, Ordinance 125315 assigned this function to OIG in 2017. However, the first Inspector General was not appointed until 2018.

Additionally, the Chapter instructs SPD to submit a copy of every written authorization to the designated auditor, which allows the auditor to review authorizations before the relevant records are purged. However, SPD did not send copies of written authorizations to any oversight entity after the previous auditor retired. SPD management stated that no auditor was assigned to fulfill this function.

The Intelligence Section purges all records relating to expired authorizations.

Chapter records disposal requirements prevented OIG from assessing older documents.

Chapter 14.12 requires the Intelligence Section to purge protected information that is no longer relevant. Additionally, in certain circumstances, Chapter 14.12 requires protected material to be purged within sixty days of the expiration of the relevant authorization.[9] Intelligence Section staff confirmed to OIG that they review and purge expired records relating to expired authorizations on a regular basis.

Per the Intelligence Section staff analyst, when an authorization is issued, she creates a calendar appointment before its expiration date as a reminder to check the status and purge the records if appropriate. If the authorization expires and the information is not involved in an active court case, the information is physically shredded or deleted if in electronic form. If the information is involved in a court case, the staff analyst reported that she checks on the status no less than every two months and purges the information when the court case is complete. The Intelligence Section only retains a log with the authorization number – neither the authorization itself or the collected information are kept.

As a result, OIG could not review past authorizations issued since the last outside audit in 2015. The log indicated that nine authorizations were issued during the scope period. Only one authorization application was available for OIG to review. The Chapter requirements appeared to have been met, with the exception that the original authorization was extended on the approval of the Intelligence Section lieutenant. Per Chapter 14.12.170, the Chief of Police must sign off on extensions of authorization periods. The Intelligence Section recognized the oversight and sent the authorization to the Chief for review after discussing the issue with OIG.

Intelligence Section personnel are knowledgeable about the requirements of Chapter 14.12 and receive annual training on similar federal regulations.

OIG interviewed Intelligence Section staff on multiple occasions and conducted a physical walk-through of the area where protected information would be stored. Staff appeared familiar with the requirements of Chapter 14.12 regarding when written authorizations would be required, more so than any other staff in SPD that OIG interviewed. In particular, the staff analyst in charge of maintaining Intelligence Section records and other administrative functions appears to be well acquainted with the Chapter.

9 This only applies to protected information collected for the purposes of dignitary protection, which Intelligence Section personnel reported to be a very rare occurrence.

Additionally, staff asserted that activities in the Intelligence Section are governed by 28 CFR Part 23, Criminal Intelligence Systems Operating Policies. These regulations are designed to ensure that criminal intelligence systems operating with support from the federal government do not violate privacy and constitutional rights. Staff asserted that they receive annual training on 28 CFR Part 23. While detailed records do not exist for this training, OIG did review a 2019 calendar appointment indicating that training on 28 CFR Part 23 was on the agenda.

Several of the operating principles of 28 CFR Part 23 are similar to Chapter 14.12 (see Appendix), although the regulation does not protect information about an individual's sexual orientation. The major difference is that the federal regulation does not outline a comparable written authorization process to Chapter 14.12.

In summary, OIG finds no indication that the Section, and by extension SPD, is out of compliance in terms of past authorizations. However, OIG cannot affirm that SPD issued past authorizations in compliance with the Chapter because the relevant records were purged in an attempt to meet Chapter record-retention requirements.

Recommendation 2: The Chief of Police should ensure there is a procedure in place to notify OIG of all approved written authorizations to collect protected information.

Recommendation 3: The Chief of Police should ensure that SPD retains records relating to approved written authorizations for at least six months, to facilitate future audit reviews.

Finding 3: OIG examination of case records indicated compliance with Seattle Municipal Code Chapter 14.12, Collection of Information for Law Enforcement Purposes; however, OIG identified training gaps that create risk for future compliance.

OIG found that SPD case records complied with Chapter 14.12 for 98 percent of reviewed cases (288/295).[10] OIG observed that compliance exists not through adherence to the code, but rather the lack of activity that would trigger the need to collect information protected by Chapter 14.12.

SPD Policy 6.060, Collection of Information for Law Enforcement Purposes, omits the municipal code requirement to seek written authorization before collecting protected information.

SPD could not provide evidence of other training that would provide necessary education to staff. If staff are not aware of the need to obtain a written authorization, they may unwittingly violate Chapter 14.12 in the rare circumstances where protected information is relevant to a case.

10 As discussed in Finding 1, OIG was not able to confirm whether the remaining 2% of cases were in compliance due to the lack of clarity in Chapter 14.12.

Patrol officers appear to rarely encounter information that would require written authorization under Chapter 14.12 in the course of their operations.

OIG reviewed a random sample of bias crime case files to determine if protected information was collected by patrol officers without authorization.[11] Bias crimes are broadly described as crimes motivated by the perpetrator's belief about the protected status of another person, such as their race, gender, religion, or sexual orientation. OIG reasoned that, of the entire universe of SPD offense reports, bias crime incidents would have the highest risk (and likelihood) of containing protected information.

OIG reviewed a sample of bias crime cases to determine if SPD collected protected information without appropriate authorization.

OIG reviewed a random sample of 295 out of 1256 bias crime incidents that occurred between May 30, 2015, and November 1, 2018.[12] OIG found that in 98 percent of cases, the information collected by the responding officer and follow-up units (if applicable) either did not contain protected information or contained information that definitively did not require a written authorization.[13]

OIG also observed cases in which the suspect of the crime had departed the scene and was unknown to both the victim and the police. In these cases, the officer would be unable to collect protected information about the suspect.

In other cases, the circumstances of the crime do not require the officer to collect protected information. For example, if a suspect uses a racial or homophobic slur prior to assaulting the victim, the officer may not need to collect information about the suspect's own sexual identity, religious associations, or political associations prior to arresting them for a bias crime.

SPD officers are not provided with sufficient guidance on the requirement to obtain a written authorization before collecting information protected by Chapter 14.12.

SPD Policy 6.060, Collection of Information for Law Enforcement Purposes, cautions officers not to document or collect certain types of information protected by Chapter 14.12. The policy states that

"Any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose."

11 While SPD does have an appointed Bias Crimes Coordinator, as referenced earlier in this report, most of the reviewed reports were written by patrol officers who responded to the original incident. The Coordinator or other assigned detectives would complete supplemental reports if the reported case warranted further investigation. These reports were reviewed by OIG when present.
12 The sample size was selected to provide a 95% confidence level that the results reflect the underlying population.
13 For the latter, the most common example we observed was victims providing information about their own sexual orientation as an explanation of why they may have been targeted by a suspect. This type of information sharing does not require written authorization.

SPD policy omits the Chapter requirement to obtain written authorization.

However, the policy omits the requirement to obtain written authorization prior to collecting information about a person's political or religious activities, providing incomplete guidance. While Policy 6.060 encourages staff to review Chapter 14.12 itself, this is not a substitute for providing complete information to staff in the text of the policy.

OIG confirmed with SPD training staff that there are no trainings addressing the requirement to obtain a written authorization.

OIG did identify an older training document that described in great detail when a written authorization would be required. However, SPD staff confirmed that this training document had been retired for some time and had been superseded by Chapter 14.12 itself.

Recommendation 4: The Chief of Police should ensure that Policy 6.060, Collection of Information for Law Enforcement Purposes, includes all requirements of Chapter 14.12, being cognizant of any updates that are contemplated by the City, and ensure staff are updated on any changes or additions to the policy or Chapter.

Finding 4: Chapter 14.12 record retention requirements appear to conflict with state law, as well as existing SPD records retention policies.

The Chapter requires certain records to be purged within short time periods. However, that requirement appears to conflict with state requirements for retention of public records, as well as existing SPD record retention practices. Aligning SPD practices with Chapter 14.12 retention schedules would reduce SPD's ability to comply with public records requests and would limit available information sources for misconduct investigations. Additionally, the records retention requirements of Chapter 14.12 are internally inconsistent, as described below, which may create confusion for both SPD employees and members of the public seeking to access the relevant information.

SPD permanently retains all body-worn video and case files.

SPD has a directive instructing department personnel to permanently retain all records until further notice. OIG confirmed this retention schedule is still in effect and that SPD is permanently retaining all body-worn video at the time of this report. SPD instituted the practice to ensure the department retains records that would be relevant to the consent decree and subsequent monitoring. Additionally, state law requires SPD to retain body-worn video for a minimum of sixty days.[14]

The Chapter requires protected information obtained without authorization to be purged in a matter of days, as discussed in more detail below. As they relate to body-worn video, these requirements conflict with the permanent records retention policy of SPD and the sixty day period required by state law.

14 See RCW 42.56.240.14.j: "A law enforcement or corrections agency must retain body worn camera recordings for at least sixty days and thereafter may destroy the records in accordance with the applicable records retention schedule."

Chapter 14.12 was written before the advent of body-worn video technology and thus does not provide guidance on its use.

For example, SPD officers activate body-worn cameras during demonstrations when they are taking law enforcement action relating to observed criminal activity. It is conceivable that doing so may capture information about the religious or political affiliations of people taking part in the demonstration, particularly those who act as witnesses and provide their names. SPD suggested to OIG that individuals on the street do not have a reasonable expectation of privacy, but Chapter 14.12 does not explicitly reference such an exception. However, it cannot be over-emphasized that the Chapter was written well before the advent of body-worn video technology and does not provide for the use of technology in modern investigative practices.

OIG acknowledges that if SPD were to delete body-worn video or case records after five days, or one of the other schedules outlined in Chapter 14.12, SPD may be in violation of state law. Additionally, SPD may be unable to meet public expectations regarding records requests or have insufficient information to investigate a complaint of misconduct or a reported crime.

Chapter 14.12 is internally inconsistent regarding record retention requirements.

Chapter 14.12 does not contain consistent guidance regarding record retention relating to protected information. For example, personnel are required to purge private sexual information that does not meet Chapter 14.12 collection requirements within seven working days, but have just five working days to purge restricted information collected without a written authorization – and only 24 hours to purge restricted information collected without a written authorization for the purposes of dignitary protection.[15]

The variety of retention requirements does not follow a logical pattern and may be difficult for staff to remember and enforce.

Recommendation 5: The Chief of Police and the City Attorney's Office should work together to review Chapter 14.12 in light of current records retention needs, and modify either the Chapter or SPD policy as appropriate.

15 If personnel are able to obtain a written authorization after the fact, they may retain the information.

Recommendations

1. The Chief of Police, in consultation with the City Attorney's Office, should develop a clear policy for whether written authorization is required prior to collecting protected information from open sources or third parties. If necessary, the Chief of Police should offer suggestions to the City regarding changes to Chapter 14.12 that would provide the required clarity.

Management Response

☑ Concur ☐ Do Not Concur

The Department concurs that Chapter 14.12's outdated and confusing language makes it difficult to apply in the context of modern technology. The Chief of Police further concurs that there is a need for clear policy for whether written authorization is required prior to collecting protected information from open sources or third parties. Given the extent of inconsistency of current provisions with present-day reality, the Department will consult with the City Attorney's Office to ensure that its practices meet the legal framework under both local and state law, while continuing to comply with the intent of the Ordinance.

Proposed Implementation Plan

SPD Legal and Intel Units will consult with assigned staff in the City Attorney's Office to create written protocol to clarify the current application of the Ordinance in light of the issues noted in the audit.

Estimated Date of Implementation: Q3 2019

---

2. The Chief of Police should ensure there is a procedure in place to notify OIG of all approved written authorizations to collect protected information.

Management Response

☑ Concur ☐ Do Not Concur

The three year-gap since the last audit hindered OIG's ability to review records relating to expired authorizations because those records were purged within sixty days of expiration as the Chapter mandates. OIG found no indication that SPD is out of compliance in terms of past authorizations, but was unable to affirm that SPD issued past authorizations in compliance with the Chapter because the relevant records were purged to meet Chapter's record-retention requirements. The Department agrees that implementing a procedure to notify OIG of all approved written authorizations to collect protected information would facilitate future audit reviews.

Proposed Implementation Plan

SPD Legal and Intel Units will coordinate with the Audit, Policy, and Research Section and the OIG to establish a protocol to notify the OIG of all approved written authorizations to collected protected information.

Estimated Date of Implementation: Q3 2019

Recommendations

3. The Chief of Police should ensure that SPD retains records relating to approved written authorizations for at least six months, to facilitate future audit reviews.

Management Response

☑ Concur ☐ Do Not Concur

Again, the three year-gap since the last audit hindered OIG's ability to review records relating to expired authorizations because those records were purged within sixty days of expiration as the Chapter mandates. The Department agrees that retaining records relating to approved written authorizations for at least six months would facilitate future audit reviews and will consult with the City Attorney's Office to ensure that its records retention protocols meet legal requirements.

Proposed Implementation Plan

Recognizing the conflict between the recommendation and the ordinance mandate with respect to records retention, SPD Legal, Intel, and Public Disclosure Units will consult with the City Attorney's Office to create written protocol to ensure that its records retention protocols meet legal requirements.

Estimated Date of Implementation: Q3 2019

---

4. The Chief of Police should ensure that Policy 6.060, Collection of Information for Law Enforcement Purposes, includes all requirements of Chapter 14.12, being cognizant of any updates that are contemplated by the City, and ensure staff are updated on any changes or additions to the policy or Chapter.

Management Response

☑ Concur ☐ Do Not Concur

The Department agrees that Policy 6.060, Collection of Information for Law Enforcement Purposes, should more fully reflect the requirements of Chapter 14.12, as currently written and as may be updated in the future, with appropriate staff notification of any changes or additions to the policy or Chapter.

Proposed Implementation Plan

SPD Legal and Intel Units will coordinate with the Audit, Policy and Research Section to establish alignment between Policy 6.060, the Ordinance, and updated protocol developed in consultation with the City Attorney's Office, as referenced in Response to Recommendation 1, above.

Estimated Date of Implementation: Q4 2019

Recommendations

5. The Chief of Police, in consultation with the City Attorney's Office, should review Chapter 14.12, SPD policy, and state law in light of current records retention needs. The Chief of Police should either modify SPD policy or offer suggestions to the City regarding revisions to the retention provisions of Chapter 14.12 to bring SPD records retention into alignment with applicable laws.

Management Response

☑ Concur ☐ Do Not Concur

The Department agrees that Chapter 14.12's retention requirements do not follow a logical pattern and are difficult for staff to remember and enforce. The Chapter's standards also conflict with State law and retention schedules established by the Washington State Archives as mandated by Chapter 40.14 RCW.

Proposed Implementation Plan

The Department will work with the City Attorney's Office to review Chapter 14.12 in light of current records retention requirements, and modify SPD policy accordingly.

Estimated Date of Implementation: Q3 2019

MANAGEMENT RESPONSE

City of Seattle
Seattle Police Department

June 7, 2019

Inspector General Lisa Judge
Office of the Inspector General

Re: Chapter 14.12 Compliance Audit

Dear Inspector General Judge:

While the Seattle Police Department's specific responses to the recommendations set forth in your audit concerning SPD's compliance with the City's Intelligence Ordinance, SMC Chapter 14.12, are presented within the audit document itself, I am taking this opportunity to provide additional comments on both the audit content and recommendations.

I want to first thank you for the professionalism of your auditors and the transparency of their process and review standards. As confidence in the legitimacy of process is so critical to building and maintaining reciprocal trust, I continue to be impressed by the clarity with which your auditors set forth their scope of review, the review standards applied, and the bases for audit outcomes. While concurring in full with the concerns noted, I take tremendous pride in your finding that, notwithstanding complexities, your office did not detect any violations of the Ordinance by SPD personnel.

Second, I appreciate that your audit highlights a frustration that SPD has long noted: that the outdated language of the Ordinance, combined with the vacancy in the city-appointed Intelligence Auditor position, has led to significant ambiguity around processes for the collection of information through media that were nonexistent and unforeseen at the time the Ordinance was enacted. Of additional concern is the direct conflict between the Ordinance and other provisions of state law under which SPD must operate, as well as the conflict between restrictions of the Ordinance and explicit mandates to SPD with respect to certain criminal investigations (as you note, for example, investigation of bias/hate crimes often *requires* SPD to collect, as elements of the crime, victim information that the Ordinance explicitly restricts). I hope that our responses to your recommendations in these respects, as set forth in the audit report itself, provide a solid path for moving forward to resolve these issues.

I also want to be forthright in acknowledging that this audit falls at a time when the rapid rise of big data and the dizzying growth in technological capacity have generated understandable concerns about the potential for government encroachment into private and

Seattle Police Department, 610 Fifth Avenue, PO Box 34986, Seattle, WA 98124-4986

constitutionally-protected affairs. Recognizing the heightened scrutiny around SPD intelligence gathering and the critical importance of transparency of practice and accountability to policy, I welcome the recommendations that the Department work with the City Attorney's Office to ensure that our practices comply with our legal responsibility under both state and local law in light of present day challenges and changed circumstances over the 40 years since the Ordinance was adopted. In doing so, however, we must not lose sight of the overarching statement of purpose articulated in Section 14.12.020: that at all times the Ordinance is to be interpreted in a manner that permits the collection and recording of information consistent with First Amendment and privacy limitations; and that the ordinance is not intended to protect criminal activity.

Again, thank you for the thorough, thoughtful, transparent and collaborative manner in which your auditors undertook this review. As always, please do not hesitate to reach out if you would like to discuss further.

Sincerely,

Carmen Best
Chief of Police

Cc: Marc Garth Green, Deputy Chief
Deanna Nollette, Assistant Chief, Investigations
Lesley Cordner, Assistant Chief, Professional Standards
Rebecca Boatright, Executive Director, Legal Affairs

Objective

The audit team sought to determine whether SPD was complying with applicable regulations for the collection of private sexual information and restricted information, per the requirements outlined in Seattle Municipal Code Chapter 14.12.

Scope

The audit scope covered activities and authorizations conducted between 5/30/2015 and 11/1/2018, based on the date of the last intelligence audit.

Methodology

To answer the audit objective, the audit team:

- Analyzed Chapter 14.12, *Collection of Information for Law Enforcement Purposes*, to determine the various requirements and processes for collecting, storing, receiving, and transmitting information protected by the Chapter;
- Reviewed SPD Policy 6.060, *Collection of Information for Law Enforcement Purposes*, to determine alignment with Chapter 14.12, and requested any available training documentation;
- Evaluated prior audit reports to identify any past issues and trends;
- Interviewed SPD personnel, including Intelligence Section personnel, the Director of Transparency and Privacy, the SPD Chief Legal Officer, and other relevant staff;
- Conducted physical walk-through of SPD Intelligence Section, including location of files relating to Chapter 14.12 authorizations;
- Analyzed documentation for the sole active authorization for compliance with Chapter 14.12;
- Developed a random sample of 295 bias crime cases and reviewed available documentation, include general offense reports and follow up investigations;
- Determined that there are no relevant officer misconduct investigations involving violations of Policy 6.060 within the scope period;
- Confirmed current SPD records retention policy and compared this policy to the requirements outlined by Chapter 14.12; and
- Consulted with the City Attorney's Office regarding OIG understanding of Chapter 14.12.

Audit Standards

OIG conducted this performance audit in accordance with generally accepted government auditing standards. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Seattle Office of Inspector General

The Office of Inspector General for Public Safety (OIG) was established in 2017 via Ordinance 125315. OIG provides oversight of management, practices, and policies of the Seattle Police Department (SPD) and Office of Police Accountability (OPA), monitoring of ongoing fidelity to organizational reforms implemented pursuant to the goals of the 2012 Federal Consent Decree and Memorandum of Understanding, and auditing and review of criminal justice system policies and practices related to policing and other criminal justice matters.

OIG is empowered to help ensure the fairness and integrity of the delivery of law enforcement services and the investigation of allegations of police misconduct. OIG makes systemic recommendations for lasting reform that are intended to reflect the values of Seattle's diverse communities.

Audit Team

Mary Dory, Auditor in Charge

Matt Miller, Auditor

Inspector General

Lisa Judge

Deputy Inspector General

Amy Tsai

Office of Inspector General

web: http://www.seattle.gov/oig/

phone: 206.684.3663

email: oig@seattle.gov