MIDDLETON POLICE DEPARTMENT	DATE March 27, 2012	POLICY 13.1.1.14
SUBJECT: **Terrorists, Watch Lists, WSIC & SAR**	REVIEWED October 24, 2018	

Refer to: WCAN; WILENET; WiWatch
History: 3/2013; 03/2015
WILEAG (5th Ed.) Standards: 13.1.1.5

Contents

Terrorist Watch List

The Terrorist Watch List is a single database of identifying information about those known or reasonably suspected of being involved in terrorist activity. All records contained in the terrorist portion of the NCIC Violent Gang and Terrorist Organization File (VGTOF) are labeled, "**Possible Terrorist Organization Member - Caution**." This is preceded by a caveat advising law enforcement that the individual may have possible ties or affiliations to terrorism.

A VGTOF return is not justification for a stop or to extend the scope or duration of an encounter. Using caution, officers should follow the normal procedure for the situation at hand (whether it be no action, inquiry, warning, citation, or arrest), noting details for subsequent reporting.

When a VGTOF terrorist record is returned in response to an NCIC inquiry, the individual about whom the inquiry was run **should not be advised that he or she is on a terrorist watch list**.

If a terrorist record contained in the VGTOF is returned in response to an inquiry of NCIC, the individual receiving the response must **follow the protocol set forth in the caveat that precedes the record** (call the number provided), even if the employee had no direct contact with the subject (just ran a plate) or it appears to be a near hit. In addition, the officer may file a Suspicious Activity Report (SAR), if the situation or behavior is suspicious.

VGTOF is considered "Law Enforcement Sensitive and unauthorized secondary dissemination of VGTOF data is prohibited."

**********SAMPLE**********

LAW ENFORCEMENT SENSITIVE INFORMATION
DO NOT ADVISE THIS INDIVIDUAL THAT THEY MAY BE ON A TERRORIST WATCHLIST.
CONTACT THE TERRORIST SCREENING CENTER (TSC) AT (866) 872-9001 DURING THIS ENCOUNTER. IF THIS WOULD EXTEND THE SCOPE OR DURATION OF THE ENCOUNTER, CONTACT THE TSC IMMEDIATELY THEREAFTER. IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.
ATTEMPT TO OBTAIN SUFFICIENT IDENTIFYING INFORMATION DURING THE ENCOUNTER, WITHOUT OTHERWISE EXTENDING THE SCOPE OR DURATION OF THE ENCOUNTER, TO ASSIST THE TSC IN DETERMINING WHETHER OR NOT THE NAME OR IDENTIFIER(S) YOU QUERIED BELONG TO AN INDIVIDUAL IDENTIFIED AS HAVING POSSIBLE TIES WITH TERRORISM.
DO NOT DETAIN OR ARREST THIS INDIVIDUAL UNLESS THERE IS EVIDENCE OF A VIOLATION OF FEDERAL, STATE OR LOCAL STATUTES.
UNAUTHORIZED DISCLOSURE IS PROHIBITED.
INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS THE PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

MKE/POSSIBLE TERRORIST ORGANIZATION MEMBER – CAUTION
ORI/DCTSC0100 NAM/INTTERR,CATEGORY THREE SEX/MRAC/U POB/AF DOB/19190110
HGT/701 WGT/050 EYE/BRO HAI/BLK SKN/ALB
GNG/INTRNTL XTMST*IFBI **SGP/HANDLING CODE 3*IFBI**
ECR/A DOP/NONEXP OCA/FBICJISCARLILEVGTOF7
MIS/THIS IS AN FBI CJISD TEST RECORD TAKE NO ACTION BASED ON THIS RECORD FOR
MIS/FURTHER INFORMATION ON THIS RECORD PLEASE CONTACT TI HARRY E CARLILE JR FBI
MIS/ CJISD 888 827-6427 OR 304 625-3578
ORI IS FBI TERRORIST SCREENING CENTER 866-872-9001
NIC/T570016320 DTE/20030228 0948 EST

**********SAMPLE**********

Wisconsin Statewide Information Center (WSIC)

The Wisconsin Statewide Information Center (WSIC) works with law enforcement statewide to build a centralized intelligence gathering and dissemination facility to fight crime and terrorism. Representatives from local, state, tribal, and federal agencies are encompassed within the WSIC (Fusion Center).

WSIC can be accessed through the WSIC tab at WILENET and includes: Contact Information; Suspicious Activity Report; Bulletins/Alerts; Resource Links; Requests for Assistance; and Requests for Information.

Suspicious Activity Reporting (SAR)

This SAR initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. SAR reports are made by local law enforcement and go to the Wisconsin State Information Center (WSIC) for analysis and sharing. A SAR is typically submitted online, the form is accessible through the WSIC tab at WILENET. Attachments (reports, images, etc.) can be uploaded to the SAR. Normally SAR reports will be approved by the ISB Commander before submittal, but can be approved by the Shift Commander if the matter is time sensitive.

WiWatch

To augment the national "If You See Something, Say Something" campaign in Wisconsin, the Wisconsin Fusion Centers have instituted WiWatch to provide a portal to educate the public and provide a means to report suspicious behavior or activity. Persons who observe suspicious activity are encouraged to call WiWatch at 1-877-WIWATCH (1-877-949-2824) or report online. Citizens may call local police in lieu of WiWatch.

Suspicious Behaviors/Activities That Should be Reported

We respect civil rights and liberties by emphasizing behavior, rather than appearance, in identifying suspicious activity.

ELICITING INFORMATION	Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person.
TESTING OF SECURITY	Interactions with or challenges to installations, personnel, or systems that reveal physical personnel or cybersecurity capabilities.
RECRUITING	Building operations teams and contacts, personnel data, banking data, or travel data.

PHOTOGRAPHY	Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc. All reporting on photography should be done within the totality of the circumstances.
OBSERVATION / SURVEILLANCE	Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g., engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.
MATERIALS ACQUISITION / STORAGE	Acquisition of unusual quantities of precursor materials, such as cell phones, pagers, fuel, and timers, such that a reasonable person would suspect possible criminal activity.
AQUISITION OF EXPERTISE	Attempts to obtain or conduct training in security concepts (military weapons or tactics) or other unusual capabilities that would arouse suspicion in a reasonable person.
WEAPONS DISCOVERY	Discovery of unusual amounts of weapons or explosives that would arouse suspicion in a reasonable person.
SECTOR SPECIFIC INCIDENT	Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector) with regard to their personnel, facilities, systems, or functions.
BREACH / ATTEMPTED INTRUSION	Unauthorized personnel attempting to enter or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g., police/security, janitor).
MISREPRESENTATION	Presenting false or misusing insignia, documents, and/or identification to misrepresent one's affiliation to cover possible illicit activity.
THEFT / LOSS / DIVERSION	Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents [classified or unclassified] that are proprietary to the facility).
SABOTAGE / TAMPERING / VANDALISM	Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.
CYBERATTACK	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
EXPRESSED OR IMPLIED THREAT	Communicating a spoken or written threat to damage or compromise a facility/infrastructure.
AVIATION ACTIVITY	Operation of an aircraft in a manner that reasonably may be interpreted as suspicious or posing a threat to people or property. May or may not be in violation of Federal Aviation Regulations.

Wisconsin Crime Alert Network (WCAN)

The Wisconsin Crime Alert Network (WCAN) is a statewide program that links law enforcement agencies with the business community and the public in a partnership to fight crime. WCAN allows law enforcement agencies to send out crime alert bulletins rapidly, to the business community and to the general public, whenever a crime or suspect may affect citizens or their businesses. Subscribers receive Crime Alerts, Amber Alerts, and Missing Person Alerts.

Law enforcement officers may issue crime alert bulletins to participating businesses and the public throughout the state or target Crime Alerts to specific business types (chosen from a list of 50 business types) and/or specific geographic areas (by county, region or statewide).

An officer may have a Crime Alert submitted to WCAN by a Dispatcher. Normally WCAN alerts will be approved by the ISB Commander, but can be approved by the Shift Commander if the matter is time sensitive.

Acts of Terrorism

The Middleton Police Department recognizes the federal government's commitment to the fight against terrorism. The Federal Bureau of Investigation (FBI) has been designated as the lead agency in all terrorism investigations. Therefore, the department will work with the FBI and Wisconsin Statewide Information Center (WSIC) in all matters suspected as a "Terrorist Act." Officers initially responding to calls related to "Terrorism" shall follow the procedures laid out in this policy.

The department will forward all suspected terrorist activity information to WSIC and assist WSIC/FBI in the manner they request with any further investigation into suspected terrorist activity.

Upon the discovery of any "Terrorist Activity" the investigating officer obtaining such information shall notify the Shift Commander and complete a report. The Shift Commander will notify the ISB Commander and Operations Captain.

The ISB Commander will normally be the point of contact for sharing Terrorist Activity Information to any other agency, but the Shift Commander may assume this role if the information is time sensitive.

Wisconsin Statewide Information Center (WSIC)
Phone: 608-242-5393
Toll Free: 888-DCI-WSIC
Fax: 608-240-3592
E-mail: WSIC@doj.state.wi.us
WILENET