RENO POLICE DEPARTMENT GENERAL ORDER

This directive is for internal use only and does not enlarge this department's, governmental entity's and/or any of this department's employees' civil or criminal liability in any way. It is not to be construed as the creation of a particular standard of safety or care in an evidentiary sense, with respect to any complaint, demand for settlement, or any other form of grievance or litigation. Violations of this directive, if substantiated, can only form the basis for intra-departmental administrative sanctions.

Chief of Police: Jerry Hoover /s/		
Legal Advisor: Karen Fraley /s/		
Approving Deputy Chief:		
General Order No: S-170-04	Issued: June 29, 2004	Supersedes: 6/900.000
General Order Title**: CRIMINAL INTELLIGENCE UNIT**		

POLICY

The objective of the Criminal Intelligence Unit is to provide the Reno Police Department with sound information that assists in efforts to protect the public and suppress criminal operations. The Unit collects and analyzes information on individuals and groups suspected of involvement in domestic and foreign-based terrorist activity. This information is given to the Deputy Chief in charge of the Detective Division for analysis and dissemination. Intelligence information that involves public safety will be provided to officers in a timely fashion.

DEFINITIONS

Intelligence

Information is the raw data from which intelligence is produced. Intelligence is the product of systematic gathering, evaluation and synthesis of raw data on individuals or groups, and activities suspected of being, or known to be, criminal in nature. The intelligence function involves the collection, collation, evaluation, analysis, and dissemination of information relating to individuals and groups known or suspected to be involved in criminal acts or in the threatening, planning, organizing or financing of criminal acts.

Organized Crime

Organized crime is a structured organization that has ongoing legal and/or illegal enterprises and relies upon tactics such as force, conspiracy, violence, corruption, and monopolistic control to elicit profits.

Terrorism

Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, civilian population, or any segment thereof, in furtherance of political or social objectives.

Terrorist Incident

A terrorist incident is a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States, or of any individual state. It is an act perpetrated to intimidate or coerce a government, civilian population, or any segment thereof, in furtherance of political or social objectives.

PROCEDURES

The Criminal Intelligence Unit is committed to the identification and suppression of any individual or group involved in domestic or foreign-based terrorist activity, and is directly responsible to the Deputy Chief in charge of the Detective Division.

Objectives

Objectives include:

- Identification of subjects involved in activities that pose a substantial threat to the health and safety of the citizens of Reno;
- Identification of potential targets for terrorism within the City of Reno. This includes law enforcement individuals and locations, public figures, public locations, and any other individuals or entities considered to be potential targets for terrorist attacks.
- Exchange of information with surrounding agencies regarding terrorism, hate groups, extremist groups, or individuals who, through their beliefs, pose a substantial threat to law enforcement and to the community;
- Creating a uniformed response to terrorist threats and terrorist activity. The Department will mirror the Office of Homeland Defense's Homeland Security Advisory System (HSAS). The criteria for threat and alert conditions is outlined in G.O. P-195-03 Emergency Response to Critical Incident.

Reports of Terrorist Activity

Complaints and reports concerning possible terrorist activity may be received from a variety of sources, including citizens, officers, and other law enforcement agencies. Investigators from the Criminal Intelligence Unit will follow-up on these reports as soon as they are received and contact appropriate agencies or jurisdictions that may be affected by such activity.

Information related to complaints of terrorist activity will be documented and maintained in the Criminal Intelligence Unit in the form of a Criminal Intelligence Report.

Records relating to Criminal Intelligence Unit investigations are not maintained in the Records Section. Records maintained by the Criminal Intelligence Unit are confidential.

Investigation

The primary mission of the Criminal Intelligence Unit is to gather information on potential and suspected criminal activity, including known terrorists or terrorist-related activity, and store that information until such time as it can and should be disseminated. The Unit will be responsible for the following:

- Referring information substantiating a planned, completed, or ongoing criminal activity to the appropriate intradepartmental division or outside criminal justice agency for follow-up/enforcement action;
- Investigating complaints of terrorist activity;
- Managing confidential informants used by the Department; and
- Maintaining specialized equipment used to conduct surveillance operations and to support the intelligence function.

Criminal Intelligence Information Processing

Raw information will be processed using the following five-step method:

Collection: This function includes not only the accumulation of raw data, but initial collection planning as well.

Evaluation: This is a review of collected raw data prior to its admission to, or removal from, the Criminal Intelligence file. This includes determining the reliability of the source and the validity of the information. The investigator reviewing the information will determine the data acceptability with emphasis on crime and unit goal relationships.

Collation: This includes the merging, indexing, and filing of new criminal intelligence with that already in hardcopy format or computerized files.

Analysis: This step compiles the various filed material together on a criminal target, and, when the materials have been studied, provides the investigator with additional knowledge.

Dissemination: This step includes the sharing of information obtained through the analytical process with other internal division or outside law enforcement agencies.

Criminal Intelligence Information Evaluation

Information obtained by the Unit will be evaluated regarding its source reliability and content validity. The following standard will be used to evaluate criminal intelligence information:

Source Reliability

Reliable – The source is unquestioned or has been well-tested in the past.
Usually reliable – The source is usually relied upon as factual, or a majority of the source's past information has proven to be reliable.
Unreliable – The source has been sporadic in the past.
Unknown – The source cannot be judged. Source authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity

Confirmed – Information has been corroborated by an investigator or other independent reliable source.
Probable – Information is consistent with past accounts.
Doubtful – Information is inconsistent with past accounts.
Cannot be judged – Information and its authenticity has not been determined by either experience or investigation.

Criminal Intelligence Information Classification

Information retained in Criminal Intelligence files should be classified in order to protect sources, investigations, and the individuals' right to privacy.

Classification of criminal intelligence information is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security classification assigned to particular documents. Documents within the Criminal Intelligence files should be reviewed on an ongoing basis to ascertain whether a different degree of document security is required. Classifications are as follows:

Sensitive

- Information pertaining to significant law enforcement cases currently under investigation
- Law enforcement or government official corruption
- Informant identification information
- Criminal intelligence reports, and
- Any other information classified as sensitive in nature.

Confidential

- Criminal intelligence reports not designated as sensitive
- Information obtained through intelligence-unit channels that is not classified as sensitive and that is for law-enforcement use only.

Restricted

- Reports that at an earlier date were classified as sensitive or confidential, but the need for high-level security no longer exists, or
- Non-confidential information prepared by and for law enforcement agencies.

Unclassified

- Civic-related information to which, in its original form, the general public has direct access*, e.g.*, birth and death certificates, or
- Media information, *e.g.*, newspaper, magazine, and periodical clippings dealing with specified criminal categories.

Criminal Intelligence Information Source

In all cases, source identification should be assessable in some form. The true identity of the source should be used unless there is a need to protect the source. In those cases where identifying the source by name is not practical for internal security reasons, a code number may be used. The Department's procedure for maintaining confidential informants will be followed in those cases.

Criminal Intelligence Information Quality Control

Information stored in the Criminal Intelligence files should undergo a thorough review for compliance with established file input guidelines and agency policy prior to being filed. The Unit supervisor is responsible for seeing that all information in the Criminal Intelligence files conforms to the filing criteria and has been properly evaluated and classified.

Criminal Intelligence Report Form

To maintain consistency in the reporting of criminal intelligence information, the following should be reflected in the report:

- Dissemination classification;
- Information status;
- Source reliability;
- Content validity;
- Name of subject referred to in information;
- Subject of information obtained;
- Source of information;
- Name of investigator preparing report; and
- Signature of reviewing supervisor.

An intelligence report will not be used as a case supplement form and will not be included in a case report file.

Criminal Intelligence Records Maintenance

The following procedures relate to the maintenance, dissemination, and security of Criminal Intelligence Unit records.

File Content

A criminal intelligence file contains information on the activities and associations of individuals, organizations, businesses and groups which are:

- known terrorists, or suspected of being, involved in terrorist activity;
- known to be, or suspected of being, involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts;
- known to be, or suspected of being, involved in criminal activities with known or suspected crime figures;

- known to be victims of, or witnesses to, criminal activities conducted by known or suspected crime figures; or
- known to be, or suspected of being, involved in illegally operated or financed business operations controlled by known or suspected crime figures.

Only information meeting the division's objectives will be stored in the criminal intelligence files. Information that does not relate to criminal conduct or activity will be excluded from said files. Information that should specifically be excluded is:

- information on an individual or group merely on the basis of their support of unpopular causes;
- information on an individual or group merely on the basis of ethnic, religious, or political affiliation or background;
- information on an individual or group merely on the basis of personal habits or predilection;
- criminal rap sheets, pretrial proceedings, sentencing memoranda or reports, incarceration reports, parole and probation reports, and arrest and citation forms; and
- information pertaining to the association with individuals that may not be of a criminal nature.

File Security

Intelligence information is confidential and sensitive by its very nature and will be maintained separately from other Department records. The Criminal Intelligence Unit will keep their files under their direct control in a secure environment, thereby preventing compromise and preserving the integrity of the information and protecting the individual's right to privacy. File access will be restricted to authorized personnel.

Criteria for File Status

Permanent Status – Information as it relates to individuals, businesses or groups suspected of being, or having been, involved in the actual or attempted planning, organizing, financing, or committing of one or more of the criminal acts listed below:

- Terrorism or terrorist activities
- Illegal gambling
- Loan-sharking
- Extortion
- Vice or pornography
- Infiltration of legitimate businesses for illegal purposes
- Stolen securities or commodities
- Bribery
- Major crimes including homicide, sexual assault, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing stolen property, and arson
- Manufacture, use, or possession of explosive devices for the purpose of fraud, intimidation, or political motivation
- Threats to public officials and/or private citizens
- Offenses involving computers or related equipment

- Narcotics offenses
- Illegal manufacture, possession, or use of firearms, or
- Any other act deemed criminal in nature.

Temporary Status – Information as it relates to individuals, businesses, or groups may be classified as “temporary” under the following circumstances:

- Subject/entity is unidentifiable
- Involvement is questionable
- Individual, organization, business, or group is not currently criminally active
- Association with a known criminal, and appearing to be jointly involved in illegal activities
- Past history of criminal conduct which indicates that they may be active again
- The reliability and validity of the information is unknown, however appears to be significant and merits temporary storage until verified, or
- Any information that does not meet the criteria for permanent status, so shall be classified as temporary.

File Dissemination

The following terms cover dissemination criteria for intelligence information:

Need to Know – The requested information is pertinent and necessary for the requesting agency in initiating, furthering, or completing an investigation.

Right to Know – The requesting agency has official capacity and statutory authority to the information requested.

Intelligence information will be disseminated to criminal justice agencies that have demonstrated a need-to-know responsibility and a right-to-know authority.

Information classified as “Sensitive” will be disseminated by the Criminal Intelligence Unit through the authority of the Deputy Chief in charge of Detectives. All other information may be released subject to the approval of the Criminal Intelligence Unit supervisor.

Information that has been received from another criminal justice agency will not be disseminated without the specific authorization of the agency that provided the information.

An audit form will be maintained on all information disseminated from the Criminal Intelligence Unit files that is released either by word of mouth or in written form. The following information will be included on the audit form:

- The date the information is being released;
- The agency or individual to which the information is being released;
- The purpose for releasing the information;
- The nature of the information being released, listed by page and paragraph; and
- The person authorizing the release of information.

File Review and Purge

Information stored in the Criminal Intelligence files will be reviewed and purged to ensure the file is current, accurate, and relevant to the needs and objectives of the Department, as well as to safeguard individuals' right of privacy. Criminal intelligence records will be reviewed on a continual basis as personnel use the material in carrying out day-to-day activities. Information that is no longer useful or relevant will be purged.

Permanent files shall be reviewed every five years to ensure that the information is updated, relevant, valid, and utilized. If the file does not meet this criterion, it will be destroyed. Temporary status information may be maintained for up to one year. If after one year, the information does not meet the permanent status criteria, it shall be destroyed. Purged documents will be destroyed in accordance with Department/City policies.