MONTPELIER POLICE DEPARTMENT

CRIMNINAL THREAT ASSESSMENTS, SECURITY ASSESSMENTS, AND REPORT CAVEATS	Related Policies: Acceptable Use of Technology Internet Postings/Social Networking Rules and Regulations
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.	
Applicable Vermont Statutes: Title 1, Chapter 5, Subchapter 3, §315 - §320	
CALEA Standard:	
Date Implemented: October 26, 2020	Review Date: October 26, 2021

I. PURPOSE: It is the purpose of this policy is to establish guidelines for the reporting and assessment of threats. Proper evaluation of threats is essential in establishing strategic operational initiatives that will effectively combat crime and the perception of crime, thus providing a safe environment for the City of Montpelier.

It is also critical for the Department to ensure sensitive information is maintained so not to compromise operations, investigations or officer and individual safety. This directive will also provide guidance regarding the use and dissemination of internal information, as well as law information provided to the Department by other law enforcement or other agencies.

II. Policy: It is the intent of Montpelier Police Department (MPD) to gather information from personnel, operational sources, law enforcement agencies, publicly accessible social media and the general public so to develop an annual Criminal Threat Assessment (CTA) which will assist in the Department's intelligence-led policing efforts. The CTA is designated as Law Enforcement Sensitive/For Official Use Only and therefore may be restricted to the public at-large and limited to individuals on a Need-to-Know basis. Officers should be aware of various policies and practices which regulate intelligence and information dissemination practices so to better facilitate the sharing of information from other law enforcement, intelligence, or investigative agencies. Primary responsibility to compile the CTA is to the Department's Investigations office, however MPD may convene a working group of Officers, Dispatchers and supervisors to compile relevant information for composition for review and approval.

CTAs by nature contain records that may reveal confidential sources, methods, information or individuals accused of but not charged with a crime. Vermont Law affords exceptions in providing information to the public to include matters that are designated confidential or by a similar term; could reasonably be expected to interfere with enforcement proceedings; could reasonably be expected to disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record of information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source; would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecution if such disclosure could reasonably be expected to risk circumvention of the law; trade secrets, etc. See Title 1: General provisions, Chapter 5: Common Law; General Rights, § Definitions; public agency; public records and documents; exemptions.

MPD personnel should also be aware of classification caveats as they may be exposed to such information and may have to use these designations in reports or communications within the department or to outside organizations.

NOTE: Some of the information contained within this policy is derived from the United Nations Office on Drugs and Crime-Criminal Intelligence Manual for Analysts, The Department of Homeland Security Management Directive System MD Number: 11042.1, Laws and Regulations Governing the Protection of Sensitive but Classified Information-The Federal Research Division, and the Office of the Director of National Intelligence-Intelligence Community Authorized Classification and Control Markings.

III. DEFINITIONS:

A. Access ─ The ability or opportunity to gain knowledge or information.

B. Caveat ─ A designation assigned which identifies potentially restricted information. Specific information can be deemed one or more caveats. MPD will utilize the following caveats:

Unclassified (U): Information not subject to a caveat. This information can be freely shared as it is easily accessible to the public via traditional means.

For Official Use Only (FOUO): The term used within the Department of Homeland Security (DHS) and Other Government Agencies (OGAs) to identify unclassified information of a sensitive nature, otherwise categorized by statue or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal, State or Municipal programs, or other programs or operations essential to national, operational or law enforcement interest. NOTE: Officers should be aware that under Executive Order 12958, there are three primary classifications of information impacting the national security of the United States: Confidential, Secret, or Top Secret. "Classified National Security Information," as amended, or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Law Enforcement Sensitive (LES): Unclassified information of a sensitive and proprietary nature that, if disclosed, could cause harm to law enforcement activities by compromising investigations and operations, tradecraft, and/or sources, witnesses, or law enforcement personnel. Officers should note that an entire document must be classified by the highest caveat designation of the information contained within (e.g. if each paragraph of a document has been caveated as Unclassified, but one paragraph is caveated as Law Enforcement Sensitive, the entire document will be classified as LES).

C. Criminal Threat Assessment ─ An evaluation of subjects, trends and information to determine the potential for criminal activity. Information contained within the assessment may only be shared with law enforcement agencies or elected Montpelier officials in efforts to protect tradecraft, on-going investigations, and sensitive information. Personnel may find it necessary to redact some information contained within the CTA and should consult with MPD Investigations for final redactions prior to the dissemination of any information contained within the CTA. The Chief of Police, or designees, are approval authorities regarding caveat designations and the release of FOUO/LES information. Officers should note that MPD does not have the authority to release sensitive information provided to the Department from an outside agency or individual. Officers should seek the approval of the applicable agency prior to releasing it.

D. Need-To-Know ─ The determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized governmental function (e.g. access is required for the performance of official duties).

E. Open Source Intelligence (OSINT) ─ Information obtained through public channels (e.g. news articles or broadcasts, social media, webpages, publicly available research, etc.).

F. Protected Critical Infrastructure Information (PCII) ─ Information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

G. Security Assessment ─ A report which identifies both strengths and potential lapses in physical security, policies and procedures, and other defects and vulnerabilities of an organization, location or structure (e.g. critical infrastructures).

H. Sensitive Security Information (SSI) ─ A specific category of information that requires protection against disclosure. 49 U.S.C 40119 limits the disclosure of this information. MPD will not include this caveat in its reporting but should be aware that it can be found on other government agency documents.

IV. PROCEDURE

A. The CTA will contain, at a minimum: Executive Summary, Uniform Crime Reporting (UCR) or National Incident-Based Reporting (NIBRs) for MPD, Washington County, and the State of Vermont, Identify national/high profile crimes or activities which occurred in the State or Region for the applicable year, Dangerous trends that advocate actions which are criminal-based civil unrest (e.g. unlawful disorderly conduct, the targeting of individuals, officials, organizations or institutions for harassment, violence, kidnapping, etc.),Trends in criminal activity/behavior within the Region, Information pertaining to known domestic, national or international terrorist groups, hate groups, gangs and other criminal organizations, Information pertaining to prevalent drugs in Montpelier, Washington County, the State of Vermont and the region, and a Summary.

B. Executive Summaries should contain no direct LES or other types of sensitive classified information and should have the caveat of “Unclassified.”

C. Each paragraph of the CTA should be labeled with the appropriate caveat.