Colorado Springs Police Department
Standard Operating Procedure

DL-1074-01 Strategic Information Center Operations

Section 1000 – Patrol Functions

Effective Date: 10/11/2021
Supersedes Date: 7/29/2020

.01 Purpose

The purpose of this directive is to establish procedures for the operations of the Strategic Information Center (StIC) and to describe the proper use of StIC products.

.02 Cross Reference

GO 104 Determining Probable Cause
GO 1074 Reporting of Suspicious Activity or Terrorist Information

.03 Definitions

Intelligence Led Policing (ILP): A proactive policing concept designed to disrupt, reduce, and prevent crime, utilizing data-driven intelligence formed through the collection and analysis of information, to strategically place resources to target crime hot spots, repeat victims, prolific offenders, and criminal groups.

.04 Procedure

The Colorado Springs Police Department (CSPD) uses ILP to effectively and efficiently deploy resources in a manner that best prevents, disrupts, and responds to a dynamic criminal and threat environment.

Through tactical and strategic analysis, decision-makers can better understand both current and future criminal activity, trends, patterns, and the impact on the community. ILP provides information so that decision-makers can utilize it as a guide to reallocate resources to address criminal activity or threats on a proactive, rather than reactive basis.

Organizational Structure

An assigned Metro Vice, Narcotics, and Intelligence Division (MVNI) Lieutenant has overall responsibility for the supervision of the intelligence and analytical functions within StIC as directed by the MVNI Commander.

Intelligence detectives and analytical staff are assigned to the StIC. The StIC serves as the information collection center for criminal and threat information, analysis, and dissemination. An analytical supervisor supervises the analytical staff and analysts may be assigned to work outside of the physical location of StIC, to provide direct support that meets an operational need, if overall StIC operations are not compromised.

In addition to the standards established for assignment in MVNI, StIC personnel are also bound by a non-disclosure agreement concerning operational activities, information, and/or intelligence from any source in the performance of their duties.

Responsibilities

StIC will be responsible for the following:

- Threat assessments
- Investigation of threats against public employees, elected officials, or others
- Investigation of threat groups or persons
- Repeat offender program
- Information/intelligence collection, analysis, and dissemination
- Identification and analysis of crime patterns involving people and/or places
- Analysis of criminal activity for commonality and strategic interdiction
- Deconfliction
- Gang related analysis and classification
- Provide liaison and support for federal partner agencies and joint task forces
- Investigative case support as requested (case enhancement)
- Primary information facilitator and liaison for Suspicious Activity Reporting suspicious activity reporting reference Homeland Security activities
- Primary liaison to the Colorado Information Analysis Center (CIAC)
- Responsible for representation of CSPD in various intelligence sharing communities and organizations

Reports & Documents

StIC produces documents under the following four categories: Strategic, Operational, Tactical, and Administrative.

- Strategic Products - support long range planning, or may focus on a single emerging topic within the criminal environment. Example: Products are future oriented and proactive. Trend reports and projections fall into this category. Data is evaluated toward gaining insight and understanding of trends in criminal behavior and the functioning of the criminal environment.

- Operational Products – are broader in scope and are geared toward understanding how resources can be allocated. These products support area commanders and managers in planning crime reduction activity and deploying resources to achieve operational objectives. Example: Products that evaluate call volumes by area, arrival times, and time spent on calls.

- Tactical Products – are narrower in scope and support short range planning. These products provide information and recommendations to aid in addressing specific and immediate needs. Example*:* Tactical products may provide information concerning a planned protest, an identified crime pattern, BOLO, request for information, etc.

- Administrative Products - are categorized as any material produced that doesn't meet the criteria of the other types and is simply crime related data. Example: may include such things as gathering statistics for a geographical area for use in a presentation that provides support to grant applications, community relations, or feasibility studies.

Reporting and Sharing of Information/Intelligence

Department members have the responsibility to direct appropriate information to StIC.

Analysis & Validation

It shall be the responsibility of StIC, through analysis and research, to determine the validity and nature of submitted raw information. StIC detectives will conduct the necessary investigation to determine the validity of the information. Information that is determined to be credible and actionable will be disseminated to the appropriate investigative entity. Prior to the dissemination, the information may receive enhancements and include such things as investigative insight, case supplements, unclassified background material, etc. Information regarding threats against public officials, infrastructure, or dignitaries will be investigated by StIC.

Information Dissemination

StIC will disseminate analytical and investigative results to affected operational units in a timely and efficient manner as well as disseminate information in various bulletins and reports. Information contained within disseminated documents from the StIC will be classified in order to protect sources, investigations, and an individual's right to privacy. The Strategic Information Center will utilize a document classification system similar to that of the Law Enforcement Intelligence Unit association.

Use of the StIC page(s) within the CSPD Intranet will be the primary information dissemination portal. Members can navigate to the StIC web page within the CSPD Intranet to discover recent alerts, bulletins, reports, maps, and resources.

Request for Products

Due to the variety and complexity of analytical products that are produced on a regular basis, a request for additional products is made through the StIC web page on the CSPD Intranet, contacting the StIC Lieutenant, or the analytical supervisor. This creates an administrative process to facilitate the proper prioritization of the request so that timelines can be determined for the creation of the product and/or the information to be gathered and interpreted.

Use of Disseminated Information

Information developed within the StIC is for the purpose of advancing legitimate public safety and law enforcement objectives among CSPD personnel and our law enforcement partners. Unauthorized access or disclosure of products developed within the StIC is prohibited. Questions related to the release of documents should be directed to the StIC lieutenant or the StIC Analytical Supervisor. With the exception of unclassified information, all other products must always be destroyed so they cannot be recovered.

Dissemination can be at several levels of the organization, which can be tailored to meet legitimate needs. Dissemination of intelligence and information products is limited to those that have both the need to know and the right to know in the performance of a law enforcement activity.

To protect the constitutional and privacy rights of all persons, information/intelligence that is disseminated will be properly formatted, classified, reviewed, and approved for dissemination following the guidelines established by federal, state and local law, rules and regulations.

Information disseminated from StIC may or may not constitute reasonable suspicion or probable cause to arrest. Despite the information received from StIC, it always remains the individual department member’s responsibility to make reasonable suspicion or probable cause

determinations based upon the knowledge, situation, and other information available to them at that time.

The information may be used to further develop investigative efforts to establish probable cause, to develop further investigative strategies or to assist in developing a response plan. Suggestions may be included with the disseminated information regarding developing community partnerships to assist in dealing with an issue or area, further follow-up processes and investigative methods and steps, or requests for information.