Colorado Springs Police Department
General Order

1074 Reporting Suspicious Activity or Terrorist Information

Section 1000 – Patrol Functions

Effective Date: 1/28/2020
Supersedes Date: 5/30/2019

.01 Purpose

The purpose of this directive is to establish procedures for handling information related to suspicious activity, organized crime, terrorism, and other threats to public safety.

.02 Cross-Reference

GO 701 First Amendment Rights
GO 885 Operation of the Strategic Information Center
GO 1303 Fair and Impartial Policing
GO 1551 Recording of Police Activity
SOP M1-29 Intelligence Files and Information
28 CFR, Part 23

.03 Discussion

Law enforcement employees fill a critical position in the area of threat identification, including terrorism. In support of this, the Colorado Springs Police Department (CSPD) seeks to gather, analyze, investigate, and disseminate information and observations that are either criminal or suspicious in nature, which may prove critical to the information/intelligence cycle.

All department members have an important role in the information/intelligence cycle. Department members contribute to the critical role of information gathering, through vigilance in their day-to-day activities. The duty to report is everyone's responsibility.

.04 Policy

It is the policy of the CSPD to accurately and appropriately gather, analyze, and record information of a criminal or non-criminal nature that indicates activity or intentions associated with foreign or domestic terrorism, and any other threat to public safety and homeland security. This investigative/administrative process will be conducted in a manner that protects the information and privacy rights of American citizens and in compliance with existing federal,

state, and department guidelines, rules, and regulations.

- Department members are required to complete the appropriate documentation of observed or reported suspicious activity and/or persons in a timely manner.

- Department members should only reference information from StIC products or any other information/intelligence report or source if that information was used to support probable cause in search or arrest warrants, or other critical case documentation.

- Department members are required to notify StIC immediately of certain suspicious activity (listed in section .30).

Department members will not communicate criminal intelligence information via email.

.05 Definitions

Strategic Information Center: The unit responsible for the collection of information that when analyzed, produces intelligence for operational, tactical, and strategic purposes. This unit is comprised of intelligence detectives and crime analysts under the Metro Vice, Narcotics, and Intelligence (Metro VNI) Division.

Suspicious Activity: Suspicious activity is any event or act that would lead a reasonable person to believe that the circumstance in question may be associated with criminal activity or behavior.

Suspicious Person: A suspicious person(s) is the individual (s) involved in the event or act of suspicious activity.

Intelligence Cycle: The intelligence cycle is the process of developing raw information into finished intelligence to use in decision-making and action. There are six steps, which constitute the intelligence cycle: planning, direction, collection, processing, analysis, and dissemination.

.10 Recognition of Suspicious Activity

Identifying suspicious activity or persons is not an exact science. One must rely on experience, judgment, and common sense to recognize suspicious activity. Suspicious activity may be determined through a member's personal observations, during the course of their day-to-day activities. Department members are expected to identify such activity or persons in a manner consistent with GO 1303 Fair and Impartial Policing.

.20 Reporting Suspicious Activity

All department members are responsible for directing all information that may be considered developing criminal or threat information to the StIC.

Members of the Colorado Springs Police Department will document observed or reported instances of suspicious activity and/or persons utilizing the CSPD "Information Report" which can be found by going to the CSPD Intranet site (***REDACTED***).

If a member chooses to complete a paper report, the report is submitted via the inter-office mail system, addressed to the Metro VNI Division to the attention of the Strategic Information Center. *This method should only be used when timeliness of the information being received by the StIC is* ***not*** *critical.*

Members completing a criminal case or incident report that they believe contains information or activity that should be reviewed by the StIC will notify the StIC lieutenant or sergeant of the specific report number so that the information can be reviewed. Members may alternatively provide a synopsis of a case report on an information report.

Department members may also notify StIC of information or alerts by contacting a StIC detective by phone, in person, or through the use of (***REDACTED***).

E-mail may **only** be used to notify StIC that the department member has information to be shared.

E-mail should **never** be used to convey criminal intelligence information, vetting of information or otherwise.

Department members are cautioned from including sensitive information in a standard police report that is unrelated to the criminal investigation. In this situation, officers will refrain from referencing any information or intelligence report or source within any publicly accessible document, or make a reference to "intelligence information" within the narrative portion of such documents.

Additionally, officers and detectives will refrain from referencing StIC products such as "(***REDACTED***)," "(***REDACTED***)," "(***REDACTED***)," and "(***REDACTED***)" in case reports or supplements. However, if the information from a StIC product was used to support probable cause in search or arrest warrants or other critical case documentation, officers will include the information in those reports.

.30 Notifications

Some reported instances of suspicious activity will require immediate notification of StIC personnel.

StIC personnel are to be notified without delay under the following reported or observed circumstances:

- All threats or suspicious activity concerning national defense or national security.
- All threats involving public officials.
- All threats or suspicious activity associated with the disruption of local, county, state or federal government services.
- All threats, security breaches or other suspicious activity involving local, county, state, or federal infrastructure and/or facilities.
- All threats associated against any political or religious group.
- All threats associated with educational facilities, schools and other quasi-governmental institutions
- Any surveillance, photography, filming, sketching, measuring, or note taking in or around local, county, state, federal infrastructure, or facility. *This does not indicate that the taking of photographs, videos or other similar activity of such buildings is illegal or constitutes criminal activity. Department members must follow the requirements of GO 701 First Amendment Rights and GO 1551 Recording of Police Activity in these situations.*
- Any attempt to breach or enter secured/sensitive areas of any local, county, state, federal infrastructure, or any other facility associated with the Department of Defense.
- Theft, purchases, attempted purchases or being in the possession of large amounts of fuel, fertilizer or any other potential explosive materials when no authorization can be determined.
- Thefts of, or being in the possession of (when not so employed) any official or service related uniforms, equipment, or vehicles (e.g., police, EMT, delivery, military, etc.)
- Impersonation of any government, service, or delivery person.
- Instances of organized gambling.
- All information regarding visiting dignitaries (e.g., public and military).
- All contacts with visiting dignitaries (e.g., public and military).
- Information on upcoming events or actions that may cause a public safety concern (e.g., planned protest, controversial speakers, groups or musical bands, large sporting events).
- All contacts with members from any extremist organizations or groups (e.g., sovereigns, militia or anti-government, hate, environmental or animal activist groups).

- Investigations involving graffiti associated with any extremist, anarchist, hate, environmental or animal activist groups.
- Contacts with identified outlaw motorcycle gang members involved in criminal activity.
- Contacts with habitual criminals who pose a community threat.
- Contacts with suspicious foreign persons.
- Investigations associated with the manufacture and/or selling of illegal firearms or explosives.
- Investigations involving the placement or use of any explosive device designed to cause structural damage, physical harm, or test the explosive yield of the device.
- Suspicious documents, notes, blueprints, diagrams, photos, film or other materials discovered that may not be attributable to the employment, social status, security clearance or hobby of the holder.

Detectives are available after hours. After hours contact must have the prior approval of a supervisor. Circumstances will determine whether the response of a MVNI detective from the Intelligence Unit is necessary.

.40 Routing and Distribution

Information Reports are routed directly to the StIC intelligence supervisor. Upon receipt, the supervisor reviews the report and makes a determination whether further investigation is warranted. The intelligence supervisor assigns the report for an investigation, closes the report with no further action, or redirects it to another responsible agency, internal unit, or person for action as deemed appropriate.

.50 Results and Return

All information received by the StIC will be reviewed for its content and applicability in the interest of public safety. When appropriate, the submitting source will be notified of the outcome of any investigated information. Often, initiating information is developed into other documents that are distributed to staff officers for internal distribution, posted on ETACS, the Colorado Information and Analysis Center, or within the Rocky Mountain Information Network.