

UNCLASSIFIED//FOR OFFICIAL USE ONLY

**Information Bulletin****Title:** False Hospital Inspections**Date:** April 25, 2005

ATTENTION: Federal Departments and Agencies, State Homeland Security Advisors and Staff, Security Managers, and State and Local Law Enforcement. Public Health, Food and Agriculture Information Sharing and Analysis Centers (ISACs).

Request for further dissemination must be approved by the DHS/Information Analysis and Infrastructure Protection (IAIP) Directorate - Requirements Division (IA-R) at DHS.IAIP@dhs.gov

Warning: This document is UNCLASSIFIED//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 the Department of Homeland Security (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.

Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS national level is YELLOW-ELEVATED.

Consistent with Intelligence Oversight directives, certain U.S. Persons (USPER) information has been minimized. Should you require the USPER information, please contact the DHS/IAIP, IA-R – Information Management staff at DHS.IAIP@dhs.gov.

OVERVIEW

This bulletin is intended to raise awareness and share information about recent suspicious reports involving hospitals. The Department of Homeland Security (DHS) has no information indicating a specific and credible threat of an al-Qaida-associated terrorist attack against hospital facilities inside the United States.

Over the past year, there have been several reported cases of personnel falsely representing themselves as Joint Commission on Accreditation of Healthcare Organizations (JCAHO). These said individuals were attempting to gain public health service information from hospital personnel, and behaved in a manner inconsistent with legitimate inspection professionals. No suspects have been detained as of this reporting.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

DETAILS

DHS has no direct threat information related to hospitals in the United States, and there is only one known example of Islamic extremists targeting hospitals. In 1995, known terrorist Shamil Basayev and Chechen rebels led a hostage taking raid at Budennovsk in southern Russia in which 2,000 hostages were taken at a hospital. About 150 of them died when Russian forces stormed the building; Basayev himself managed to escape.

However, DHS has noted an increased number of suspicious incidents involving hospitals. On March 27, 2005, a New Jersey hospital experienced its fourth separate incident in a six-week period. Three male subjects in their 30s and 40s, possibly of Middle Eastern descent, spoke fluent unaccented English and presented themselves as physicians from JCAHO, an association that accredits 15,000 plus health care organizations per year in the United States. According to the New Jersey Office of the Attorney General/Office of Counter Terrorism, the subjects inquired about capacity, services, and operations of the hospital and left the facility when their questions were not answered.

From February 26 to March 10, 2005, three other U.S. hospitals in Boston, Los Angeles, and Detroit also reported individuals posing as JCAHO inspectors. These individuals similarly behaved in a manner inconsistent with professional inspection staff and were described respectively as:

- A Caucasian man and woman at the Los Angeles hospital
- A male of South Asian descent at the Boston hospital
- A Caucasian woman at the Detroit hospital

JCAHO administrators have stated that these suspects were not with JCAHO and that there were no planned inspections at these facilities. The suspicious individuals entered hospitals at 3 a.m. local time in Los Angeles and Boston; the Detroit entry time was reported only as "AM." Suspects from all three locations left immediately after being challenged by hospital staff.

- Hospitals routinely hire commercial inspection teams before a JCAHO inspection, to evaluate their processes, etc. These teams would typically inspect during normal day duty hours and report to senior hospital management/administrators.
- Early morning evaluations are out of character, at least in the initial stages of a pre-JCAHO "spin-up."
- U.S. hospitals offer easy public access and would be recognized by terrorist planners as easy, accessible targets. Known targeting of such facilities would instill great panic and fear in the general public.

OTHER RECENT HOSPITAL PROBING

These most recent nationwide impersonations are more noteworthy when seen in the broader context with similar incidents which have occurred from October 2004 to February 2005.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- In October 2004, two hospitals in the Phoenix, AZ metropolitan area reported suspicious activity, including photography, requests of building layout, inquiries regarding the location of the pharmacy, and computer fraud.
- Three men inquired as to the location of the pharmacy at St. Joseph's Hospital in Phoenix. These men had previously visited hospitals in Texas and Indiana. All three hospitals are distribution points for the antidote medicines for biological attacks.
- On February 7, 2005 at approximately 10 a.m., two individuals (SUBJECTS) who identified themselves as special agents representing the Department of Defense and CIA entered the emergency room at Middletown Regional Hospital, NY. The SUBJECTS requested to see the charge nurse and presented identification badges. The SUBJECTS asked the nurse a series of questions concerning capacity for cardiac care, trauma care, heliport, and private rooms. As the hospital staff's suspicion of the SUBJECTS increased, the SUBJECTS left the building. The hospital staff did collect a business card from one of the SUBJECTS, and it appears to be fraudulent.

While these suspicious activities may exhibit characteristics of criminal activity or even possible pre-operational planning activity, DHS has no information indicating that they are tied to a specific and credible threat of an al-Qaida-associated terrorist attack against hospital facilities inside the United States. DHS, in coordination with its Intelligence Community partners, continues to monitor and assess the validity of all intelligence to identify any specific threats.

TRENDS

The use of false credentials to gain entry into hospitals is not new. However, according to JCAHO, these new events mark a different trend because of the number of incidents over this time period and nature of the questions seeking information on services. As an emerging pattern, this activity needs to be closely followed and reported.

Recon activity can lead to hospitals being selected as targets for possible criminal break-ins or terrorist attacks.

- Damage assessment on consequences to national security: if a hospital is successfully compromised, potential consequences are:
 - Loss of service that they provide during times of crises
 - Compromise of critical research capabilities
 - Damage or loss of storage for drugs and antidotes
 - Loss of public trust

SUGGESTED PROTECTIVE MEASURES

DHS recommends the following general protective measures:

Access Control:

- Advise appropriate staff, both medical and non-medical, of the potential for unauthorized personnel to present apparently legitimate credentials and/or be wearing

UNCLASSIFIED//FOR OFFICIAL USE ONLY

recognizable uniforms in order to gain access to a facility. Ensure that they understand the potential threat to a medical facility that houses people, chemicals as well as equipment, and provide instructions on how to deal with suspicious events. Encourage employees to confront all suspicious individuals or individuals without proper identification, particularly in sensitive areas, such as:

- Laboratories
 - Pharmacies
 - Physical plant
 - Shipping and Receiving
- Maintain control over all entrance points and monitor all exit points. Using Closed Circuit TV (CCTV), record all movements in both areas. Ensure that there is adequate lighting to support CCTV and that there are no obstructions to CCTV field of view (e.g., overgrown vegetation). If possible, maintain card access technology to all areas beyond the main entrance.
 - Enforce stringent credentialing and badging of all hospital employees. Implement credentialing and badging of contractors, official visitors, inspectors, and others with hospital business.
 - Do not allow access or give information to JCAHO representatives without first contacting hospital administration and senior security representatives.
 - Require photo identification of JCAHO representatives. Contact JCAHO office to verify that an inspection has been authorized.
 - Provide security guard and hospital administration staff escort to JCAHO representatives as they conduct inspections. Defer any requests for access or information that are not consistent with established inspection protocols.
 - Inspect parcels and packages being brought into the facility by JCAHO representatives. Conduct random inspections of parcels and packages brought in by visitors.
 - Ensure that all areas that are not open to the public (e.g., pharmaceutical storage areas, laboratories, HVAC and utility equipment areas, cleaning supply closets, etc.) are locked. Inspect locks and other security hardware on doors, windows, and other facilities.

Inspection:

- Increase inspections and inventorying of sensitive materials and equipment (e.g., pharmaceuticals, radiological material). Remove unnecessary sensitive material and equipment. Require rigorous materials accounting for all sensitive materials and equipment movement.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- At regular intervals during each day, inspect interior and exterior of buildings, storage areas, waste bins, closets, and other areas for suspicious packages. Report any unusual items to security office.
- At irregular intervals during each day, inspect HVAC intakes; electric, gas, water, telecommunications feeds into the facility for signs of tampering.

Communications:

- Test operation of internal communication systems (e.g., from medical personnel to security office) and external communication facilities (e.g., to local law enforcement).
- Test alarm systems for proper operation.

Security Force:

- Ensure security guard force is fully briefed and trained in handling suspicious persons and/or packages.
- Review points of contact with local law enforcement and Joint Terror Task Force. Establish periodic communication to update threat situation.
- Contact local police at first contact with any suspicious activity, and if possible record and document the following information:
 - All identification information to include JCAHO identification and secondary form of identification. Secondary identification should have a photo of the individual.
 - A full description of the individual(s), to include clothing worn.
 - The license plate (to include state), make and model of any vehicle.
- If not in place, add CCTV to all access points, parking areas, exterior of all access points, and driveways leading to access points.

Cyber Security:

- Review cyber security procedures to prohibit unauthorized access to data and information. Restrict access to computer systems to necessary personnel.
- Review the facility web page, and eliminate information not necessary for public cyber access to the facility and that might be sensitive.

Security Plan:

- Review the security plan and procedures for dealing with this type of threat. Update as necessary.

REPORTING NOTICE:

DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force (JTTF) – the FBI regional phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm> – and the Homeland Security Operations Center (HSOC). The HSOC can be reached via telephone at 202-282-8101 or by email at HSCenter@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the HSOC. The NICC can be reached via telephone at 202-282-9201 or via email at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact (POC).

For comments or questions related to the content or dissemination of this document, please contact the DHS/IAIP, IA-R – Information Management staff at DHS.IAIP@dhs.gov.