



Advisory

Title: Homeland Security Advisory System Increased to ORANGE for Financial Institutions in Specific Geographical Areas

Date: August 1, 2004



Warning: This document is **FOR OFFICIAL USE ONLY (U//FOUO)**. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official. For comments or questions, please contact the DHS/IAIP Information Analysis -Requirements Division via email at DHS.IAIP@DHS.GOV.

This is a joint DHS and FBI Advisory.

ATTENTION: Homeland Security Advisors, Federal Departments and Agencies, Law Enforcement and First Responders, Information Sharing and Analysis Centers, and the Intelligence Community

Based on this notification, the United States Homeland Security Advisory System (HSAS) level for the financial services sector in New York City, Northern New Jersey and Washington, D.C.; is raised from YELLOW -ELEVATED to ORANGE - HIGH. The threat level for the rest of the nation remains at YELLOW – ELEVATED.

OVERVIEW

(U) The following information is meant to advise state and local officials and private sector owners and operators of critical facilities about indicators of terrorist attack planning. Our understanding of this threat could change as new information becomes available.

DETAILS

(U//FOUO) Recent credible and specific intelligence reporting indicates terrorist operatives have done extensive research and reconnaissance activity against major U.S. and international financial institutions in Washington, D.C., Northern New Jersey and New York City. These include: the Citigroup buildings in the New York City area, the New York Stock Exchange Building in New York City, the International Monetary Fund and the World Bank Buildings in Washington D.C., and the Prudential Insurance Company of America in Newark, New Jersey. The reporting provides a level of detail that is unusually specific, to include information about the interior configurations of these buildings, as well as infrastructure, services, and buildings that surround the targets of interest.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) The reporting does not specify the timing or mode of attack. Based on the nature of the reconnaissance information, however, the most likely means of attack would be a Vehicular Borne Improvised Explosive Device (VBIED), to include limousines, large vans, trucks, and oil tankers which could be placed in underground parking areas or near highly populated entrance ways. A joint DHS/FBI Information Bulletin "Potential Threat to Homeland Using Heavy Transport Vehicles," issued on 30 July 2004, outlines terrorist use of VBIEDs overseas as well as in the United States. In addition, consideration appears to have been given to Improvised Explosive Devices (IEDs) being carried into facilities by operatives. An Information Bulletin released on 29 May 2004, titled "Terrorist Threat to the Homeland," highlighted the intelligence and law enforcement communities' concern that al-Qaida and other extremist groups may seek to influence or disrupt key events to include the Democratic and Republican Parties' National Conventions this summer and the U.S. Presidential Election in November.

(U//FOUO) Other possible modes of attack are the use of IEDs in subways and other public transport systems in close proximity to these targets. Terrorist use of aircraft as weapons against Homeland targets is another mode of attack to consider.

(U//FOUO) We have limited information indicating terrorist intent and plans to conduct computer network attacks against U.S. financial institutions.

SUGGESTED PROTECTIVE MEASURES:

(U//FOUO) Recommended protective measures for **owners and operators, security managers**, and where appropriate, **state and local government entities**:

- Increase the number of visible security personnel.
- If possible implement random inspection of backpacks, briefcases, suitcases, etc. of people entering facilities.
- Institute/increase vehicle, foot and roving security patrols; vary size, timing and routes.
- Implement random security guard shift changes.
- Approach all illegally parked vehicles in and around facilities, question drivers and direct them to move immediately; if the owner cannot be identified, have vehicle towed by law enforcement.
- Arrange for law enforcement vehicles to be parked randomly near entrances and rearrange exterior vehicle barriers, traffic cones, and road blocks to alter traffic patterns near facilities.
- Limit the number of access points and strictly enforce access control procedures.
- Deploy explosives detection devices and explosives detection canine teams.
- Increase perimeter lighting.
- Deploy visible security cameras and motion sensors.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Institute a robust vehicle inspection program to include checking the undercarriages 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 filtration, if feasible.
- Consider installing remotely controlled barrier gates, remove controls at potential entry points for a VBIED, and reinstall to a remote secure site with closed circuit TV and phones to monitor access. This would help counter an attack where terrorists kill guards and activate the barrier devices themselves.
- 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 if feasible.
- Facilities deemed to be high risk may consider establishing off-site delivery facilities where all vehicles bring outside cargo for screening.
- Establish multiple, layered entry points at high risk facilities.
- Post signs stating that vehicles parked in unauthorized areas will be towed immediately.
- Identify key areas in and/or adjacent to a facility where a terrorist could park a vehicle and be in close proximity to large numbers of personnel.
- Prohibit parking in these areas or conduct a thorough search of vehicles.
- Monitor such areas with security cameras.
- Commercial bus and truck park operators should review current security procedures and consider counter theft measures as appropriate.

(U//FOUO) For **subways and enclosed public spaces**, we recommend the following protective measures:

- Ensure critical street vents, doors, and fences have appropriate security measures in place to include surveillance cameras, locks, and covers.
- Monitor street vents, doors, and fences for unauthorized access or exploitation of security boundaries.
- Ensure critical subway system assets have sufficient lighting.
- Ensure passive vehicle barriers are employed to protect crowded or popular subway stations or other critical areas from VBIEDs.
- Implement security sweeps of subway stations for suspicious activities and suspect packages.
- Conduct increased monitoring and review of video surveillance footage to identify any preoperational surveillance activities.
- Review incident/emergency response plans.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- Report any suspicious medical conditions of multiple personnel in subways/enclosed public spaces (e.g. shopping malls).

(U//FOUO) For **personnel**, we recommend the following protective measures:

- Ensure that 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 to immediately report any situation that appears to constitute a threat or suspicious activity.
- Encourage personnel to take notice and report suspicious packages, devices, unattended briefcases, or other unusual items or 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, stairwells and rally points to ensure safe egress and marshalling of all employees in an emergency.

(U//FOUO) For **computer networks**, we recommend the following protective measures:

- Review contingency plan(s).
- Brief computer security/incident response staff on current situation/threat.
- Exercise/validate key points of contact.
- Check alternate communications paths.
- Validate readiness of backup sites.
- Ensure files are backed up and current.
- Monitor network for abnormal activity.

DHS and the FBI encourage recipients of this Advisory to report information concerning suspicious or criminal activity potentially related to terrorism to the local FBI Joint Terrorism Task Force and the Homeland Security Operations Center (HSOC). The HSOC may be reached by phone at (202) 282-8101 or by email at HSCenter@dhs.gov.