

THREAT CONDITION ORANGE

High Risk of Terrorist Attack within the State of Ohio

FEDERAL GOVERNMENT ACTIONS: A High Condition is declared when there is a high risk of terrorist attacks. In addition to the measures taken in the previous threat conditions, federal departments and agencies will consider the following protective measures:

- Coordinate necessary security efforts with federal, state, and local law enforcement agencies, National Guard or other security and armed forces;
- Take additional precautions at public events, possibly considering alternative venues or even cancellation;
- Prepare to execute contingency procedures, such as moving to an alternate site or dispersing the workforce; and
- Restrict access to a threatened facility to essential personnel only.

AUTOMATIC STATE GOVERNMENT ACTIONS: In addition to the measures taken in the previous threat conditions, the State of Ohio will take the following default actions.

- The state of Ohio will change threat levels automatically when changes to national threat conditions are announced by the federal government.
- The chair of the State of Ohio Security Task Force will convene the Task Force to consider incident related changes to threat levels and make recommendation to the Governor to downgrade or upgrade independent of federal actions as appropriate.
- The State Emergency Operations Center will be partially activated to facilitate and coordinate information with lead federal and local agencies of supporting state agencies as dictated by the circumstances.
- The State of Ohio EOC will provide daily briefings and/or situation reports.
- The Ohio State Highway Patrol will coordinate with the FBI and other lead federal law enforcement agencies, as well as applicable state and local agencies.
- The Ohio Emergency Management Agency will coordinate with the Federal Emergency Management Agency and with local governments via county EMAs.
- The Ohio Emergency Management Agency will establish contact with the Coordinating Center for Homeland Security.

In addition to the above, departments and agencies will consider the following actions:

Action Number	Action:
O-1	Notify government officials of the increased threat condition.
O-2	Continue, or introduce all measures listed in the Ohio Homeland Security Alert Level Action Plan YELLOW.
O-3	Consider activating 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	Provide a daily briefing to EOC staff and government officials.
O-5	Place all emergency management and specialized response teams on full alert status.
O-6	If not already accomplished, implement critical infrastructure facility security plans. * See O-6a through O-6k for detailed recommended actions.
O-7	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	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	Consider activating the jurisdiction's Emergency Public Information System. Coordinate information releases with municipal, county, and state governments if possible. ¹
O-10	Test communications and warning systems to ensure operability.
O-11	Ensure personal protective equipment (PPE) and specialized response equipment is checked, issued, and readily available for deployment.
O-12	Review policy and plans relating to restricting access to critical facilities and infrastructure.
O-13	Consider limiting access to computer facilities.
O-14	Increase staffing to monitor computer and network intrusion detection systems and security monitoring systems.
O-15	Ensure the availability of sufficient technical resources to respond to and mitigate a cyber attack.
O-16	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	Contact critical infrastructure facilities including businesses, high-profile individuals, schools, hospitals, etc. to discuss the heightened threat and security and contingency operations.

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-18	Check all equipment for operational readiness, fill fuel tanks, and check specialized response equipment. (Hazmat, TRS, SWAT, bomb squad, command post, generators, etc.)
O-19	Consider off-site mail / package processing and sorting facility to reduce the threat to government employees.
O-20	Review all plans, orders, SOPs / SOGs, personnel details, and logistical requirements related to the introduction of a higher threat level.
O-21	Check inventories of critical supplies and re-order if necessary.
O-22	Be alert to suspicious activity and report it to the proper authorities.
O-23	Instruct all citizens to report suspicious activities, packages and people to law enforcement.
O-24	Encourage personnel to avoid routines, vary times and preplan with family members and supervisors.

SECURITY RECOMMENDATIONS

*O-6 Facility Security Plans - Actions For Consideration:	
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.
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 entrances(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 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	Implement stringent identification procedures to include "hands-on" checks of security badges for all personnel.
O-6j	Keep critical response vehicles in a secure area or in an indoor facility. Keep garage doors closed except for bona fide needs.
O-6k	Increase defensive perimeters around key structures and events.

THREAT CONDITION RED

Severe Risk of Terrorist Attack within the State of Ohio

FEDERAL GOVERNMENT ACTIONS: Severe Condition (Red). A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time.

In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:

1. Increasing or redirecting personnel to address critical emergency needs;
2. Assigning emergency response personnel, pre-positioning, and mobilizing specially trained teams or resources;
3. Monitoring, redirecting, or constraining transportation systems; and
4. Closing public and government facilities.

AUTOMATIC STATE GOVERNMENT ACTIONS:

- Change Alert Level to RED based on the Federal level.
- OSHP and other response organizations cancel all leave, vacation, training, schools and travel to maximize staffing levels.
- Activate the Joint Information Center (JIC).
- Initiate armed security of state EOC.
- Staff the state Emergency Operations Center (EOC) with all response agencies and state agencies plus FEMA, FBI, and other local / federal agencies.
- Convene the State Of Ohio Security Task Force (SOS TF).
- Governor will consider calling a full cabinet meeting.
- Activate selected National Guard units to provide immediate response capability.
- 52nd Weapons of Mass Destruction Civil Support Team (WMD CST) will report to Rickenbacker Air Base.
- If the event threatens or actually impacts the State, Governor will consider issuing an emergency declaration.

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 a significant personnel and economic considerations.

Action Number	Actions
R-1	Notify government officials of the increased threat condition.
R-2	Continue, or introduce all measures listed in the Ohio Homeland Security Alert Level Action Plan ORANGE.
R-3	Consider the necessity for initiating assistance or submitting support requests in accordance with the Emergency Management Assistance Compact (EMAC) or the Intrastate Mutual Aid Compact (IMAC) considerations.
R-3	In the absence of a state “Declaration of Disaster”, consider a local declaration to authorize activation of the local emergency management system.
R-4	Staff Emergency Operations Center (EOC) or Command Post on a 24-hour basis. Partial or full activation are dependent on the extent and severity of the situation. Provide armed security for this facility.
R-5	Maintain and monitor communications and warning systems and provide periodic operational status reports to next higher level of government.
R-6	Implement appropriate staff recall / staffing plans. Keep all personnel responsible for implementing anti-terrorist plans at their places of duty.
R-7	If not already accomplished, implement critical infrastructure security plans. <i>*R-7a through R-7h have detailed recommended actions.</i>
R-8	Consider releasing non-critical function personnel.
R-9	Ensure 24-hour access to the jurisdiction’s Principal Executive Officer (County Board, Chair, Mayor, Village President) or their designated alternate.
R-10	If not already accomplished, implement the Emergency Public Information System. ²
R-11	Brief all EOC, government and first response personnel on critical facility evacuation routes and contingency communications plans, as applicable. Provide direction regarding what equipment, supplies should be taken in the event of an evacuation.
R-12	Ensure welfare checks of government personnel and critical facilities throughout the day and night.
R-13	Activate, or place on high alert specialized response teams / personnel. (i.e.: hazmat, TRS, EMS, SWAT Crisis Counseling, etc.)
R-14	Be prepared to go to controlled access routes serving critical infrastructure facilities and evacuation routes.
R-15	Consider increasing security at water treatment facilities and increase the frequency of testing for impurities and contaminants.
R-16	Maintain communications with, and provide security for hospitals and critical medical facilities, if appropriate.
R-17	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.

R-18	Consider relocating government workers to alternate work site.
------	--

SECURITY RECOMMENDATIONS

*R-7 Facility Security Plans - Actions For Consideration:	
R-7a	Consider making 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 areas.
R-7c	Control access and implement positive identification of all personnel within operational or mission support areas – no exceptions.
R-7d	Search all suitcases, 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 critical facility 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. No deliveries should be opened inside of the critical facility, and minimal personnel should be in the immediate area when packages are opened.