



MARINE SAFETY INFORMATION BULLETIN

These bulletins are purely informational for the maritime community within this Captain of the Port zone. They advise you of emerging information & situations that may impact our Marine Transportation System. As important, they help to manage expectations & facilitate cooperation regarding actions that we may be taking and/or that you may need to employ in the interest of safety/security. Increased vigilance in our maritime world hinges significantly upon proactive engagement & information sharing with the private sector, which has the primary responsibility for security & safety at their waterfront facilities & vessels.

BULLETIN NO: 021-03

Date: November 14, 2003

SUBJECT: Department of Homeland Security Advisory

Attn: Security Managers

1. Enclosed is a security advisory from the Department of Homeland Security today. This advisory will be updated if additional relevant information is received. Currently no change to the Homeland Security Advisory System level is anticipated – the current level is **Yellow**.

2. The USCG continues to be on a heightened state of alert consistent with the current Homeland Security threat level and the traditional surge of boaters during the summer season. We are taking appropriate measures consistent with the existing safety and security posture. The USCG is working with DHS, DOT, the FBI, and other security/law enforcement agencies to ensure the security of ports, waterways and facilities. You are encouraged to continue close cooperation and coordination of necessary safety/security efforts with your local/state law enforcement agencies. Report any suspicious activity to the Coast Guard via marine radio or via our 24-hour Coast Watch Hotlines or the National Response Center.

Connecticut: (800) 774-8724.

Long Island, NY: (800) 697-8724.

Other areas: (800) 424-8802 (National Response Center)

J. J. Coccia
Captain, U.S. Coast Guard
Captain of the Port Long Island Sound

Encl: (1) Department of Homeland Security Advisory

SUBJECT: Department of Homeland Security Advisory

**Information Bulletin****Title:** Vehicle Borne Improvised Explosive Devices (VBIEDs)**Date:** November 10, 2003

ATTENTION: Homeland Security Advisors, Security Managers, and Chemical and Energy Information Sharing Centers

DHS intends to update this Information Bulletin should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is YELLOW.

OVERVIEW

The use of VBIEDs allow terrorists to place large amounts of explosives against hard or soft targets with a high degree of mobility – in effect turning these VBIEDs into precision weapons that cause mass casualties and physical destruction. VBIED attacks require less coordination, planning, expertise, material, and money than the more spectacular type of terrorist methods, such as aircraft hijackings or employment of weapons of mass destruction, yet still can achieve the mass casualty objective.

The Department of Homeland Security (DHS) believes that a truck bombing by terrorists may be preempted if the general public remains alert for certain indicators. The VBIED threat against the US or host nation interests abroad remains high. While DHS has no specific information to indicate that a truck bombing of any kind is currently being planned in the United States, it is possible terrorists may attempt to employ VBIED operations against targets in the US. VBIEDs have been used successfully here in the past – most notably the 1993 World Trade Center and 1995 Oklahoma City bombings. Lastly, terrorists have learned that hitting multiple soft targets simultaneously with multiple VBIEDs is a tactic that works.

DETAILS

The recent VBIED operation in Riyadh on 8 November 2003 was conducted against a housing compound inhabited by various nationalities, but mostly Arabs. While details of the terrorist bombing are sketchy at this time, it appears the attackers either stole a Saudi military/police vehicle or painted a vehicle to resemble one. According to Saudi officials, 17 people were killed and over 100 were injured. Press reports indicate:

- The operatives entered the compound by disguising themselves as Saudi security/police. They wore security uniforms and drove two vehicles into the compound with at least one vehicle similar to that used by police. At least two of the suspected Al-Qaeda operatives opened fire on their way into the guarded Muhaya complex.
- It is believed that the second vehicle that followed behind the first was the actual VBIED.

The May and November Riyadh bombings signal a change in tactics from simply driving a single VBIED to a target to tactics in which multiple vehicles are used and security personnel are confronted with assault teams equipped with small arms to gain access through the perimeter in order to allow suicide VBIEDs to gain entry to the target area. In the most recent incident this tactic was modified to include armed confrontation coupled with the use of uniforms and vehicles that appear to be from security or law enforcement.

SUBJECT: Department of Homeland Security Advisory

Other facilities that have been targeted by the “traditional” use of VBIEDs have been hotels and apartment complexes, as well as moving passenger buses. This tactic allows for attacks to be conducted without entering a facility and requires a protective strategy to include areas outside the controlled perimeter of the facility. Another VBIED tactic to maximize casualties uses secondary explosive devices to target responders and crowds exiting the site of the initial explosion.

There is no standard type of vehicle associated with vehicle borne improvised explosive devices (VBIEDs.) Vehicle selection depends on vehicles common to and available in a region, vehicles possessing routine access to the area, and the security posture of the intended target. The typical tactic for the employment of a VBIED is to drive a single vehicle to the target, park the vehicle, and allow the vehicle to detonate via time delay or by remote control. Another tactic is the use of suicide drivers, driving up to the target and detonating the vehicle by use of a “dead-man” switch. As evidenced by attacks in Iraq, terrorist may also use garbage trucks, ambulances or other emergency vehicles.

POTENTIAL VBIED INDICATORS

The existence of any one of the following indicators does not in and of itself suggest terrorist activity. Each incident should be carefully assessed, along with other information available to determine whether there is cause for further investigation:

- Theft of explosives, blasting caps, or fuses, or certain chemicals used in the manufacture of explosives.
- Rental of self-storage space for the purpose of storing chemicals or mixing apparatus.
- Delivery of chemicals directly from the manufacturer to a self-storage facility or unusual deliveries of chemicals to residential or rural addresses.
- Chemical fires, toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel/motel rooms, or self-storage units.
- Modification of truck or van with heavy duty springs to handle heavier loads.
- Small test explosions in rural wooded areas.
- Treatment of chemical burns or treatment for missing hands/fingers.
- Untreated chemical burns or missing hands/fingers.

SUGGESTED PROTECTIVE MEASURES

Terrorists continue to select soft targets for attack -- particularly those that will yield a high casualty count. Some examples include but are not limited to: residences, recreational and shopping venues, and business buildings and complexes. All available antiterrorism measures should be rigorously reexamined including but not limited to: physical security perimeters, set back distances between security fences and key buildings, and barricades.

- Encourage personnel to be alert and to immediately report any situation that appears to constitute a threat or suspicious activity.
- Guard force turn-over procedures and personnel authentication practices.
- Rearrange exterior vehicles barriers, traffic cones, and road blocks to alter traffic patterns near facilities.
- Institute/increase visible vehicle, foot and roving security patrols that vary in size, timing and routes.
- Implement random security guard shift changes.

SUBJECT: Department of Homeland Security Advisory

- Arrange for law enforcement vehicles to be parked near entrances and exits.
- 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 an owner can not be identified, have vehicle towed by law enforcement.
- Increase perimeter lighting.
- Deploy visible security cameras and motion sensors.
- Review security camera footage daily to detect possible indicators of preoperational surveillance.
- Remove vegetation in and around perimeters and maintain regularly.
- Institute a robust vehicle inspection program, including but not limited to 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 explosives detection canine teams.
- Conduct vulnerability studies focusing on physical security, structural engineering, infrastructure engineering, power, water, and air infiltration, if feasible.

USE OF OFFICIAL IDENTIFICATION, UNIFORMS, AND VEHICLES

As illustrated by this latest attack, terrorist groups may utilize police or military identification, uniforms, and vehicles as effective ways to increase access and decrease scrutiny in furtherance of planning and operations. Hundreds of official identification cards, badges, decals, uniforms, and government license plates have been reported stolen or lost. Additionally, a number of private companies have reported receiving suspicious inquiries about renting official delivery vehicles, and emergency services representatives have received unusual requests for detailed vehicle descriptions. There is no historical baseline to compare recent theft or suspicious inquiry data, and the intent or resolution of many of the thefts cannot be determined.

The worldwide proliferation of individuals or “companies” that traffic in high-quality imitations of official identification, uniforms, or vehicles is a related issue that increases the possibility such items could be used to facilitate future terrorist attacks and further complicates efforts to prevent their acquisition.

Several press reports this year have referred to the theft and sale over the Internet of a large number of United Parcel Service (UPS) uniforms. Although these reports proved to be false, they did bring to the public’s attention the potential security concerns pertaining to missing or stolen identification, uniforms, or vehicles.

DHS reminds all recipients to remain vigilant for the disappearance of, or suspicious inquiries regarding, official identification cards, badges, decals, uniforms, government license plates, and vehicles, and to establish practices that account for missing items. DHS encourages recipients to report suspicious incidents to the proper authorities and to remain vigilant for any nexus to terrorism.

SUGGESTED PROTECTIVE MEASURES

Recognizing that possession of some combination of official identification cards, badges, decals, uniforms, government license plates, and vehicles tends to reduce suspicion and might allow an individual or vehicle greater access to sensitive facilities, the following protective measures are suggested:

- Keep comprehensive records of all official identification cards, badges, decals, uniforms, and license plates distributed, documenting any anomalies, and canceling access to items that are lost or stolen.
- Practice accountability of all vehicles, including tracking vehicles that are in service, in repair status, or sent to salvage.

SUBJECT: Department of Homeland Security Advisory

- Safeguard uniforms, patches, badges, ID cards, and other forms of official identification to protect against unauthorized access to facilities, including stripping all decommissioned vehicles slated for resale and/or salvage of all agency identifying markings and emergency warning devices.
- Check multiple forms of valid identification for each facility visitor.
- Verify the legitimate business needs of all approaching vehicles and personnel.
- Improve identification card technology to eliminate reuse or unauthorized duplication.
- Alert uniform store vendors of the need to establish and verify the identities of individuals seeking to purchase uniform articles.
- Ensure all personnel are provided a security briefing regarding present and emerging threats.

DHS encourages recipients of this Information Bulletin to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.