



## **Alert 03- 025**

### **TITLE: Homeland Security Advisory System Increase to National Level ORANGE May 20, 2003**

The following information is meant to advise state and local officials and those who own and operate critical facilities about possible indicators of terrorist attack planning.

In the wake of the terrorist bombings in Saudi Arabia and Morocco, intelligence reports indicate that terrorists may attempt attacks against targets in the United States. Al-Qa'ida, and those sympathetic to their cause, remains the principal threat. Threats may also emanate from other anti-US terrorist groups and ad hoc groups or disgruntled individuals not connected to existing terrorist organizations or state sponsors of terrorism.

International terrorist groups, such as Al-Qa'ida, have demonstrated the ability to plan and conduct complex attacks, simultaneously, against multiple targets. Recent terrorist attacks overseas have demonstrated the use of small arm equipped assault teams, large vehicle borne explosive devices, and suicide bombers. The bombings in Riyadh, Morocco, and Israel underscore terrorists' desires to attack soft targets. At the same time, intelligence reports in recent months point to a wide range of possible infrastructure targets that Al-Qa'ida may have plans to attack. These include:

- Key assets such as nuclear power plants, dams and government facilities,
- Energy sector to include power generating facilities, fuel farms, and gas stations,
- Transportation sector to include passenger rail; freight trains carrying toxic industrial chemicals; civil aviation; rail and vehicle bridges; tunnels; subways,
- Direct attacks on financial institutions.

Terrorists are opportunistic. They exploit vulnerabilities left exposed, choosing the time, place and method of attack according to the weaknesses they observe or perceive. Increasing the security of a particular type of target makes it more difficult for terrorists to successfully strike. In order to protect ourselves from those that desire to harm our friends, families, businesses, and the nation, it is important to maintain awareness and look for suspicious activity or "things out of place."

### **Surveillance Activities**

Few terrorist attacks are executed without pre-operational surveillance of the desired target. Surveillance is done to determine target suitability, security and noticeable patterns in the targets movements, physical security, and the surrounding environment.

Key activities suggesting possible terrorist surveillance is in progress may include:

- Foot surveillance involving 2-3 individuals working together.
- Mobile surveillance using bicycles, scooters, motorcycles, sport-utility vehicles, cars, trucks, boats or small aircraft.
- Persons or vehicles being seen in the same location on multiple occasions; persons sitting in a parked car for an extended period of time.
- Persons not fitting into the surrounding environment, such as wearing improper attire for the location, or persons drawing pictures or taking notes in an area not normally of interest to a tourist.
- Persons using possible ruses to cover their activities, such as taking on a disguise as a beggar, demonstrator, shoe shiner, fruit or food vendor, street sweeper, or a newspaper or flower vendor not previously recognized in the area.
- Persons videotaping or photographing security cameras or guard locations. Unusual or prolonged interest in security measures or personnel, entry points and access controls, or perimeter barriers such as fences or walls.
- An increase in anonymous threats followed by individuals noticeably observing security reaction drills or procedures. Questioning of security or facility personnel by an individual(s) that appears benign.

### **Suicide Bombers**

While not a guarantee, some of the visible markers associated with suicide bombers known to have attacked soft targets such as restaurants or night spots have included:

- Irregular dress – loose fitting clothes, large sweatshirt, vest, jacket in hot weather.
- Repeated patting of the self (checking the location of the switch, etc).
- Irregular or inappropriate baggage being carried such as a large briefcase into a club or restaurant.
- Luggage or kit/gym bag obviously weighed down more than normal.
- Hands in pockets of trousers or outer clothing; and, individual refuses to show hands/palms when told to do so.
- Do not discount the prospect for male or female suicide bombers or even male/female suicide team.

### **BUSINESS AND SMALL GOVERNMENT PROTECTIVE ACTIONS**

- Maintain situational awareness of world events and ongoing threats.
- Ensure all levels of personnel are notified via briefings, email, voice mail and signage of any changes in threat conditions and protective measures.
- Encourage personnel to be alert and immediately report any situation that appear to constitute a threat or suspicious activity.
- Encourage personnel to take notice and report suspicious packages, devices, unattended briefcases, or other unusual materials immediately; inform them not to handle or attempt to move any such object.
- Encourage personnel to keep their family members and supervisors apprised of their whereabouts.
- Encourage personnel to know the location of emergency exits and stairwells and rally points to ensure the safe egress of all employees.

- Increase the number of visible security personnel.
- Rearrange exterior vehicle barriers, traffic cones, and road blocks to alter traffic patterns near facilities and patrols by alert security forces.
- Institute/increase vehicle, foot and roving security patrols varying in size, timing and routes.
- Implement random security guard shift changes.
- Arrange for law enforcement vehicles to be parked randomly near entrances and exits.
- Review current contingency plans and, if not already in place, develop and implement procedures for receiving and acting on threat information, alert notification procedures, terrorist incident response procedures, evacuation procedures, bomb threat procedures, hostage and barricade procedures, chemical, biological, radiological and nuclear (CBRN) procedures, consequence and crisis management procedures, accountability procedures, and media procedures.
- When the aforementioned plans and procedures have been implemented, conduct internal training exercises and invite local emergency responders (police, fire, rescue, medical and bomb squads) to participate in joint exercises.
- Coordinate and establish partnerships with local authorities to develop intelligence and information sharing relationships.
- Place personnel on standby for contingency planning.
- Limit the number of access points and strictly enforce access control procedures.
- Approach all illegally parked vehicles in and around facilities, question drivers and direct them to move immediately, if owner can not be identified, have vehicle towed by law enforcement.
- Consider installing telephone caller I.D., record phone calls, if necessary.
- Increase perimeter lighting.
- Deploy visible security cameras and motion sensors.
- Remove vegetation in and around perimeters, maintain regularly.
- Institute a robust 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.
- Deploy explosive detection devices and explosive detection canine teams.
- 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 and around facilities.

## PERSONAL PROTECTIVE MEASURES

- Make a Plan for what you will do in an emergency
- Make a kit of emergency supplies
- Be informed about what might happen
- Visit <http://ready.gov> for more detailed information

DHS continues to encourage individuals to report information concerning suspicious or criminal activity to law enforcement or a Homeland Security watch office. Individuals may report incidents online at <http://www.nipc.gov/incident/cirr.htm>, and Federal agencies/departments may report incidents online at <http://www.fedcirc.gov/reportform.html>. Contact numbers for the DHS watch centers are: For private citizens and companies, (202) 323-3205, 1-888-585-9078, or [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov); for the telecom industry, (703) 607-4950 or [ncs@ncs.gov](mailto:ncs@ncs.gov); and for Federal agencies/departments, (888) 282-0870 or [fedcirc@fedcirc.gov](mailto:fedcirc@fedcirc.gov). DHS will update this alert should it receive additional relevant information, including information provided to it by the community.