

The Financial and Banking Information Infrastructure Committee (FBIIC)
Advisory for Homeland Security Threat Alert Level Severe (Red)

The Department of Homeland Security (DHS) is developing guidance on the appropriate preparedness actions for private sector financial organizations to consider should the Threat Level be raised to Severe (Red). In addition, the Financial Services Sector Coordinating Council (FSSCC), a private sector group created to represent the financial services industry, is developing a detailed list of actions that will be tailored for the financial services sector. The FBIIC has developed the following advisory as interim guidance in the interest of furthering preparedness for the financial services sector. As is customary, institutions contemplating a change in their operating status should contact their primary regulator.

- Financial institutions should make every effort to ensure continuity of their operations during a Severe Threat Alert Level (Red) to the extent they can do so without subjecting employees, customers, or the general public to danger, and within the constraints imposed by federal, state and local laws. Customers have entrusted our financial institutions with their assets. It is important for customers to have confidence that they can access their assets, particularly during times of higher anxiety.
- Financial institutions should make individual decisions based on their business continuity/emergency preparedness practices, the specific circumstances affecting/impacting their operation, and applicable federal and state regulations.
- Financial institutions should review the situation and circumstances surrounding the change in the threat level and make a determination as to any additional actions that should be taken. The process should, at a minimum, include reviewing the general guidance issued by DHS when the Threat Level was raised to High (Orange). (*See attached Homeland Security Information Bulletin 03-002*).

NOTE: We have no information at this time that suggests the need or intent to raise the Threat Alert Level to Severe (Red).

HOMELAND SECURITY INFORMATION UPDATE

Suggested Guidance on Protective Measures

Information Bulletin 03-002

National Threat Warning System–Homeland Security Information Update–HSAS Threat Level Orange (High); joint guidance from the Department of Homeland Security and the FBI.

As recipients were advised, the Homeland Security Advisory System (HSAS) was raised to High (Orange) from Elevated (Yellow) on 2/7/03. This communication provides critical infrastructure owners/operators suggested guidance for developing protective measures based on this heightened threat condition. This communication also provides potential indicators of threats involving weapons of mass destruction.

PART I: GENERAL PROTECTIVE MEASURES

In addition to continuing all precautions from the lower threat condition (Yellow), the following general protective measures may be utilized. Recipients are advised to take other appropriate steps, in conjunction with local conditions, policies, and procedures. The list that follows is not intended to be exhaustive, but merely illustrative:

- Coordinate necessary security efforts with Armed Forces or law enforcement agencies.
- take additional precautions at public events.
- review contingency plans to work at an alternate site or with a dispersed work force.
- review plans to restrict access to facilities.

PART II: SPECIFIC PROTECTIVE MEASURES FOR INFRASTRUCTURE OWNERS/OPERATORS AT HIGH CONDITION (ORANGE)

- announce threat condition high (orange) to all employees.
- consider full or partial activation of emergency operations center.
- review policy and plans relating to restricting access to critical facilities and infrastructure.
- conduct periodic inspections of building facilities and HVAC systems for potential indicators/irregularities
- direct people to the Red Cross website for further review of protective measures for families and businesses.

- enhance security at critical facilities.
- institute/increase vehicle, foot and roving security patrols.
- implement random security guard shift changes.
- increase visibility in and around perimeters by increasing lighting and removing or trimming vegetation.
- implement stringent identification procedures to include conducting “hands on” checks of security badges for all personnel, if badges are required.
- remind personnel to properly display badges, if applicable, and enforce visibility.
- rearrange exterior vehicle barriers to alter traffic patterns near facilities.
- 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 the owner can not be identified, have vehicle towed by law enforcement.
- if possible, 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.
- instruct citizens to report suspicious activities, packages and people, and report all suspicious activity immediately to local law enforcement.
- x-ray packages, if possible, prior to entry, and inspect handbags, and briefcases, if possible.
- encourage personnel to avoid routines, vary times and routes, and pre-plan with family members and supervisors.
- validate vendor lists for all routine deliveries and repair services.
- restrict vehicle parking close to buildings.
- inspect all deliveries and consider accepting shipments only at offsite locations.
- require identification, sign-in, and escorts for visitors.
- instruct people to be especially watchful for suspicious or unattended packages and articles either delivered or received through the mail.
- send a public information officer to the state joint information center.

- install special locking devices on manhole covers in and around critical infrastructure facilities.
- initiate a system to enhance mail and package screening procedures (both announced and unannounced).
- 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, shelter in place 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.

PART III: POTENTIAL INDICATORS OF THREATS INVOLVING WEAPONS OF MASS DESTRUCTION (WMD)

POTENTIAL INDICATORS OF WMD THREATS OR INCIDENTS:

- unusual/suspicious packages or containers, especially those found in unlikely or sensitive locations, such as those found near air intake/HVAC systems or enclosed spaces.
- unusual powders or liquids/droplets/mists/clouds, especially found near air intake/HVAC systems or enclosed spaces.
- signs of tampering or break-in to a facility or maintenance/utility area
- reports of suspicious person(s) or activities, especially those involving sensitive locations within or around a building
- dead animals/birds, fish, or insects
- unexplained/unusual odors. Smells may range from fruity/flowery to sharp/pungent, garlic/horseradish-like, bitter almonds, peach kernels, and new mown grass/hay.
- unusual/unscheduled spraying or discovery of spray devices or bottles

The Department of Homeland Security encourages individuals to report information concerning suspicious activity to their local FBI Joint Terrorism Task Force (JTTF) office, <http://www.fbi.gov/contact/fo/fo.htm>, the Department of Homeland Security, or to other appropriate authorities. Individuals can reach the Homeland Security WATCH AND WARNING UNIT at (202) 323-3205, toll free at 1-888-585-9078, or by email to nipc.watch@fbi.gov.