KENTUCKY HOSPITAL ASSOCIATION
HOMELAND SECURITY ADVISORY SYSTEM
GUIDELINES

BACKGROUND

The Nation requires a Homeland Security Advisory System to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. Such a system provides warnings in the form of a set of graduated "Threat Conditions" that increase as the risk of the threat increases. At each Threat Condition, Federal departments and agencies implement a corresponding set of "Protective Measures" to further reduce vulnerability or increase response capability during a period of heightened alert. The primary focus is on PREVENTION – to deter, detect, deny, defend and defeat.
This system is intended to create a common vocabulary, context, and structure for an ongoing national discussion about the nature of the threats that confront the homeland and the appropriate measures that should be taken in response. It seeks to inform and facilitate decisions appropriate to different levels of government and to private citizens at home and at work.

There are five Threat Conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

1. **Low Condition (Green)**. This condition is declared when there is a low risk of terrorist attacks. Consider the following general measures in addition to the agency-specific Protective Measures they develop and implement:
    1. Refining and exercising as appropriate preplanned Protective Measures;
    2. Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and
    3. Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

2. **Guarded Condition (Blue)**. This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
    1. Checking communications with designated emergency response or command locations;
    2. Reviewing and updating emergency response procedures; and
    3. Providing the public with any information that would strengthen its ability to act appropriately.

3. **Elevated Condition (Yellow)**. An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, consider the following general measures in addition to the Protective Measures that they will develop and implement:
    1. Increasing surveillance of critical locations;
    2. Coordinating emergency plans as appropriate with nearby jurisdictions;
    3. Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and
    4. Implementing, as appropriate, contingency and emergency response plans.

4. **High Condition (Orange)**. A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, consider the following general measures in addition to the agency-specific Protective Measures that they will develop and implement:
    1. Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
    2. Taking additional precautions at public events and possibly considering alternative venues or even cancellation;
    3. Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
    4. Restricting threatened facility access to essential personnel only.

5. **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, 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 and pre-positioning and mobilizing specially trained teams or resources;
    3. Monitoring, redirecting, or constraining transportation systems; and
    4. Closing facilities.

The higher the Threat Condition, the greater the risk of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat Conditions shall be assigned by the Attorney General in consultation with the Director of Homeland Security on a national basis. Threat Conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector. Assigned Threat Conditions shall be reviewed at regular intervals to determine whether adjustments are warranted.

KENTUCKY

In Kentucky Threat Conditions may be assigned by the Governor for statewide alerts, the County Judge Executives for countywide threats, and the Mayor for citywide threats. The assignment of a Threat Condition shall prompt the implementation of an appropriate set of Protective Measures. Protective Measures are the specific steps an organization shall take to reduce its vulnerability or increase its ability to respond during a period of heightened alert.

The decision whether to publicly announce Threat Conditions shall be made on a case-by-case basis.

A decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

1. To what degree is the threat information credible?
2. To what degree is the threat information corroborated?
3. To what degree is the threat specific and/or imminent?
4. How grave are the potential consequences of the threat?

SUGGESTED ACTIONS

What follows are suggested actions to be taken by various organizations/entities if the Governor, County Judge Executive or Mayor increases the Threat Condition to a high condition (orange) or severe condition (red).

The first step is for law enforcement to conduct a threat assessment to identify and evaluate potential threats on the basis of such factors as capabilities, intentions, past activities, current intentions and specific targeting. Additionally, specific threat information must be assessed by its credibility, corroboration, specificity, imminence and gravity.

Next, organizations must do a criticality assessment to determine what is to be protected (people, equipment, capabilities, services, production levels, etc.) and prioritize by significance if lost. Also consider the level of visibility, value of target, hazards – if attacked, population capacity and collateral mass casualties prioritized by loss of life or injuries; economic loss: national, state, regional, etc.; effect on U.S. defense capabilities, and political or social impact.

Then, assess vulnerabilities of the above and develop protective measures in such areas as structural engineering, physical security, operational security, information security, blast physics and personnel assurance.
When developing protective measures consider the three-ring strategy. The inner ring is the target, the middle ring is for defense and the outer ring is to detect and deter.

Also, consider the means of threat delivery including plane, motorcycle, train, car, truck, bus, boat, subway, animals, package, sewer, individual(s), utility line, heating or air conditioning system and balloons.

There are seven security categories to be considered including physical security, operational security (human interaction with information), information and cyber security, personnel assurance, personal protection, information operations, other planning concerns and issues.

PHYSICAL SECURITY

Regarding physical security, consider credentials, searches (routine and random), inspections and access control for at least employees, contractors, vendors, visitors and media, including their vehicles and equipment. The use of barriers (multiple types and styles) should be considered internally and externally to buildings.

Other areas of concern include parking and traffic control; random patrols; security and screening for mail, deliveries, uniforms, vehicles, weapons, equipment, food and water, ventilation systems, communications and computer systems, blueprints, underground tunnels and pipelines, alarms, detection and lighting systems; access areas; electronic surveillance; lock and key control; line of sight restrictions and removal of vegetation and other visibility restrictions.

Consider the use of armed guards, rules of engagement for use of force, identification of friendly forces, quick response teams, access and checkpoints, restricted areas, reporting procedures and training.

OPERATIONAL SECURITY

Regarding operational security (human interaction with information), consider limits on the use and control of computers and access to the Internet; locations and attendance for meetings, conferences, etc.; telephones, tape recorders, wireless devices, fax machines, copiers, scanners, etc.; trash and old documents, draft working documents, media releases; photography of the facility (inside and out); work at home projects; routes; access; breach of security reporting and training.

INFORMATION SECURITY

Regarding information security, consider protecting criticality assessments, critical program information and records, critical technologies, contingency plans, standard operating procedures, intellectual property, proprietary information, activity schedules and timelines, recovery capabilities and their timelines, alert procedures, breach of security reporting and training.

PERSONNEL ASSURANCE

Regarding personnel assurance consider background investigations, continuous evaluation programs, drug and polygraph testing. Consider reporting policies concerning foreign context, travel (foreign and domestic), suspicious requests, personal changes and/or problems, personal financial reporting, standards of conduct and ethics, counter-intelligence surveillance, breach of security reporting and training.

PERSONAL PROTECTION

Regarding personal protection consider individual protective equipment; detectors and sensors for food and water sources, heating and air conditioning, mail, packages and all deliverables; personal health precautions such as regular medical evaluations, updated immunizations, mental health screening, support groups to assist families; prepositioning of vaccines and/or medications; training exercises to test plans for emergency immunization, evacuation, bomb threats, shelter in place and decontamination; personal and family emergency preparedness action for homes; frequent changes in patterns and schedules; alternate use of entry and exits.

INFORMATION OPERATIONS

Regarding information operations, consider establishment of a joint information center to control media releases and interviews. Targeted information should be directed at public announcements; employees and their families; contractors and vendors; community leadership; law enforcement; fire service; emergency medical services; public works; medical, religious and business leaders; schools and volunteer organizations. There should be established procedures for reporting suspicious activity; dead or sick animals; unexplained/unusual orders, fluids, droplets, mists or clouds; unusual/unscheduled spraying or discovery of spray devices; human health issues and concerns. Consider the method(s) to use including print, radio, TV, meetings, Internet.

OTHER PLANNING CONCERNS AND ISSUES

Regarding other planning concerns and issues, consider incident command/unified command procedures pre-event; identification and marking of functions and individuals; interoperable/integrated communications; internal flow of information, intelligence and warnings; location of the command post, logistics support area, life support area, communication centers; establishment of priorities of work; staff meeting requirements, recall procedures, vacation and time off policies and off-site support requirements; examination of legal issues; accounting and expense training; business and travel arrangements; management of VIP visits; disbursal of work force; reexamination of job descriptions, duties and responsibilities; sustainment of operations; prepositioning of supplies and equipment; planning for civil disturbance, inclement weather, bomb threats, hostage barricade, “white powder” incidents; frequent review of threat assessment; and exercises.

The desired outcomes are to maintain economic viability and growth including revenues and jobs and assurance of critical services, public health and safety, public confidence and morale, and local continuity of government.

CHECKLIST

Some specific things to consider are indicated below. However, organizations must develop their own plans based on the suggestions already provided.

Level	Emergency Department	Laboratory	Pharmacy	Public Safety	Other Departments	Administration
GREEN	Review implications, roles and responsibilities for each individual. Perform monthly assessment/inventory of decontamination area/supplies/personal protection equipment (PPE). Be alert for trends in patient symptoms. Ensure telephone numbers for local and state health departments AND resource hospital are readily available and current. Ensure that in-house call tree is current. Develop staffing modification plans, including rest cycles and provision of family member care. Perform and document weekly radio	Identify level capabilities of laboratory (Level A B Level D) Arrange for contracted laboratory to provide specimen testing beyond facility's capabilities. Arrange for transport of specimens and for education of transporters on safe transport of specimens. Ensure call tree is current. Develop staffing modification plans, including rest cycles and provision of family member care. Be alert for trends in culture/test ordering. Report concerns to appropriate personnel. Report suspicious	Ensure call tree is current. Develop staffing modification plans, including rest cycles and provision of family member care. Report suspicious circumstances and/or individuals to appropriate person.	Ensure call tree is current. Develop staffing modification plans, including rest cycles and provision of family member care. Continue common sense practices in daily security routines. Report suspicious circumstances and/or individuals to appropriate person.	Ensure call tree is current. Develop staffing modification plans, including rest cycles and provision of family member care. Report suspicious circumstances and/or individuals to appropriate person.	Provide training or refresher courses for all hospital staff on color-coding system. Ensure call tree is current. Develop staffing modification plans, including rest cycles and provision of family member care. Review hospital and state disaster plans. Have public relations or public safety staff monitor news information stations for change in Threat Con. Have a "basic" unified public information (PI) message available to an "all –hazards" approach. Provide PI seminars to key personnel within the institution. Ensure telephone numbers for local and state health departments AND resource hospital are readily available and current.

🟩	checks. Report suspicious circumstances and/or individuals to appropriate person.	circumstances and/or individuals to appropriate person.				Report suspicious circumstances and/or individuals to appropriate person.
BLUE	Continue all measures as outlined in Green Threat Con. Alert appropriate staff to heightened Threat Con. Check all equipment for operational readiness. Review disaster preparedness protocols for department. Review call tree and staff modification plan. Inventory emergency disaster medical bags. Check expiration dates and completeness of bags. Check that all disaster related paper work is	Continue all measures as outlined in Green Threat Con. Alert appropriate staff to heightened Threat Con. Review disaster preparedness protocols specific to department. Ensure the laboratory is secure. Review call tree and staff modification plan. Be alert for trends in patient culture/testing patterns. Inform appropriate personnel if suspicious patterns noted. Check all equipment for operational readiness.	Continue all measures as outlined in Green Threat Con. Alert appropriate staff to heightened Threat Con. Review disaster preparedness protocols specific to department. Ensure the pharmacy is secure. Review call tree and staff modification plan. Inventory antidotes/ medications levels. Note expiration dates. Check all equipment for operational readiness.	Continue all measures as outlined in Green Threat Con. Alert appropriate staff to heightened Threat Con. Review disaster preparedness protocols specific to department. Implement security plans appropriate to the facility (e.g., monitoring of entrances/exits, including those in professional office buildings). Prohibit casual access by unauthorized personnel. Ensure all vehicles are secured. Check all equipment for operational	Continue all measures as outlined in Green Threat Con. Check all equipment for operational readiness. Alert appropriate staff to heightened Threat Con. Review disaster preparedness protocols specific to department. Ensure the department is secure. Review the call tree and staff modification plan.	Assign staff person to watch for faxes/E-mails/ correspondence. Continue all measures as outlined in Green Threat Con. Alert all departments, including medical staff, to heightened Threat Con. Review disaster preparedness protocols specific to department. Ensure the department is secure. Review call tree and staff modification plan. Check all equipment for operational readiness. Test group page capabilities with Threat Con status. Have public relations and public safety staff monitor news information

	available. Duplicate as necessary Assess communications readiness (radios, walkie-talkies and other redundant communication systems). Inventory decontamination area supplies and equipment, including PPE. Be alert for trends in patient symptoms.			readiness.		stations (CNN, MSNBC) for change in Threat Con. Refresh key personnel on media protocols. Provide media training for all key personnel (e.g., ED physicians, charge nurses, EMS coordinator, nursing supervisor). Conduct tabletop exercises for key personnel.
YELLOW	Continue all measures as outlined in Green and Blue Threat Con. Consider alternative work schedules for staff if condition escalates. Review hospital and state disaster plans with all shifts. Inventory available internal resources (beds, pharmacy stock, laboratory supplies, ancillary services) daily. Perform disaster call tree drill, including color	Continue all measures as outlined in Green and Blue and Threat Con. Ensure all staff is alerted to the heightened Threat Con. Review emergency plans for this color condition with all shifts. Consider alternative work schedules for operational staff if condition escalates. Check inventory of critical supplies; reorder if	Continue all measures as outlined in Green and Blue Threat Con. Ensure all staff is alerted to the heightened Threat Con. Review emergency plans for this color condition with all shifts. Consider alternative work schedules for operational staff if condition escalates. Check inventory of critical antidotes/ medications;	Continue all measures as outlined in Green and Blue Threat Con. Ensure all staff is alerted to the heightened Threat Con. Review emergency plans for this color condition with all shifts. Remind all hospital staff to be suspicious and inquisitive and to maintain heightened awareness of people, vehicles and activities. Ensure call tree is available and	Continue all measures as outlined in Green and Blue Threat Con. Ensure all staff is alerted to the heightened Threat Con. Review emergency plans for this color condition with all shifts. Consider alternative work schedules for operational staff if condition escalates. Check inventory of critical supplies; reorder if necessary.	Continue all measures as outlined in Green and Blue Threat Con. Ensure all staff, including medical staff, is alerted to the heightened Threat Con. Review emergency plans for this color condition with all shifts. Consider alternative work schedules for operational staff if condition escalates. Review hospital and state disaster plans. Review incident command structure and command

	alert in call. Review disaster related paperwork. Ensure it is readily assessable. Ensure decontamination area is operational. Ensure the emergency medical disaster bags are readily available.	necessary.	reorder if necessary.	current. Consider alternative work schedules for operational staff if condition escalates. Increase spot checks of specific high-risk entrances/exits (e.g., loading docks, professional office buildings). Document security checks. Do not leave vehicles unattended and unlocked. Move vehicles and objects (trash containers, etc.) away from the building. Lock and regularly inspect all buildings, rooms and storage areas not in regular use. At the beginning and end of each shift, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings for suspicious packages.		center operations. Ensure communications equipment, including telephone numbers of governmental agencies, is available and operational. Instruct telecommunications staff to complete a group page with color alert system and document response times. Inventory available internal resources (beds, pharmacy supplies, laboratory capabilities, ancillary services). Evaluate elective admissions and determine need to cancel elective admissions. Review media protocols and have public relations staff monitor news information stations continuously for change in Threat Con. Be aware of large-scale community events (sporting events, concerts, etc.). Consult with law enforcement officials/emergency medicine/IDPH on message to be disseminated. Ensure that all key personnel have same message (cue cards, talking points, etc.). Assign person on

🟨						each shift to be media representative.
ORANGE	Continue all measures as outlined in Green, Blue and Yellow Threat Con. Ensure all staff is alerted to heightened Threat Con. Ready decontamination area equipment and supplies. Ensure PPE is available for all staff. Inventory categories on disaster form (bed/ blood availability, availability of medical teams/bags). Audit internal resource availability (e.g., beds/monitored beds, blood supply, antibiotic/IV supply, ventilator supply, linen supply, food/water supply). Ensure security of emergency department. Activate call tree; place staff on full alert status. Advise staff of	Continue all measures as outlined in Green, Blue and Yellow Threat Con. Ensure all staff is alerted to heightened Threat Con. Ensure security of laboratory. Activate call tree; place staff on full alert status. Advise staff of shift modifications if plan escalates. Ensure that PPE and specialized response equipment and supplies are checked and readily available.	Continue all measures as outlined in Green, Blue and Yellow Threat Con. Ensure all staff is alerted to heightened Threat Con. Activate call tree; place staff on full alert status. Advise staff of shift modifications if plan escalates.	Continue all measures as outlined in Green, Blue and Yellow Threat Con. Ensure all staff is alerted to heightened Threat Con. Activate call tree; place staff on full alert status Advise staff of shift modifications if plan escalates. At the beginning and end of each shift, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings for suspicious packages. Limit access points to the absolute minimum and strictly enforce entry control procedures. Enforce parking of vehicles away from main hospital buildings. Identify and	Continue all measures as outlined in Green, Blue and Yellow Threat Con. Ensure all staff is alerted to heightened Threat Con. Activate call tree; place staff on full alert status. Advise staff of shift modifications if plan escalates.	Continue all measures as outlined in Green, Blue and Yellow Threat Con. Ensure all staff is alerted to heightened Threat Con. Consider activation of facility disaster preparedness plan. Have the IC sheets available Assess readiness of the command center Activate call tree; place staff on full alert status. Advise staff of shift modifications if plan escalates. Check all telecommunications equipment for operational readiness. Review transfer agreements in anticipation of patient transfer to other appropriate facilities. Contact private providers with Threat Con Alert for possible rapid evacuation of patients to other facilities. Test all internal communications

	shift modifications if plan escalates. Check equipment and supplies at patient care/treatment locations as outlined in facility internal disaster plan (professional office buildings, outpatient departments, etc.). Be alert for trends in patient symptoms. Notify appropriate person if trends noted. Be alert for increase in ambulance transport times. Check inventory of critical supplies; restock if necessary.			protect all designated vulnerable points. Lock all exterior doors except the main facility entrance(s). Check identification of all visitors. Require a sign-in log with information from each visitor's identification. Increase defensive perimeters around key structures.		and warning systems. Alert CFO to begin collecting expense data (personnel, equipment, supplies, transfer costs) related to Threat Con Alert.
RED	Continue all measures as outlined in Green, Blue, Yellow and Orange Threat Con. At each shift change report current status of each department. Ensure all staff is alerted to the heightened Threat Con.	Continue all measures as outlined in Green, Blue, Yellow and Orange Threat Con. Ensure all staff is alerted to the heightened Threat Con. Activate call tree. Secure as many additional staff as necessary. Advise staff of	Continue all measures as outlined in Green, Blue, Yellow and Orange Threat Con. Ensure all staff is alerted to the heightened Threat Con. Activate call tree. Secure	Continue all measures as outlined in Green, Blue, Yellow and Orange Threat Con. Ensure all staff is alerted to the heightened Threat Con. Implement parking restrictions and park vehicles away from	Continue all measures as outlined in Green, Blue, Yellow and Orange Threat Con. Ensure all staff is alerted to the heightened Threat Con. Activate call tree. Secure as many additional staff as necessary. Advise staff of	Continue all measures as outlined in Green, Blue, Yellow and Orange Threat Con. Ensure that all staff is alerted to the heightened Threat Con. Activate facility disaster preparedness plan. Open up the hospital incident

🟥	Activate full ED command center if applicable Activate call tree. Secure as many additional staff as necessary. Advise staff of schedule modifications. Maintain communication with hospital command post. Have disaster paperwork in order. Activate decontamination area, including supplies and PPE. Have medical bags ready for deployment.	schedule modifications. Maintain communication with hospital command post. Ensure critical supplies are available. Ensure that PPE and specialized response equipment and supplies are available. Check all equipment for operational readiness. Alert contracted lab of Threat Con Red Alert and the possibility that specimens may be sent to them.	as many additional staff as necessary. Advise staff of schedule modifications. Maintain communication with hospital command post. Ensure critical antidotes/ medications are available for staff and patients.	facility. Place traffic and pedestrian barriers in place. Put up signage indicating patient treatment areas, information area, family area, etc. Control access and implement positive identification of all persons - no exceptions. Search all suitcases, brief cases, packages, etc., brought into the facility. Secure all doors. Maintain a security presence at a single point of access to each building and check identification of all visitors. Maintain a sign-in log. Check all bags, suitcases, brief cases and packages at the security point. Increase defensive perimeters around facility. Make frequent checks of the exterior. Deliveries	schedule modifications. Maintain communication with hospital command post. Ensure critical antidotes/ medications are available for staff and patients. Check all equipment for operational readiness.	command center Activate call tree. Secure as many additional staff as necessary. Advise staff of schedule modifications. Provide for day care/child care facilities for staff responding to Threat Con Red Alert. Arrange for food service to provide meals to staff.

				should not be accepted unless approved by supervisory staff. All deliveries are to be opened outside the facility and minimal personnel should be in the immediate area when deliveries are opened.		

Family Preparedness

- Create an emergency communications plan.
- Establish a meeting place.
- Assemble a disaster supplies kit.
- Replace stored food and water every six months.
- Check on the school emergency plan.
- Contact school/business to determine status of the school/work day.
- Listen to radio/TV and monitor the Internet for information/instructions.
- Be alert to suspicious activity and report it to property authorities immediately.
- Discuss childrens' fears concerning possible/actual terrorist attacks.
- Exercise caution when traveling.
- Keep copies of important documents in a watertight, fireproof container.
- Teach family members how to shut off utilities in the home.
- Make arrangements for pets.
- Post emergency telephone numbers and teach children how and when to call 911.
- Locate safe places in your home for each type of disaster and determine the best escape routes.
- Test and recharge fire extinguishers according to manufacturer's instructions.
- Test smoke detectors monthly and replace batteries annually.
- Coordinate plans with neighbors.
- Establish a household rule: only a responsible adult may open an outside door to a visitor.
- Ensure that adults know how to call the utility company to verify utility workers' identities before permitting their entry.
- Cut back the shrubbery from blocking windows.
- Put good locks on all doors and windows.
- Put up additional exterior lighting and a peephole.
- Display "guard dog", "security", or "alarm service" warning signs.

5/1/03