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

Developed By The
Illinois Terrorism Task Force

This page intentionally left blank

TABLE OF CONTENTS

This page intentionally left blank

INSTRUCTION TO USERS

This guidebook is designed to assist units of county and local government initiate standardized actions as the result of increased terrorist threat levels within the United States and the State of Illinois. This guide provides a number of recommendations that may be issued by the State of Illinois 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. Each recommended action has been numbered to allow the State to recommend implementation of specific actions, i.e: "implement G-1 through G-4". County and local 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 State of Illinois.

Throughout this document various terms are used. For definition, these terms are defined below.

"C" refers to county 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)
Financial Institutions	(include processing facilities)
Government Buildings	
Media	(radio and television transmission sites, EAS activation points)
Office Buildings	(especially multi-national corporations)
Religious Institutions	
Retail / Public Areas / Hotels / Conference Centers	
Schools	(elementary through colleges)

"L" refers to local 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.**

This page intentionally left blank

DISSEMINATION OF THREAT CONDITION ADVISORIES WITHIN THE STATE OF ILLINOIS

Following notification of a change in the Threat Condition from the Homeland Security Coordination Center, FEMA's 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 of Illinois will disseminate threat condition advisory messages and other related strategic information in the following manner:

1. IEMA will alert, via NAWAS, the following:
    a. ISP Command Center
    b. ISP District Headquarters
    c. NAWAS Extensions (City of Chicago, key counties, National Weather Service Forecast Offices)

2. IEMA will alert appropriate state officials, state government agencies, and Red Center, who will in turn be responsible for notifying their district and / or satellite offices.

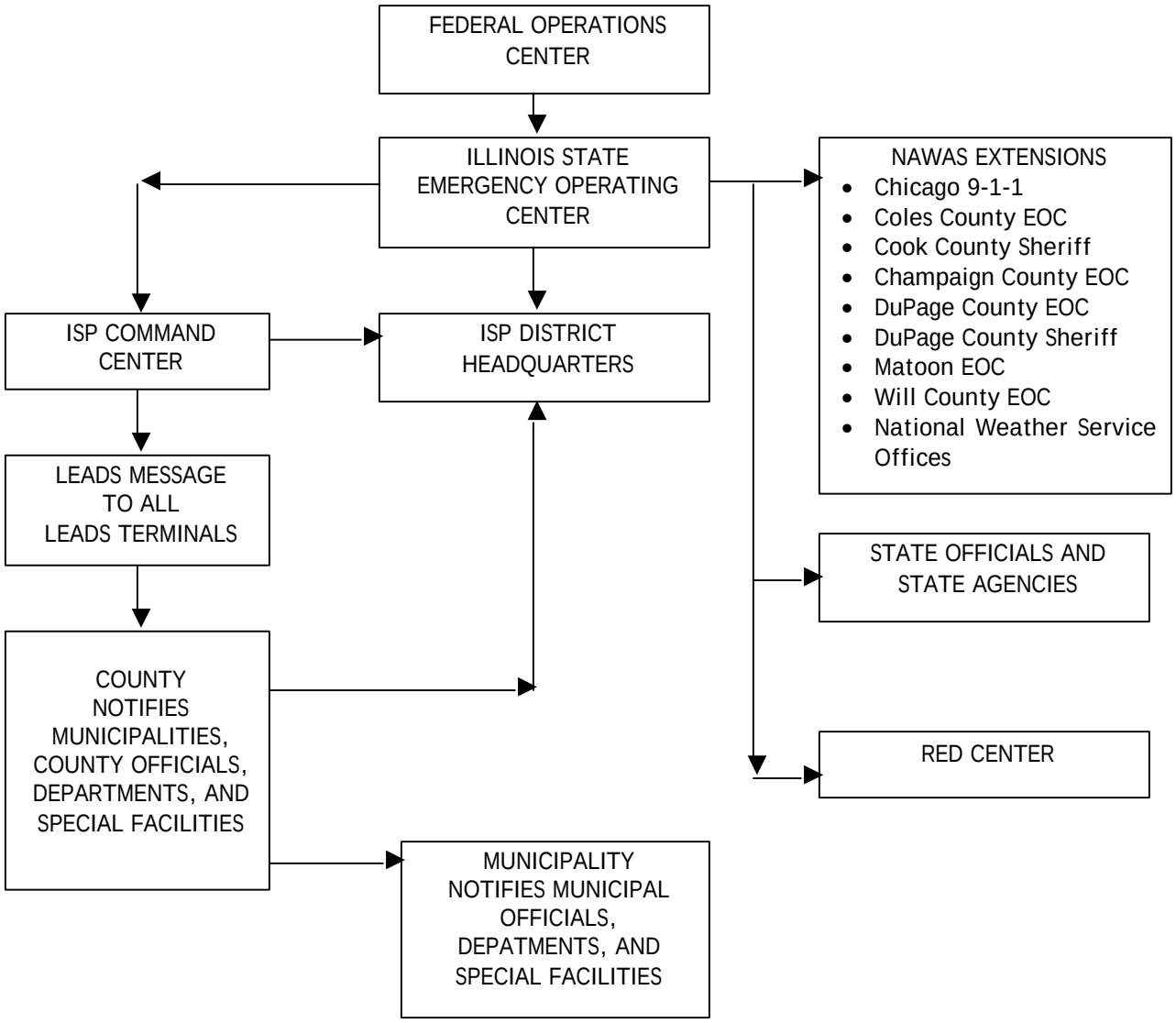
3. The ISP Command Center will disseminate the threat advisory via a statewide LEADS message to all LEADS terminals.

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

5. Each municipality will be responsible for disseminating the threat advisory to its municipal officials, departments and to identified special facilities (schools, hospitals, industries, etc.)

6. Following the receipt of the statewide consolidated confirmation report at the State Emergency Operating Center, or 30 minutes after initial dissemination by IEMA, whichever occurs first, IEMA will authorize the release of pre-developed media information appropriate for the identified threat level.

FIGURE 1 – THREAT CONDITION DISTRIBUTION SYSTEM



THREAT CONDITION
GREEN

Low Risk Of Terrorist Attack Within The State of Illinois

INITIATING EVENT:

Normal operating conditions.

FEDERAL GOVERNMENT ACTIONS:

- 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

STATE GOVERNMENT ACTIONS:

- Regular operations with 24-hour IEMA communications center, agency duty officers, and IEMA duty officer.

COUNTY / LOCAL ACTIONS:

Action Number	Applicable To:		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		L	Disseminate the GREEN advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning / Alerting Notification List.
G-2	C	L	Report suspicious circumstances and / or individuals to law enforcement agencies.
G-3	C	L	Routine operations without security stipulations are allowable.
G-4	C	L	Continue to include responder safety and common sense practices in daily routines.

This page intentionally left blank

THREAT CONDITION
BLUE - GUARDED

General Risk Of Terrorist Attack Within The State of Illinois

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).

FEDERAL GOVERNMENT ACTIONS:

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

STATE GOVERNMENT ACTIONS:

- All agencies with 24-hour duty officers on call
- State Emergency Operations Center (SEOC) Manager, IEMA Chief of Operations, and IEMA Director serving as 24-hour terrorism duty officer on weekly rotating basis in addition to normal IEMA duty officer.

COUNTY / LOCAL ACTIONS:

Action Number	Applicable To:		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	L	Continue, or introduce all measures listed in Threatcon GREEN Advisory.
B-3	C	L	Conduct a briefing for EOC staff and emergency response personnel and government officials as needed or required.
B-4	C	L	Review all applicable emergency plans. (Emergency Operations Plan, SOP / SOGs, personnel staffing schedules, internal security plans, etc.)
B-5	C	L	Implement security plans appropriate to the facility.

B-6	C	L	Dispatch centers should prohibit any form of casual access by unauthorized personnel.
B-7	C	L	Ensure that all government vehicles, and private vehicles parked at government sites, are secured.
B-8	C	L	Review and update public and private critical infrastructure target listings.
B-9	C	L	Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment. (hazmat, TRS, SWAT, bomb squad, command post, generators, etc.)
B-10	C	L	Brief emergency response personnel on increased security / safety concerns appropriate to the threat level. (security measures, suspicious situations, etc.)
B-11	C	L	Monitor and test communications and warning systems at periodic intervals.
B-12	C	L	Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the threat level.
B-13	C	L	Assess mail handling procedures against intelligence in relation to the current threat level.
B-14	C	L	Be alert to suspicious activity and report it to the proper authorities.

.

THREAT CONDITION
YELLOW - ELEVATED

Significant Risk Of Terrorist Attack Within The State of Illinois

INITIATING EVENT:

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

FEDERAL 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

STATE GOVERNMENT ACTIONS:

- Weekly briefings of all agency liaisons in the State Emergency Operations Center (SEOC)
- All agency liaisons on 30-minute call back to the SEOC

COUNTY / LOCAL ACTIONS:

Action Number	Applicable To:		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		L	Disseminate the YELLOW advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning / Alerting Notification List.
Y-2	C	L	Continue, or introduce all measures listed in Threatcon BLUE Advisory.
Y-3	C	L	Provide weekly briefings to EOC staff, government officials, and first responders regarding the current threat advisory level and local implications.
Y-4	C	L	Implement critical infrastructure facility security plans. (See Security Recommendations)
Y-5	C	L	Brief and stress information and operational security issues to first responders and government officials.

Y-6	C	L	Share pertinent information directly related to the threat level with first responders and government officials.
Y-7	C	L	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	L	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	L	Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (hazmat, TRS, SWAT, bomb squad, command post, etc.)
Y-10	C	L	Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items.
Y-11	C	L	Check recall roster and recall processes for accuracy. Review vacation / day off roster and consider staffing options if the situation escalates.
Y-12	C	L	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	L	Meet with appropriate representatives of critical infrastructure facilities to review contingency and evacuation plans and brief employees.
Y-14	C	L	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	L	Review all plans, orders, SOPs / SOGs, personnel details, and logistical requirements related to the introduction of a higher threat level.
Y-16	C	L	Check inventories of critical supplies and re-order if necessary
Y-17	C	L	Be alert to suspicious activity and report it to the proper authorities.

SECURITY RECOMMENDATIONS / CONSIDERATIONS

Number	Recommended Action
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 chasis 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.

THREAT CONDITION ORANGE

High Risk Of Terrorist Attack Within The State of Illinois

INITIATING EVENT:

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

FEDERAL 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.

STATE GOVERNMENT ACTIONS

- Regular business hours staffing of State Emergency Operations Center by all agencies
- 24-hour on-call duty officers from state 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 / LOCAL ACTIONS:

Action Number	Applicable To:		Recommended Action:
O-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.
O-1		L	Disseminate the ORANGE advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning / Alerting Notification List.
O-2	C	L	Continue, or introduce all measures listed in Threatcon YELLOW Advisory.
O-3	C	L	Activate the jurisdiction's Emergency Operations Center (EOC) for an initial situation briefing of EOC staff and government officials. Following the initial briefing maintain limited staffing, as warranted and appropriate.

O-4	C	L	Provide a daily briefing to EOC staff and government officials.
O-5	C	L	Place all emergency management and specialized response teams on full alert status
O-6	C	L	If not already accomplished, implement critical infrastructure facility security plans (See Security Recommendations)
O-7	C	L	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.
O-8	C	L	Advise staff of contingency plans for shift modifications, assignments, work / rest cycles and family member care / assistance and security plans if the situation escalates.
O-9	C	L	Activate the jurisdiction's Emergency Public Information System. Coordinate information releases with municipal, county, and state governments, if possible.[1]
O-10	C	L	Test communications and warning systems to ensure operability.
O-11	C	L	Ensure personal protective equipment (PPE) and specialized response equipment is checked, issued, and readily available for deployment.
O-12	C	L	Suspend public tours of critical infrastructure facilities.
O-13	C	L	Limit access to computer facilities. No outside visitors.
O-14	C	L	Increase staffing to monitor computer and network intrusion detection systems and security monitoring systems.
O-15	C	L	Ensure the availability of sufficient technical resources to respond to and mitigate a cyber attack.
O-16	C	L	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.
O-17	C	L	Contact critical infrastructure facilities including: businesses, high-profile individuals, schools, hospitals, etc. to discuss the heightened threat and security and contingency operations.
O-18	C	L	Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment. (hazmat, TRS, SWAT, bomb squad, command post, generators, etc.)
O-19	C	L	Consider off-site mail / package processing and sorting facility to reduce the threat to government employees.
O-20	C	L	Review all plans, orders, SOPs / SOGs, personnel details, and logistical requirements related to the introduction of a higher threat level.
O-21	C	L	Check inventories of critical supplies and re-order if necessary.
O-22	C	L	Be alert to suspicious activity and report it to the proper authorities.

SECURITY RECOMMENDATIONS / CONSIDERATIONS

Number	Recommended Action
O-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.
O-6b	Limit access points to critical infrastructure facilities to the absolute minimum, and strictly enforce entry control procedures.

[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

O-6c	Enforce parking of vehicles away from sensitive buildings.
O-6d	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.
O-6e	Identify and protect all designated vulnerable points. Give special attention to vulnerable points outside of the critical facility.
O-6f	Erect barriers and obstacles to control the flow of traffic, as appropriate.
O-6g	Coordinate closing public roads and facilities that might make critical facilities more vulnerable to attack.
O-6h	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.
O-6i	Keep critical response vehicles in a secure area or in an indoor facility. Keep garage doors closed except for bona fide needs.
O-6j	Increase defensive perimeters around key structures and events.

This page intentionally left blank

THREAT CONDITION
RED

Severe Risk Of Terrorist Attack Within The State of Illinois

INITIATING EVENT:

A WMD terrorism incident has occurred which requires an immediate process to identify, acquire, and plan the use of federal resources to augment state and local authorities in response to limited or major consequences of a terrorist use or employment of WMD.

FEDERAL 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
  - Closing public and governmental facilities
  - Increasing or redirecting personnel to address critical emergency needs

STATE GOVERNMENT ACTIONS:

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

COUNTY / LOCAL 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.

Action Number	Applicable To:		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		L	Disseminate the RED advisory to municipal departments, municipal government officials, and special facilities identified on the municipal Warning / Alerting Notification List.
R-2	C	L	Continue, or introduce all measures listed in Threatcon ORANGE Advisory.
R-3	C	L	In the absence of a state "Declaration of Disaster", consider a local declaration to authorize activation of the local emergency management system.
R-4	C	L	Staff Emergency Operations Center (EOC) or Command Post on a 24-hour basis. Provide security for this facility.
R-5	C	L	Maintain and monitor communications and warning systems and provide periodic operational status reports to next higher level of government.
R-6	C	L	Implement appropriate staff recall / staffing plans. Keep all personnel responsible for implementing anti-terrorist plans at their places of duty.
R-7	C	L	If not already accomplished, implement critical infrastructure security plans. (See Security Recommendations)
R-8	C	L	Consider releasing non-critical function personnel.
R-9	C	L	Ensure 24-hour access to the jurisdiction's Principal Executive Officer (County Board Chair, Mayor, Village President) or their designated alternate.
R-10	C	L	In not already accomplished, implement the Emergency Public Information System.[2]
R-11	C	L	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	L	Ensure welfare checks of government personnel and facilities throughout the day and night.
R-13	C	L	Activate, or place on high alert specialized response teams / personnel. (i.e.: hazmat, TRS, EMS, SWAT, Crisis Counseling, etc.)
R-14	C	L	Be prepared to control access routes serving critical infrastructure facilities and evacuation routes.
R-15	C	L	Increase security at water treatment facilities and increase the frequency of testing for impurities and contaminants.
R-16	C	L	Maintain communications with, and provide security for hospitals and critical medical facilities, if appropriate.
R-17	C	L	Stress the possibility of a secondary attack against first responders.

SECURITY RECOMMENDATIONS / CONSIDERATIONS

Number	Recommended Action
R-7a	Make a positive identification of all vehicles located or operating within operational or mission support 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.

[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.

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 faciliteis 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.

This page intentionally left blank

SAMPLE WARNING / ALERTING NOTIFICATION LIST

DATE		THREAT ADVISORY LEVEL	

NOTIFY	PHONE NUMBER	TIME NOTIFIED	PERSON CONTACTED	OPERATOR INITIALS
County Government				
County Board Chair				
Sheriff				
Emergency Management				
Highway Department				
Local Government				
Mayor or Village President				
Police Chief				
Fire Chief				
Emergency Management				
Critical Facilities				
Schools				
Hospitals				
Day Care				

This page intentionally left blank