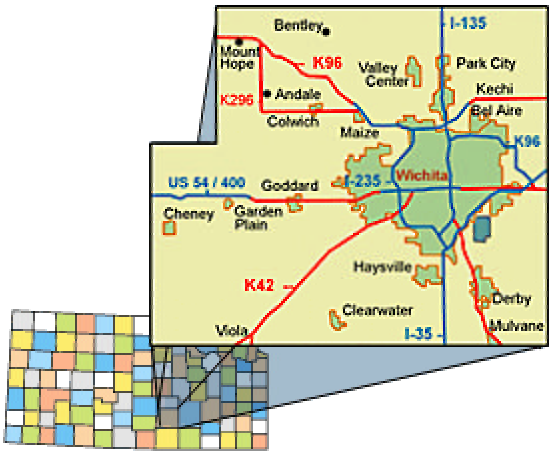
COUNTY AND MUNICIPAL GOVERNMENT GUIDELINES FOR IMPLEMENTATION OF THE HOMELAND SECURITY ADVISORY SYSTEM



Adapted by the Sedgwick County Homeland Security Advisory Committee

TABLE of CONTENTS

INSTRUCTION TO USERS

This guidebook is designed to assist units of county and city government to initiate standardized actions as the result of increased terrorist threat levels within the United States and Sedgwick County. This guide provides a number of recommendations that may be issued following a recommendation issued by the National Homeland Security Office in Washington DC.

These recommendations have been developed in a generic format to allow the county, municipal government, fire protection district, or other entity to develop specific implementation procedures appropriate for the size and complexity of the jurisdiction. A generic overview of each of the combined threat alert levels is followed by more specific tasks for each level. Each recommended action has been numbered to allow recommended implementation of specific actions, i.e.: "implement G-1 through G-4". County and municipal units of government are encouraged to develop additional action steps as appropriate for their jurisdictions. It is suggested however, that locally developed actions be numbered in a range beginning with the number "100" to avoid confusion with those recommendations issued by the region. Further specific steps may be developed by local government entities depending of their own objectives, capabilities and resources.

Please remember, these actions are not prescriptive or required, they are suggestions to consider in light of any intelligence which may indicate a credible threat aimed at the Wichita / Sedgwick County area.

Throughout this document various terms are used. For definition, these terms are defined below.
"C" refers to county/city government
"Critical Infrastructure Facility" refers to facilities within the jurisdiction that may be terrorist targets, examples include:

Electrical Energy (generation / switching / load dispatch)
Emergency Services (emergency operations centers, fire, law enforcement, medical)
Gas and Oil production
Telecommunications (9-1-1 centers, critical tower sites, telephone and communications infrastructure)
Transportation (terminals, bridges, etc)
Water (distribution systems and treatment plants)
Government Buildings
Media (radio and television transmission sites, EAS activation points)
Schools (elementary through colleges)
Industry

"M " refers to municipal units of government, which are defined as municipal governments, fire protection districts, townships, and other special districts as appropriate.

PLEASE NOTE ...This document is provided as a guidance document to assist local planners develop detailed procedures. While this guidance is not confidential in nature, the document developed at the local level should be considered as a restricted document, not for release to the public. The locally developed document should contain as much detail as necessary to ensure adequate levels of security for the users jurisdiction.

DISSEMINATION OF THREAT CONDITION ADVISORIES WITHIN SEDGWICK COUNTY

(This is a sample of how information may be shared)

Following notification of a change in the Threat Condition from the Homeland Security Coordination Center, Federal Emergency Management Agency's (FEMA) Federal Operations Center will broadcast threat condition notifications over the National Warning System (NAWAS) to all fifty states, including local warning points, and will conduct a roll call after the broadcast to ensure receipt. Each state will verify receipt by their local warning points.

The State will disseminate threat condition advisory messages and other related strategic information in the following manner:

1. State EMA will alert, via NAWAS, the following:
    a. State Patrol Headquarters
    b. NAWAS Extensions (key counties, National Weather Service Forecast Offices)
2. State EMA will alert appropriate state officials, state government agencies, who will in turn be responsible for notifying their district and / or satellite offices and allied agencies.

3. Each county will disseminate the threat condition advisory to appropriate county officials, departments and agencies, and designated municipal warning entry points (one per municipality).

4. Each municipality will be responsible for disseminating the threat advisory to its municipal officials, departments and to identified special facilities (schools, hospitals, industries, etc.) This will be accomplished by using the existing network of identified Emergency Management points of contact within each of the communities within Sedgwick County.

5. Following the receipt of the statewide-consolidated confirmation report at the State Emergency Operations Center, State EMA or the appropriate government agency will authorize the release of pre-developed media information appropriate for the identified threat level.

6. Dissemination of information to Law Enforcement and Fire Service agencies through parallel Information systems should also occur the same manner, i.e. FBI. However, local jurisdictions should develop interagency communication systems, i.e. Joint Information System to facilitate their process.

Page left blank for development of

Threat Condition Distribution System

Sedgwick County Emergency Services
Sedgwick County Homeland Security Coordinating Committee
Terrorism Warning System Considerations

Threat Level	Recommended Protocols	Recommended Actions
GREEN Low risk of terrorist attacks.	Lowest risk of terrorist activity.	**Normal** operations with assessment and monitoring for possible terrorism activity.
BLUE General risk of terrorist attacks. In addition to above measures.	**When there is a general threat of terrorist activity.** **Note** and report suspicious circumstance, packages, and activity. **Ensure** essential facilities are secured and building integrity is maintained. **Emergency Service** units exercise heightened caution when responding to related calls for service. **Police** conduct location verification "drive by" of potential critical sites.	**All** elected officials and Department Directors notified of potential problems/threat as indicated. **Personnel** maintain routine security posture. **Regular** shifts maintained. **Contact** or establish liaison with Federal, State and local agencies to evaluate threat.
YELLOW Significant risk of terrorist attacks. In addition to above measures	**When there is a specific threat of possible terrorist activity.** **Implement** physical security measures. **Conduct** cursory check for suspicious items, persons, and vehicles. **Limit** public access to critical infrastructure, sites, and facilities. **All** personnel to wear ID cards whether in uniform or not while in secured facilities.	**All** elected officials and Department Directors notified of the potential problem/threat. **Daily** liaison with Federal, State, and local agencies as appropriate.
ORANGE High risk of terrorist attacks. In addition to above measures.	**When there is a specific threat of possible terrorist activity.** **Erect** barricades and obstacles to control traffic if warranted. **Terminate** all non-essential contract work and deliveries to critical infrastructure and facilities. **Conduct** detailed searches of all operational areas and vehicles. **Limit** or restrict parking around sensitive areas and buildings. **Increase** security forces at appropriate sites.	**Activate** joint information center as indicated. **Activate** EOC if warranted. **Consider** alternate staffing plans and additional staffing. **Ready** mass casualty and other special support resources. Ongoing liaison with Federal, State, and local authorities as appropriate.
RED Severe risk of terrorist attacks. In addition to above measures.	**When terrorist attack is imminent or is occurring.** **Deny** access to all non-essential personnel. Verify identities and the need for access to essential critical facilities. **Restrict**/deny parking in controlled areas. **Limit** responses to non-emergency EMS calls as indicated.	**Emergency** recall of all personnel should be considered. **Full** IMS Command System activation and/or Unified Command Activated. **Activate** EOC. **Deploy** MCI resources as needed **Activate** joint information center.

THREAT CONDITION GREEN

Low Risk of Terrorist Attack Within the Region

INITIATING EVENT:
Normal operating conditions.

General Government Guidelines:

- Refining and exercising preplanned protective measures.
- Ensuring personnel receive training on Homeland Security Advisory System, departmental, or agency-specific protective measures
- Regularly assessing facilities with vulnerabilities and taking measures to reduce them.

OTHER GOVERNMENT ACTIONS:

- Regular operations with agencies having 24-hour communications centers, or agency duty officers.

COUNTY (C) / MUNICIPAL (M) ACTIONS:

ACTION NUMBER	By	By	Recommended Action:
G-1	C		Disseminate the GREEN advisory to county departments / agencies, municipal and fire district dispatch centers, and county government officials identified on the county Warning / Alerting Notification List.
G-1		M	Disseminate the GREEN advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning / Alerting Notification List
G-2	C	M	Report suspicious. circumstances and / or individuals to law enforcement agencies.
G-3	C	M	Routine operations without security stipulations are allowable.
G-4	C	M	Continue to include responder safety and common sense practices in daily routines.

Page Left Intentionally blank

THREAT CONDITION
BLUE – GUARDED

General Risk of Terrorist Attack within the Region

INITIATING EVENT:
Received threats that do not warrant actions beyond normal liaison notifications or placing assets or resources on a heightened alert (agencies are operating under normal day-to-day conditions).

General Government Guidelines:

- Checking communications with designated emergency response or command locations
- Reviewing and updating emergency response procedures
- Providing the public with necessary information

OTHER GOVERNMENT ACTIONS:
All agencies with 24-hour duty officers on call

COUNTY (C) / MUNICIPAL (M) ACTIONS:

Action Number	By	By	Recommended Action:
B-1	C		Disseminate the BLUE advisory to county departments / agencies, municipal and fire district dispatch centers, and county government officials identified on the county Warning / Alerting Notification List.
B-1	L		Disseminate the BLUE advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning/Alerting Notification List
B-2	C	M	Continue, or introduce all measures listed in Threat condition GREEN Advisory.
B-3	C	M	Review all applicable emergency plans. (Emergency Operations Plan, SOP/SOGs, personnel staffing schedules, internal security plans, etc.)
B-4	C	M	Implement security plans appropriate to the facility.
B-5	C	M	Dispatch centers should prohibit any form of casual access by unauthorized personnel.
B-6	C	M	Ensure that all government vehicles are secured.
B-7	C	M	Review and update public and private critical infrastructure target

			listings.
B-8	C	M	Continue routine checks of all equipment for operational readiness, fill fuel tanks, and check specialized response equipment. (hazmat, TRS, SWAT, bomb squad, command post, generators, etc.)
B-9	C	M	Brief emergency response personnel on increased security/safety concerns appropriate to the threat level. (security measures, suspicious situations, etc.)
B-10	C	M	Monitor and test communications and warning systems at periodic intervals.
B-11	C	M	Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the threat level.
B-12	C	M	Assess mail handling procedures against intelligence in relation to the current threat level.
B-13	C	M	Be alert to suspicious activity and report it to the proper authorities.

THREAT CONDITION
YELLOW – ELEVATED

Significant Risk of Terrorist Attack Within the Region

INITIATING EVENT:
Intelligence or an articulated threat indicates a potential for a terrorist incident. However this threat has not yet been assessed as credible.

GENERAL GOVERNMENT ACTIONS:

- Increasing surveillance of critical areas
- Coordinating emergency plans with related agencies
- Assessing further refinement of protective measures within the context of the current threat information
- Implementing, as appropriate, contingency plans and emergency response plans

OTHER GOVERNMENT ACTIONS:

- As conditions warrant, provide a weekly or other regular interval briefing for EOC staffing.

COUNTY (C) / MUNICIPAL (M) ACTIONS:

Action Number	By	By	Recommended Action:
Y-1	C		Disseminate the YELLOW advisory to county departments / agencies, municipal and fire district dispatch centers, and county government officials identified on the county Warning / Alerting Notification List.
Y-1		M	Disseminate the YELLOW advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning / Alerting Notification List.
Y-2	C	M	Continue, or introduce all measures listed in Threat condition BLUE Advisory.
Y-3	C	M	Provide weekly briefings to EOC staff, government officials, and first responders regarding the current threat advisory level and local implications. (As required)
Y-4	C	M	Continually review and be prepared to implement critical

			infrastructure facility security plans. (See security recommendations)
Y-4a	Remind all personnel to be suspicious and inquisitive and maintain heightened awareness of people, vehicles, and activities		
Y-4b	Increase spot checks of specific high-risk targets / facilities.		
Y-4c	Do not leave emergency response vehicles unattended. If it is necessary to leave the vehicle, lock it and check the vehicle and its chassis underside before opening the door and starting the engine.		
Y-4d	Move vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature.		
Y-4e	Lock and regularly inspect all buildings, rooms, and storage areas not in regular use.		
Y-4f'	At the beginning and end of each work shift, as well as at other regular and frequent intervals inspect the interior ad exterior of buildings in regular use for suspicious packages.		
Y-4g	Check all deliveries to facilities. Advise families of responders to check home deliveries.		
Y-5	C	M	Brief and stress information and operational security issues to first responders and government officials.
Y-6	C	M	Share pertinent information directly related to the threat level with first responders and government officials.
Y-7	C	M	Consider alternative work schedules of operational and staff personnel if the situation escalates. Include plans to maximize staffing and response capabilities with defined work / rest cycles.
Y-8	C	M	Consider plans and contingencies to assist public safety employees' family members regarding safeguard issues if the situation escalates and personnel are recalled leaving their family alone for extended periods of time.
Y-9	C	M	Continue routine checks of all equipment for operational readiness, fill fuel tanks, check specialized response equipment (hazmat, TRS, SWAT, bomb squad, command post, etc.)
Y-10	C	M	Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items.
Y-11	C	M	Check recall roster and recall processes for accuracy. Review vacation / day off roster and consider staffing options if the situation escalates.
Y-12	C	M	Identify any planned community events where a large attendance is anticipated. Consult with event organizers regarding contingency plans, security awareness, and site accessibility and control.
Y-13	C	M	Continue Meetings with appropriate representatives of critical infrastructure facilities to review contingency and evacuation plans and brief employees.
Y-14	C	M	Increase the frequency of backups for critical information systems and ensure availability of technical support. (i.e.: systems programmers, technical personnel, redundancy of equipment, off-site storage of critical data, stockpile of critical spare parts, off-site data recovery site)
Y-15	C	M	Review all plans, orders, SOPs / SOGs, personnel details, and logistical requirements related to the introduction of a higher threat level.
Y-16	C	M	Check inventories of critical supplies and re-order if necessary
Y-17	C	M	Be alert to suspicious activity and report it to the proper authorities.

THREAT CONDITION ORANGE

High Risk of Terrorist Attack Within The Region

INITIATING EVENT:

A threat assessment indicates that the potential threat is credible, and confirms the involvement of WMD in the developing terrorist incident.

GENERAL GOVERNMENT ACTIONS:

- Crisis management response will focus on law enforcement actions taken in the interest of public safety and welfare, and is predominantly concerned with preventing and resolving the threat.
- Consequence management response will focus on contingency planning and pre-positioning of tailored resources, as required.

OTHER GOVERNMENT ACTIONS:

- EOC activation level 2 call list on 3O-minute call back to the EOC
- 24-hour on-call duty officers from staff
- Prepare to, and if necessary, activate a Joint Information System or Joint Information Center (JIC) near the threatened area. Coordinate the release of information with appropriate local, county, state, and federal agencies.

COUNTY (C) / MUNICIPAL (M) ACTIONS:

Action Number	By	By	Recommended Action:
0-1	C		Disseminate the ORANGE advisory to county departments/ agencies, municipal and fire district dispatch centers, and county government officials identified on the county Warning / Alerting Notification List.
0-1		M	Disseminate the ORANGE advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning / Alerting Notification List.
0-2	C	M	Continue, or introduce all measures listed in Threat condition YELLOW Advisory.
O-3	C	M	Activate the jurisdiction's Emergency Operations Center (EOC) (level 2) for an initial situation briefing of EOC staff Following the initial briefing, maintain limited staffing, as warranted/appropriate.
0-4	C	M	Provide a daily briefing to EOC staff and government officials. As appropriate.

0-5	C	M	Place all emergency management and specialized response teams on full alert status
0-6	C	M	If not already accomplished, implement critical infrastructure facility security plans (See Security Recommendations)
0-6a	At the beginning and end of each work shift, as well as at other regular and frequent intervals inspect the interior and exterior of buildings in regular use for suspicious packages.		
0-6b	Limit access points to critical infrastructure facilities to the absolute minimum, and strictly enforce entry control procedures.		
0-6c	Increase security patrols around critical infrastructure facilities. Contact allied government agencies within the jurisdiction and advise them of the need for increased security and awareness.		
0-6d	Identify and protect all designated vulnerable points. Give special attention to vulnerable points outside of the critical facility.		
0-6e	Erect barriers and obstacles to control the flow of traffic, as appropriate.		
0-6f	Consider closing public roads and facilities that might make critical facilities more vulnerable to attack.		
0-6g	Lock all exterior doors except the main facility entrance(s). Check all visitors' purpose, intent and identification. Ensure that contractors have valid work orders outlining tasks to be performed within the secured facility. Require a visitors sign-in log with information from their identification. Escort visitors when they are in the facility until they leave. Check where the visitors were or worked to assure nothing is amiss or left behind.		
0-6h	Keep critical response vehicles in a secure area or in an indoor facility. Keep garage doors closed except for bona fide needs.		
0-6i	Increase defensive perimeters around key structures and events.		
0-7	C	M	Contact all personnel to ascertain their recall availability. Plan modifications where appropriate to staffing schedules to provide the maximum recall surge of personnel if needed.
0-8	C	M	Advise staff of contingency plans for shift modifications, assignments, work / rest cycles and family member care / assistance and security plans if the situation escalates.
0-9	C	M	Activate the jurisdiction's Emergency Public Information System. Coordinate information releases with municipal, county, and state governments, if possible. [1]
0-10	C	M	Test communications and warning systems to ensure operability.
0-11	C	M	Ensure personal protective equipment (PPE) and specialized response equipment is checked, issued, and readily available for deployment.
0-12	C	M	Suspend public tours of critical infrastructure facilities.
0-13	C	M	Limit access to computer facilities. No outside visitors.
0-14	C	M	Increase staffing to monitor computer and network intrusion detection systems and security monitoring systems.
0-15	C	M	Ensure the availability of sufficient technical resources to respond to and mitigate a cyber attack.
0-16	C	M	If not already accomplished, identify any planned community events where a large attendance is anticipated. Consult with event organizers regarding contingency plans, security awareness, and site accessibility and control. Consider recommendations to cancel the event if warranted by the current situation.
0-17	C	M	Contact critical infrastructure facilities including: elected officials, businesses, schools, hospitals, etc. to discuss the heightened threat and security and contingency operations.
0-18	C	M	Check all equipment for operational readiness, fill fuel tanks, check

			specialized response equipment. (hazmat, TRS, SWAT, bomb squad, command post, generators, etc.)
0-19	C	M	Consider off-site mail/package processing and sorting facility to reduce the threat to government employees.
0-20	C	M	Review all plans, orders, SOPs / SOGs, personnel details, and logistical requirements related to the introduction of a higher threat level.
0-21	C	M	Check inventories of critical supplies and re-order if necessary.
0-22	C	M	Be alert to suspicious activity and report it to the proper authorities.

1 The local Emergency Public Information System should be identified in the local Emergency Operations Plan, Examples of methods to disseminate emergency information may include' local website, telefax distribution, reverse 9-1-1, hotline systems, and press releases, etc

When Threat Is General Or Not For This Area

Continue recommended actions for Threat Condition ORANGE and Review recommended actions for Threat Condition RED (within the region). Remain vigilant of intelligence information and be prepared to move to Condition RED (within the region) as necessary.

THREAT CONDITION
RED

Severe Risk of Terrorist Attack
Within The Region

INITIATING EVENT:

A WMD terrorism incident is imminent or has occurred.

GENERAL GOVERNMENT ACTIONS:
Response is primarily directed toward public safety and welfare and the preservation of human life, including:

- Assigning emergency response personnel and pre-positioning of specially trained teams
- Monitoring, redirecting or constraining transportation systems
- Recommend closing selected public and governmental facilities
- Increasing or redirecting personnel to address critical emergency needs

OTHER GOVERNMENT ACTIONS:

- Around the clock staffing of Emergency Operations Center (EOC) involving all agencies that are standing members of the EOC plus other agencies as deemed appropriate
- Following assessment of the situation, if the event threatens or actually impacts the Region, issuing a declaration of a "State of Disaster" by the appropriate authority.
- Activation of a Joint Information Center (JIC) to include representatives from affected areas and agencies.

COUNTY (C) / MUNICIPAL (M) ACTIONS:

It is anticipated that actions listed under this threat level will be initiated and sustained for a relatively short period of time, based on guidance from federal and state governments, due to significant personnel and economic considerations.

Number	By	By	Recommended Action:
R-1	C		Disseminate the RED advisory to county departments / agencies, municipal and fire district dispatch centers, and county government officials identified on the county Warning / Alerting Notification List.
R-1		M	Disseminate the RED advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning/Alerting Notification List.
R-2	C	M	Continue, or introduce all measures listed in Threat condition ORANGE Advisory.
R-3	C	M	Consider a local declaration to authorize activation of the local emergency management system .
R-4	C	M	Staff Emergency Operations Center (EOC) or Command Post on a 24-hour basis. Provide security for this facility.
R-5	C	M	Maintain and monitor communications and warning systems and provide periodic operational status reports to next higher level of government.
R-6	C	M	Implement appropriate staff recall/staffing plans. Keep all personnel responsible for implementing anti-terrorist plans at their places of duty.
R-7	C	M	If not already accomplished, implement critical infrastructure security plans. (See Security Recommendations)
R-7a	Make a positive identification of all vehicles located or, operating within critical government areas.		
R-7b	If not already accomplished, implement parking restrictions and park vehicles away from critical facilities.		
R-7c	Control access and implement positive identification of all personnel -no exceptions.		
R-7d	Search all suitcases, briefcases, packages, etc brought into a critical facility.		
R-7e	Secure all doors to communications, command centers, and data processing centers. Maintain a security presence on a single point of access to each structure and check identification of potential visitors to determine valid purpose of entry. Maintain a sign-in log. Check all bags, briefcases and packages at the security point. All authorized visitors must be escorted while in the facility.		
R-7f	Increase defensive perimeters, including manpower, around critical facilities. Make frequent checks of the exterior of critical facilities and begin spot checks of lower risk targets.		
R-7g	Consider placing an individual (career or volunteer) on watch at all critical facilities		

	24-hours a day until the threat level has diminished.		
R-7h	Deliveries to critical facilities should not be accepted unless approved by supervisory staff. All deliveries should not be opened inside of the critical facility, and minimal personnel should be in the immediate area when the package is opened.		
R-8	C	M	Consider releasing non-critical function personnel.
R-9	C	M	Ensure 24-hour access to the jurisdiction's Principal Executive Officer (County Board Chair, Mayor, Village President) or their designated alternate.
R-10	C	M	If not already accomplished, implement the Emergency Public Information System.[2]
R-11	C	M	Brief all EOC, government and first response personnel on critical facility evacuation routes and contingency communications plans. Provide direction regarding what equipment, supplies should be taken in the event of an evacuation.
R-12	C	M	Ensure welfare checks of government personnel and facilities throughout the day and night.
R-13	C	M	Activate, or place on high alert specialized response teams / personnel. (i.e.: hazmat, TRS, EMS, SWAT, Crisis Counseling, etc.)
R-14	C	M	Be prepared to control access routes serving critical infrastructure facilities and evacuation routes.
R-15	C	M	Increase security at water / sewer facilities and increase the frequency of testing for impurities and contaminants.
R-16	C	M	Maintain communications with, and provide security for hospitals and critical medical facilities, if appropriate.
R-17	C	M	Stress the possibility of a secondary attack against first responders.

2 The local Emergency Public Information System should be identified in the local Emergency Operations Plan, Examples of methods to disseminate emergency information may include' local website, telefax distribution, reverse 9-1-1, hotline systems, and press releases, etc,

SAMPLE WARNING / ALERTING NOTIFICATION LIST

Date: _____ THREAT ADVISORY LEVEL _____

Notify	Notification Mechanism (phone, pager, e-mail	Time Notified	Person Contacted (for phone only)	Operators Initials
County Government				
Chair / Elected Officials				
Sheriff				
Emergency Mgt.				
Public Works				
Manager's Office				
EMS				
Fire District #1				
District Courts				
Health Department				
MMRS				
Courthouse Security				
County Counselor				
County Health Department				
Municipal Government				
Mayor/Elected				
Police Chief				
Fire Chief				
Public Works				
Manager's Office				
Water / Sewer				
City Attorney				
Airport Authority				
Environmental Health				

Critical Facilities / Others				
Schools USD 259				
Hospitals				
FBI				
Secret Service				
TSA				
Universities				
McConnell AFB				

REFERENCES

Kansas City Missouri Police Department
"Homeland Security Advisory System Report on Possible Use of System Within Metro Kansas City"

Heart of America Fire Chiefs
"MARC Homeland Security Committee Terrorism Warning System Recommendations"

MARCER
"MARC – Emergency Medical Services Regional Homeland Security Coordinating Committee Terrorism Warning System Considerations"

State of Illinois Terrorism Task Force
"County and Municipal Government Guidelines for Implementation of the State of Illinois Homeland Security Advisory System"