

Learn “Threat Levels” - Review below **Homeland Security Advisory System** to see what your family or business should do at each color.

Know the targets - Terrorists usually prefer to pick targets that bring little damage to themselves and areas that are easy to access by the public (like international airports, military and government buildings, major events, schools, malls, etc.) Some other high risk targets include water and food supplies, nuclear power plants, and high-profile landmarks.

Things to watch out for:

- **unknown packages** - DO NOT accept a package or case from a stranger
- **unattended bags** - report unattended bags or backpacks to authorities and don't ask strangers to watch your stuff or leave bags or purses alone (esp. when traveling)
- **emergency exits** - always be aware of where EXITS are... just casually look around for signs since most are marked well in public places

Make a plan - Review Section 1 to develop a **Family Emergency Plan** and **Disaster Supplies Kit**. And Appendix B has plans & tips for **businesses**.

Get involved - Join a local Citizen Corps or CERT. (*see pages 222-224*)

ABOUT THE HOMELAND SECURITY ADVISORY SYSTEM

In March 2002, the **Homeland Security Advisory System (HSAS)** was implemented using color-coded “Threat Conditions” that increase or decrease based on reports from the Intelligence Community.

HSAS’s “Threat Conditions” or “Threat Levels”:

SEVERE = RED (Severe risk of terrorist attacks)

HIGH = ORANGE (High risk of terrorist attacks)

ELEVATED = YELLOW (Significant risk of terrorist attacks)

GUARDED = BLUE (General risk of terrorist attacks)

LOW = GREEN (Low risk of terrorist attacks)

Alerts and threat conditions can be declared for the entire nation, or for a specific geographic area or industry. The public should stay current with news and alerts issued by officials ... and be aware, be prepared, and have a plan at all threat levels.

The **District of Columbia Homeland Security and Emergency Management Agency (HSEMA)** developed and contributed the following

“Terrorist Threat Advisory System” that mirrors the national Homeland Security Advisory System. The HSEMA’s suggested precautions provide general guidance only to help organizations and families take actions best tailored for their needs. *Please note, there are some protective measures for federal departments and agencies per DHS included here too.*

LOW (Green) - a **low risk** of terrorism. Routine security is implemented to preclude routine criminal threats.

Residents are advised to:

- Continue to enjoy individual freedom. Participate freely in travel, work, and recreational activities.
- Be prepared for disasters and family emergencies.
- Develop a family emergency plan.
- Keep recommended immunizations up-to-date.
- Know how to turn off power, gas, and water service to your house.
- Know what hazardous materials are stored in your home and how to properly dispose of unneeded chemicals.
- Support the efforts of your local emergency responders (fire fighters, law enforcement and emergency medical service).
- Know what natural hazards are prevalent in your area and what measures you can take to protect your family. Be familiar with local natural and technological (man-made) hazards in your community.
- Volunteer to assist and support community emergency response agencies.
- Become active in your local Neighborhood Crime Watch program.
- Take a first aid or Community Emergency Response Team (CERT) class.

Business owners and managers are advised to:

- Develop emergency operations and business contingency plans.
- Encourage and assist employees to be prepared for personal, natural, technological, and homeland security emergencies.
- Conduct emergency preparedness training for employees and their families.
- Develop a communications plan for emergency response and key personnel.
- Conduct training for employees on physical security precautions.
- Budget for physical security measures.

Federal departments and agencies should consider:

- Refine and exercise planned Protective Measures.
- Ensure emergency personnel receive proper training on HSAS measures.
- Assess facilities for vulnerabilities and take measures to mitigate them.

GUARDED (Blue) - a **general risk** of terrorism with no credible threats to specific targets.

In addition to previously mentioned precautions, residents are advised to:

- Continue normal activities but be watchful for suspicious activities. Report suspicious activity to local law enforcement.
- Review family emergency plans.
- Avoid leaving unattended packages or briefcases in public areas.
- Increase family emergency preparedness by purchasing supplies, food, and storing water.
- Increase individual or family emergency preparedness through training, maintaining good physical fitness and health, and storing supplies.
- Monitor local and national news for terrorist alerts.

In addition to all previously mentioned precautions, business owners and managers are advised to:

- Ensure that key leaders are familiar with the emergency operations and business contingency plans.
- Review, update, and routinely exercise functional areas of plans.
- Review and update the call down list for emergency response teams.
- Develop or review Mutual Aid agreements with other facilities and/or with local government for use during emergencies.
- Review physical security precautions to prevent theft, unauthorized entry, or destruction of property.
- Have you provided for:
 - Employee picture ID badges?
 - Background checks on all employees (as applicable)?
 - Access control and locking of high security areas at all times?
 - All security keys marked with "Do not Duplicate"?
 - Surveillance Cameras?
 - Backup power?
 - An alarm system?

In addition to all previously mentioned precautions, federal departments and agencies should consider:

- Check communications with designated emergency response or command locations.
- Review and update emergency response procedures.
- Provide public with information that would strengthen its ability to act appropriately.

ELEVATED (Yellow) - an **elevated risk** of terrorist attack but a specific region of the USA or target has not been identified.

In addition to previously mentioned precautions, residents are advised to:

- Continue normal activities, but report suspicious activities to the local law enforcement agencies.
- Network with your family, neighbors, and community for mutual support during a disaster or terrorist attack.
- Learn what critical facilities are located in your community and report suspicious activities at or near these sites.
- Contact local officials to learn about specific hazards in community.
- Develop a family plan and check contents of your **Disaster Supplies Kit** (see *Section 1*). Individual or family emergency preparedness should be maintained through training, good physical fitness and health, and storing food, water, and emergency supplies.
- Monitor media reports concerning situation.

In addition to all previously mentioned precautions, business owners and managers are advised to:

- Announce Threat Condition **ELEVATED** to employees.
- Review vulnerability and threat assessments and revise as needed.
- Identify and monitor government information sharing sources for warnings and alerts.
- Update and test call down list for emergency response teams and key employees.
- Review, coordinate, and update mutual aid agreements with other critical facilities and government agencies.
- Establish and monitor more active security measures.
- Review employee training on security precautions (bomb threat procedures, reporting suspicious packages, activities, and people). Conduct communications checks to ensure contacts can be maintained.

In addition to all previously mentioned precautions, federal departments and agencies should consider:

- Increase surveillance of critical locations.
- Coordinate emergency plans with nearby jurisdictions, as needed.
- Assess whether the precise characteristics of the threat require further refinement of preplanned protective measures.
- Implement, as appropriate, contingency and emergency response plans.

HIGH (Orange) - credible intelligence indicates that there is a **high risk** of a local terrorist attack but a specific target has not been identified.

In addition to previously mentioned precautions, residents are advised to:

- Resume normal activities but expect some delays, baggage searches, and restrictions due to heightened security at public buildings and facilities.
- Continue to monitor world and local events as well as local government threat advisories.
- Report suspicious activities at or near critical facilities to local law enforcement agencies by calling 9-1-1.
- Inventory and organize emergency supply kits and test emergency plans with family members. Reevaluate meeting location based on threat.
- Consider taking reasonable personal security precautions. Be alert to your surroundings, avoid placing yourself in a vulnerable situation, and monitor the activities of your children.
- Maintain close contact with family and neighbors to ensure their safety and emotional welfare.

In addition to all previously mentioned precautions, business owners and managers are advised to:

- Announce Threat Condition **HIGH** to all employees and explain expected actions.
- Place emergency response teams on notice.
- Activate the business emergency operations center if required. Establish ongoing liaison with local law enforcement and emergency management officials.
- Monitor world and local events. Pass on credible threat intelligence to key personnel.
- Ensure appropriate security measures are in place and functioning properly.
- Instruct employees to report suspicious activities, packages, and people.
- Search all personal bags, parcels, and require personnel to pass through magnetometer, if available.
- Inspect intrusion detection systems and lighting, security fencing, and locking systems.
- Inspect all deliveries and consider accepting shipments only at off-site locations.
- Remind employees to expect delays and baggage searches.
- Implement varying security measures (*listed on next page*)

*The following measures incorporate a comprehensive list of security actions, some of which may need to be implemented at lower levels. They are designed to respond to the elevation to **HIGH Risk (Orange)** of terrorist attacks.*

(Orange) Security Measures for Businesses - Little or No Cost Actions

- Increase the visible security personnel presence wherever possible.
- Rearrange exterior vehicle barriers (traffic cones) to alter traffic patterns near facilities.
- Institute / increase vehicle, foot, and roving security patrols.
- Implement random security guard shift changes.
- Arrange for law enforcement vehicles to be parked randomly near entrances and exits.
- Approach all illegally parked vehicles in and around facilities, question drivers and direct them to move immediately. If owner cannot be identified, have vehicle towed by law enforcement.
- Limit number of access points and strictly enforce access control procedures.
- Alter primary entrances and exits if possible.
- Implement stringent identification procedures to include conducting 100% "hands on" checks of security badges for all personnel (if used).
- Remind personnel to properly display badges, if applicable, and enforce visibility.
- Require two forms of photo identification for all visitors.
- Escort all visitors entering and departing.
- X-ray packages and inspect handbags and briefcases at entry if possible.
- Validate vendor lists for all routine deliveries and repair services.

Security Measures for Businesses - Actions That May Bear Some Cost

- Increase perimeter lighting.
- Remove vegetation in and around perimeters, maintain regularly.
- Institute a vehicle inspection program to include checking under the undercarriage of vehicles, under the hood, and in the trunk. Provide vehicle inspection training to security personnel.
- Conduct vulnerability studies focusing on physical security, structural engineering, infrastructure engineering, power, water, and air infiltration, if feasible.
- Initiate a system to enhance mail and package screening procedures (both announced and unannounced).
- Install special locking devices on manhole covers in & around facilities.

(Orange) In addition to all previously mentioned precautions, federal departments and agencies should consider:

- Coordinate 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 cancellation.
- Prepare to work at an alternate site or with a dispersed workforce.
- Restrict access to a threatened facility to essential personnel only.

SEVERE (Red) - terrorist attack has occurred or credible and corroborated intelligence indicates that one is imminent (a **severe risk**). Normally, this threat condition is declared for a specific location or critical facility.

In addition to previously mentioned precautions, residents are advised to:

- Report suspicious activities and call 9-1-1 for immediate response.
- Expect delays, searches of purses and bags, and restricted access to public buildings.
- Expect traffic delays and restrictions.
- Residents should have **Disaster Supplies Kits** stocked and in place ready to go (medicines, glasses, important legal and financial papers) and emergency supplies kits (first aid kits, duct tape, blankets, non-perishable food, water) for sheltering in place, if requested to do so. (*see Section 1*)
- Take personal security precautions to avoid becoming a victim of crime or terrorist attack.
- Avoid participating in crowded optional public gatherings, like sporting events and concerts. However, do not avoid going to public emergency gathering locations such as hospitals and shelters, if directed or necessary. These locations will have developed and initiated a strong security plan to protect the residents.
- Do not travel into areas affected by the attack or that are likely to become an expected terrorist target.
- Keep emergency supplies accessible and automobile fuel tank full.
- Be prepared to either evacuate your home or shelter-in-place on order of local authorities. (*see EVACUATION in Section 2*)
- Be suspicious of persons taking photographs of critical facilities, asking detailed questions about physical security or dressed inappropriately for weather conditions. Report incidents immediately to law enforcement.
- Closely monitor news reports and Emergency Alert System (EAS) radio/TV stations.
- Assist neighbors who may need help.
- Ensure pets can be readied quickly for boarding or evacuation.
- Avoid passing unsubstantiated information and rumors.
- Prepare to activate your personal Family Emergency Plan. (*see Section 1*)

In addition to all previously mentioned precautions, business owners and managers are advised to:

- Announce Threat Condition **SEVERE** and explain expected actions.
- Deploy security personnel based on threat assessments.
- Close or restrict entry to the facility to emergency personnel only and restrict parking areas close to critical buildings.
- Maintain a skeleton crew of emergency employees.
- Deploy emergency response and security teams.
- Activate Operations Centers (if applicable).

- Maintain close contact with local law enforcement, emergency management officials and business consortium groups (Chamber of Commerce, Board of Trade, etc.)
- Be prepared to implement mutual aid agreements with government and with other similar/neighborhood businesses/industries.
- Provide security in parking lots and company areas.
- Report suspicious activity immediately to local law enforcement.
- Restrict or suspend all deliveries and mail to facility. Emergency supplies or essential shipments should be sent to off-site location for inspection.
- Activate your business emergency / contingency plan.

(Red) In addition to all previously mentioned precautions, federal departments and agencies should consider:

- Increase or redirect personnel to address critical emergency needs.
- Assign emergency response personnel and pre-position and mobilize specially trained teams or resources.
- Monitor, redirect, or constrain transportation systems.
- Close public and government facilities not critical for continuity of essential operations, especially public safety.

For more information about **D.C. HSEMA's** Homeland Security Terrorist Threat Advisory System, visit <http://hsema.dc.gov> For more information about the **Department of Homeland Security** and to stay current on national security alerts and warnings, visit www.dhs.gov.

ABOUT CYBER ATTACKS

There are 3 key risk factors related to information technologies systems:

- A direct attack against a system “through the wires” alone (called hacking) -- meaning an attacker or user “hacks” in or gains “**access**” to restricted data and operations.
- An attack can be a physical assault against a critical IT element meaning an attacker changes or destroys data, modifies programs or takes control of a system (basically can cause a loss of data “**integrity**” = data is no good).
- The attack can be from the inside -- meaning private information could get in the wrong hands and become public or identities stolen (basically “**confidentiality**” is broken = data is no longer secure or private).

Cyber attacks target computer networks that run government, financial, health, emergency medical services, public safety, telecommunications,