



Alexandria Police Department
Directive 10.2



INTELLIGENCE

Effective Date: 04-13-2010	 Cancels: 08-04-2009
Updated Date: 04-12-2013	Section(s): 10.2.08
Updated Date: 01-21-2020	Section(s): Updated FCI references
Updated Date:	Section(s):
	SME Review Date: 2023

CONTENTS

- 10.2.01 PURPOSE AND POLICY
- 10.2.02 GENERAL
- 10.2.03 DEFINITIONS
- 10.2.04 RESPONSIBILITIES
- 10.2.05 REPORTING
- 10.2.06 HANDLING OF INFORMATION
- 10.2.07 SURVEILLANCE CAPABILITY
- 10.2.08 TRAINING

10.2.01 PURPOSE AND POLICY

The purpose of this directive is to identify the intelligence gathering responsibilities and functions within this agency.

It is the policy of this Department to develop, accept, and analyze intelligence information on criminal conduct or any matter that may threaten the welfare and public safety of our citizens.

10.2.02 GENERAL [40.2.1]

Police by nature tend to approach all things with an apprehension/prosecution state of mind. The intelligence function is not designed specifically for that purpose, although it can end up with that result.

Since its inception, this Department has, through the Investigations Division, collected traditional criminal intelligence information to aid in forecasting where potential threats to the community might arise.

A sound guiding principle in the collection of criminal intelligence is: “to ensure civil rights; investigative techniques shall be lawful and only as intrusive as necessary to gather sufficient information to prevent the criminal act and/or identify and prosecute violators.”

Code of Virginia § 15.2-1722, states it shall be the duty of the sheriff or chief of police of every locality to insure [sic], in addition to other records required by law, the maintenance of adequate personnel, arrest, investigative, reportable incidents, and non-criminal incidents records necessary for the efficient operation of a law-enforcement agency.

After September 11, 2001, this agency found it necessary to create a formal counter-terrorism intelligence unit, to face the changing needs. The Office of Homeland Security and Operational Preparedness reported directly to the Chief of Police and its primary focus was toward domestic and international terrorism. It is now the *Financial Crimes and Intelligence Unit*, within the *Investigations* Division.

Legal Considerations:

While intelligence plays a key role in law enforcement operations, it can also be the instrument of abuse if such operations are not properly organized, focused, and directed. Accordingly, care must be taken to ensure that aggressive enforcement and intelligence gathering do not become incursions upon a person's rights as delineated in the United States Constitution. Guidance may be found in PD 10.30, Search Warrants, and PD 10.37, Warrantless Searches. Aggressive intelligence gathering must not become a fishing expedition to garner sensitive or confidential information on individuals for whom there is no reasonable suspicion of criminal activity. Targeting people is unlawful without some evidence of criminal behavior:

- If the reason for the target is the support of an unpopular cause, it is unlawful.
- If they are being targeted because of their political beliefs, religion, race, ethnicity, or other attribute or characteristic, it is inherently unlawful, i.e., people who are perceived to be Muslim. Refer also to PD 2.4, Non-Biased Policing.
- Targeting without lawful justification can result in civil rights suits and vicarious liability lawsuits, which can be both costly and embarrassing to the Police Department. Officers are reminded that if while acting under the color of state law, they violate the civil rights of a person, the officer and his or her chain of command may be sued in federal court under 42 USC 1983, Civil Action for Deprivation of Civil Rights.

Monitoring an individual's behavior is proper if reasons can be articulated that reasonably support the belief that:

- The person may be involved in criminality now or in the future.
- There is a reasonable belief of a threat to public safety.

The U.S. Code of Federal Regulations: 28 CFR 23.3(b)(3) states that criminal intelligence information that can be put into a criminal intelligence sharing system is “information relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and meets criminal intelligence system submission criteria.” Further, 28 CFR 23.20(a) states that a system shall only collect information on an individual if “there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity. [40.2.2]

Information obtained or collected in violation of any applicable Federal, State, or local law or ordinance is prohibited. [40.2.1]

10.2.03 DEFINITIONS

Intelligence Process: The collection, analysis, creation, dissemination and application of information and knowledge for the protection of the security interests of the government and the general citizenry.

Terrorism: There is no single, universally accepted, definition of terrorism. Terrorism is often defined as the deliberate creation and exploitation of fear in pursuit of political or social change through the threat or use of violence. Any such act is designed to have far-reaching psychological effect beyond the immediate attack and is meant to instill fear in a wider audience. Through the publicity generated by their violence, terrorists seek to gain leverage, influence, and power to affect their desired change.

Code of Virginia § 18.2-46.4 defines the "Act of terrorism" as an act of violence committed with the intent to (i) intimidate the civilian population at large; or (ii) influence the conduct or activities of the government of the United States, a state, or locality through intimidation.

Domestic Terrorism: The unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or its territories without foreign direction, committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

International Terrorism: Violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. The acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

Traditional Criminal Intelligence: Information that relates to criminal activity in crimes against persons, property, narcotics, or to gangs, and does *not* directly relate to domestic or international terrorism.

Law Enforcement Only: Commonly used qualifier that the information is not to be released outside of recognized law enforcement agencies.

No Secondary Release: A designation that the information is not to be further released beyond this Department, except by the originator.

10.2.04 RESPONSIBILITIES

[40.2.3 a&b]

Every employee of this Department is responsible for developing, gathering, and relaying potential intelligence information to the appropriate unit. [40.2.1]

Financial Crimes and Intelligence Unit

The *Financial Crimes and Intelligence Unit (FCI)* has the primary role of developing, accepting, analyzing, and distributing domestic/international terrorism and public security intelligence information for this agency. If it becomes aware of intelligence information that requires further investigation, and unit resources are not sufficient, the information will be passed on to either another Department unit or an appropriate federal agency for follow up. If it becomes privy to traditional criminal, gang and/or narcotics intelligence information, it will be passed on to the appropriate unit for further development. [40.2.1] [40.2.2] [40.2.3c]

The *FCI Unit* will assess potential targets of opportunity, both of infrastructure and persons of importance, existing in or visiting the City of Alexandria. In addition, they will consult with other City agencies on matters that relate to the security of the City. *FCI* will perform its function in areas related to special events and potential local or area-wide domestic unrest. It will also be the Department's rumor control point. Any employee, who receives or learns of information regarding terrorism issues, should broach them with *FCI* members for confirmation of validity. [40.2.1]

The *FCI Unit* will maintain liaison contacts with other local, state, and federal intelligence function units. In addition, it will have one of its members attached to the FBI's Joint Terrorism Task Force. Any contact with any local, state and federal agencies in reference to domestic or international terrorism must be made through the *FCI Unit*. [40.2.1]

Investigations Division

The Investigations Division will continue to pursue its own handling of traditional criminal, gang and narcotics intelligence information. It will maintain liaison contacts with other local, state, and federal agencies involved in criminal, narcotics, and/or gang intelligence. If the Investigations Division becomes privy to domestic/international terrorism or public security intelligence information, it will be passed on to the *FCI Unit*

for further development. It will maintain members on joint task forces as deemed appropriate by this Department. The Investigations Division will retain oversight of the Hate Crimes function. If a potential Hate Crime has domestic or international terrorism overtones, a cooperative decision will be made as to which unit will pursue the case.

[40.2.3, c]

10.2.05 REPORTING

Employees obtaining intelligence information that is possibly related to terrorism will promptly review it with their supervisors. It is important that the developing employee does a thorough job and obtains as much information as possible. The supervisor should then initiate contact with a member of the **FCI** Unit for guidance on how to proceed. In most cases the employee will be asked to create a police information report. This is important to document and track the information. If circumstances dictate the need for a member of the **FCI** Unit to respond, they will do so. [40.2.3,b,c]

Information related to traditional criminal, gang and narcotics intelligence will be handled in the same manner and be directed toward the appropriate Investigations Division supervisor.

The Investigations *Division* commander and the *FCI Unit* commander will in person, as necessary, brief the Chief of Police on any significant intelligence information developed and what subsequent actions were taken as a result. Procedurally, e-mail should be avoided on any sensitive information.

10.2.06 HANDLING OF INFORMATION

A. Information Distribution:

Intelligence information is of no use if it is developed and then not acted upon. This does not mean that all intelligence information is released to all persons. In the majority of occasions intelligence information will be widely distributed, in some cases it will not. This is guided entirely by a specific operational need to know. However, any information that is possessed by this Department that is deemed to be critical to an officer's safety will be released so as to mitigate any such threat. [40.2.3,c]

B. Information Security:

Information Security is the responsibility of everyone. If you possess information that is not supposed to be passed on, do not pass it on. If you were given an intelligence document and you no longer need it, do not simply discard it; destroy it (shredding is preferred). Employees should also be diligent of information security in their radio and cell phone transmissions. [40.2.3,b]

The most common distribution points for intelligence will be via the MDB Intelligence page and Roll Call notices. If general distribution is to occur, the information will be put on the MDB Intelligence page and hardcopy versions will be provided to *the Field Operations* Bureau's *Assistant* Chief *and the Administrative Bureau's Assistant Director* for distribution. The MDB Intelligence page is an inside the Department only access page.

Any such distributions will be on a Law Enforcement Only basis and are not to be passed on, in any format, outside the law enforcement community. On some occasions, the distribution will be on a No Secondary Release basis and is not to be released outside this Department, including other law enforcement agencies. [40.2.3,c]

C. Information Protection/Retention:

The *FCI Unit*, Investigations Division and the Vice Narcotics Section will each keep their intelligence information secure from unauthorized access. The information will be physically stored in such a manner as to ensure that only those needing access will have it available. This may involve coded access cards, physical locks and or passwords. Each involved unit, the Vice Narcotics *Section* and the *FCI Unit*, will assign a person who will be responsible for:

1. Retention and protection of intelligence information files.
2. Recommending reclassifying and purging of information in their respective intelligence files on an ongoing basis.
3. Reviewing records more than five years old to determine if they are still relevant or if they should be destroyed by shredding or some other appropriate method.
4. Obtaining permission from their commanders before any record destruction.
5. Retaining documentation of any relevancy review and related destruction of records and forwarding a copy of such documentation to *the Audits, Accreditation and Directives Section*. [40.2.3,d]
6. The Commander of the Investigations Division will conduct an annual review of Department procedures and process used in the gathering of intelligence information to ensure all legal and privacy requirements are being met. To include:
 - a. Is the Department seeking ways to enhance intelligence sharing efforts and foster information sharing by participating in task forces and state, regional, and federal information sharing initiatives;

- b. Have individuals' privacy and constitutional rights been considered at all times;
- c. Has there been compliance with Department policies and procedures;
- d. Have there been Internal *or external* complaints related to intelligence gathering and this directive; and
- e. Obtaining feedback on the process performed and the products produced by the intelligence function. (This step allows evaluation of performance or effectiveness.) [40.2.3,e]

10.2.07 SURVEILLANCE CAPABILITY

Several Department units have surveillance capabilities. A cooperative relationship will be maintained if a unit has a bonafide need for surveillance resources. This can either be the need for personnel or specialized equipment. Whoever is managing the surveillance operation will have oversight of the personnel involved. However, any specialized equipment utilized will remain in the possession of and under the control of the owning unit's trained operator. Requests for specialized surveillance needs will be arranged through direct contact of the commanders of the units involved.

10.2.08 TRAINING

Training of all personnel in the collection, processing, and sharing of suspicious incidents and criminal intelligence relating to criminal and homeland security activities will be conducted in keeping with Department procedures for each new or updated intelligence directive. Field Training officers will ensure training on this directive with new officers during their field training. Supervisors are encouraged to periodically discuss the contents of this directive at their roll call briefings.

Training opportunities are also available through the Northern Virginia Criminal Justice Training Academy and other approved entities on a variety of criminal and homeland security intelligence topics.

The *Financial Crimes and Intelligence Unit* conducts periodic Department training on past terrorist events, fraudulent identification documents and terrorism trends. Fraudulent document training is also provided to participants of the Citizen's Police Academy. [40.2.3,c]

By Authority Of:

**Michael L. Brown
Chief of Police**