Department of Homeland Security Daily Open Source Infrastructure Report for 07 November 2005

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The New Jersey Star−Ledger reports that a man without a boarding pass eluded security Saturday at Newark Liberty International Airport and boarded a flight to Miami before the flight crew realized he was there illegally. (See item 12)
- The Honolulu Star Bulletin reports that Hawai`i is the first state to establish airport surveillance of avian flu or other viruses that may be introduced by travelers. (See item 27)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *November 06, Associated Press* — **Thousands in Indiana left without power following devastating tornado.** A tornado tore across southwestern Indiana early Sunday, November 6, cutting a swath through a mobile home park and smashing homes as residents slept, leaving at least 17 people dead and about 200 injured, officials said. The tornado, which knocked out power to thousands, touched down near Henderson, KY, and then jumped the Ohio River into Indiana about 2:15 a.m. CST, striking the Eastbrook Mobile Home Park in the state's southwest corner around Evansville, IN. Mike Roeder, a spokesperson for utility company Vectren, said 25,000 homes were without power, mostly in Warrick County. There also were reports of natural gas leaks.

Source: http://www.indystar.com/apps/pbcs.dll/article?AID=/20051106/ NEWS01/511060524

2. *November 04, Associated Press* — **Gas shortage could cause power outages this winter.** A shortage of natural gas caused by this year's hurricanes will have to be managed closely to avoid rolling blackouts in New England this winter, industry officials say. Residential and commercial gas customers will not be affected but some gas−fired power plants around New England may not be able to make electricity if there is a shortage unless they can operate on another source of fuel. "A significant amount of the natural gas supply may be out of production," said Ellen Foley, a spokesperson for ISO New England, the organization that dispenses electricity to New England. The organization gathered with Vermont officials and utilities this week to evaluate the threats to the area's power supply. "This is not a question of whether our utilities have enough power supply to meet their needs. They do," said David O'Brien, commissioner of the Vermont Department of Public Service. The concern is that there might not be enough power to maintain the region's power grid without taking steps to reduce power use. Utility officials said the most stringent step would be rolling blackouts.
ISO New England: http://www.iso−ne.com/
Source: http://www.boston.com/news/local/vermont/articles/2005/11/04/gas_shortage_could_cause_power_outages_this_winter/

3. *November 03, Department of Energy* — **Federal government increases renewable energy use over 1000 percent since 1999.** The Department of Energy (DOE) announced on Thursday, November 3, that the federal government has exceeded its goal of obtaining 2.5 percent of its electricity needs from renewable energy sources by September 30, 2005. The largest energy consumer in the nation, the federal government now uses 2375 Gigawatt hours (GWh) of renewable energy. “Particularly in light of tight oil and gas supplies caused by Hurricanes Katrina and Rita, it is important that all Americans −− including the federal government −− increase energy efficiency and the use of renewable fuels,” said Secretary of Energy Samuel W. Bodman. When the Executive Order goal was set in 1999, renewable energy from biomass, geothermal, solar and wind projects only accounted for some 173 GWh. DOE’s Federal Energy Management Program worked to helped federal agencies meet the goal by purchasing renewable energy or utilizing renewable technologies at individual sites. Solar panels, on−site wind projects and thousands of geothermal ground source heat pumps have been installed across the federal government.
Source: http://www.energy.gov/engine/content.do?PUBLIC_ID=19120&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4.

November 05, Associated Press — **U.S. charges four with stealing defense documents.** An engineer and Chinese television director are among four people indicted on charges of stealing secret documents on Navy warships and trying to smuggle them to China, prosecutors said Friday, November 4. Chi Mak, a naturalized U.S. citizen from China who lives in Los Angeles County, was arrested October 28. He allegedly took computer disks from Anaheim, CA, defense contractor Power Paragon, where he was lead engineer on a research project involving warship propulsion systems, according to an FBI affidavit. He also allegedly e−mailed photos and reports about the project to his home computer. Authorities say Chi Mak and his wife copied the information onto CDs and delivered them to Mak's brother, Tai Wang Mak, a broadcast and engineering director for the Phoenix North American Chinese Channel, who was then going to travel to Hong Kong with the documents. Chi Mak and Tai Wang Mak were both charged, along with their wives, Rebecca Laiwah Chiu and Fuk Heung Li, according to a spokesperson for the U.S. attorney's office. The four face charges of stealing government property, transportation of stolen goods and conspiracy, said spokesperson Thom Mrozek.
Source: http://www.cnn.com/2005/LAW/11/05/navy.indictments.ap/index.html?section=cnn_latest

5. *November 04, Associated Press* — **Pentagon eyeing cuts in weapons programs.** Struggling to pay for a costly war in Iraq, the Pentagon is considering as much as $15 billion in cuts to aircraft, shipbuilding and other weapons purchases as it begins to craft a budget for next year. Defense analysts and congressional staff say such reductions could hamper efforts to replace equipment worn out in the Iraq and Afghanistan wars and outdated Cold War−era weapons systems. Defense Secretary Donald H. Rumsfeld on Tuesday, November 1, said the department has to move funds around to ensure that the country gets what it needs to fight both conventional conflicts and unconventional threats, such as the insurgency in Iraq. Among the programs being considered for significant cuts or delays are the Joint Strike Fighter, the Pentagon's next generation, all−purpose fighter; the C−17 transport plane; the Navy's new DD(X) destroyer; and a reconnaissance aircraft called the Aerial Common Sensor. Military contractors are bracing for the cuts, or even decisions to eliminate entire programs. Lockheed Martin's chief financial officer Chris Kubasik recently said to analysts that the future of its reconnaissance aircraft was in question, saying, "it is premature to predict an outcome at this time."
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/11/04/AR2005110400231.html

[Return to top]

Banking and Finance Sector

6. *November 05, Monterey Herald (CA)* — **Safeway discloses security breach.** Safeway Inc. has notified employees in California that their personal information may have been compromised when a company laptop was stolen from a manager's home in August. The computer contained reports that included names, Social Security numbers, hire dates and work locations of employees in California and Hawaii, according to a company letter sent to current and former employees dated October 14. No employees have reported problems with their credit since they became aware of the situation, according to Safeway representatives. The computer was protected with a power−on password.

Source: http://www.montereyherald.com/mld/montereyherald/13090239.ht m

7. *November 04, Finextra Research* — **Bank makes two factor authentication mandatory.** Bank of America is making its SiteKey two factor authentication service a compulsory part of sign−in for its 14.5 million Internet banking customers. The bank launched the free SiteKey service in June this year. Customers signing up to the free service are asked to select a Passmark −− a small image and a brief phrase −− and three challenge questions. This information is then requested whenever the customer logs in to access an online account. SiteKey was orginally an optional service, but the bank will now make it a mandatory part of its Web banking system in the states where it is available. The bank had originally said that SiteKey would be installed across the U.S. by the end of the year, but the deployment is now expected to be completed in early 2006, several months later than planned. Last month the Federal Financial Institutions Examination Council set an end−2006 deadline for the banking industry to introduce multi−factor authentication for high risk Internet transactions. According to Sanjay Gupta, e−commerce executive at Bank of America, the bank is the first major bank to offer this level of protection.
Source: http://www.finextra.com/fullstory.asp?id=14482

8. *November 03, Securities and Exchange Commission* — **SEC urges investors to protect their online brokerage accounts from identity thieves.** The Securities and Exchange Commission (SEC) on Thursday, November 3, issued an investor guide designed to inform Americans about steps they can take to protect their online brokerage accounts from unauthorized activity by intruders. Regulators believe that some identity thieves are targeting online brokerage accounts for intrusion. Over the past few months, the SEC has become aware of numerous situations in which unauthorized individuals have gained access to other people's online brokerage accounts. Some of these scammers have stolen money from investors by transferring funds from the online brokerage accounts to outside accounts. "We are concerned that many investors aren't taking appropriate precautions when accessing their online brokerage accounts," said SEC Investor Education Director Susan F. Wyderko. "In our guide, we offer tips on how online investors can protect their personal information from intruders," said Wyderko.
SEC's investor guide: http://www.sec.gov/investor/pubs/onlinebrokerage.htm
Source: http://www.sec.gov/news/press/2005−158.htm

9. *November 03, IT Week* — **New laws and better authentication are being developed to combat online crime in the UK.** At a recent phishing−awareness event in London, members of financial institutions discussed the wider problems of e−crime as well as phishing attacks where crooks pose as legitimate firms or individuals to commit fraud. Struan Robertson, senior solicitor at law firm Pinsent Masons, which hosted the event, said scammers are trying new tactics −− launching attacks in new languages, for example, so while scams may be declining in number, they are becoming more sophisticated. Tom Salmond, e−crime intelligence manager with the Barclays financial crime management team, said firms must do more to combat online crime. Salmond said that insider fraud poses the biggest threat to banks and online security, second only to the threat of organized criminal gangs, who may also try to place recruits within target firms. To deal with the problem Salmond called for more cross−border and cross−sector collaboration.
Source: http://www.itweek.co.uk/itweek/analysis/2145502/catching−phi shers

10. *November 01, Department of Justice* — **Houston man pleads guilty to federal identity theft charges.** Chad Hatten, of Houston, TX, pleaded guilty to a five−count superseding indictment charging him with four counts of access device fraud and one count of aggravated identity theft, the Department of Justice and the U.S. Attorney's office for the Southern District of Texas announced on Tuesday, November 1. Hatten faces up to 52 years in prison and fines of up to $1,000,000. As part of his plea, Hatten admitted to being a member of the Shadowcrew criminal organization, an international criminal organization with numerous members that promoted and facilitated a wide variety of criminal activities including, among others, electronic theft of personal identifying information, credit card and debit card fraud, and the production and sale of false identification documents. As a member of the Shadowcrew criminal organization, Hatten used the Shadowcrew Website to engage in credit card fraud and gift card vending. In addition to possessing and using stolen credit card numbers to obtain things of value, Hatten was also charged with possessing equipment used to encode counterfeit credit cards with stolen numbers.
Source: http://www.justice.gov/opa/pr/2005/November/05_crm_582.html

[Return to top]

Transportation and Border Security Sector

11. *November 06, Associated Press* — **Pirates fire at cruise ship.** Pirates armed with grenade launchers and machine guns tried to hijack a luxury cruise liner off the eastern African coast, but the ship shifted into high gear and outran them, officials said. Two boats full of pirates approached the Seabourn Spirit about 100 miles off the Somali coast Saturday, November 5, and opened fire while the heavily armed bandits tried to get onboard, said Bruce Good, spokesperson for the Miami, FL, based Seabourn Cruise Line, a subsidiary of Carnival. The attackers never got close enough to board the Spirit, but one member of the 161−person crew was wounded by shrapnel, the cruise line president, Deborah Natansohn, said. The vessel's 151 passengers, mostly Americans with some Australians and Europeans, were gathered in a lounge for their safety, Good said. None were wounded. There has been a steep increase in piracy this year along Somalia's coastline, with 15 violent incidents reported between March and August, compared with just two for all of 2004, according to the International Maritime Bureau, a division of the International Chamber of Commerce that tracks trends in piracy.
Source: http://www.iht.com/articles/2005/11/06/news/pirate.php

12. *November 06, Star−Ledger (NJ)* — **Newark Airport security breach.** A man without a boarding pass eluded layers of security Saturday, November 5, at Newark Liberty International Airport and boarded an American Airlines flight to Miami before the flight crew realized he was there illegally, authorities said. Danis Ballard, 29, of Irvington, NJ, was escorted off the plane about 6 a.m. EST, only to then escape from American personnel, who eventually had to contact Port Authority Police, according to Tony Ciavolella, a department spokesperson. Police eventually apprehended Ballard inside the terminal and charged him with criminal trespass, Ciavolella said. Ciavolella said the FBI and region's Joint Terrorism Task Force were notified of the incident and that Ballard was detained until about 3 p.m. EST, when he was released with a summons on the trespass charge and not deemed a security threat. Authorities said Ballard showed only a printed flight itinerary, which is not an airline ticket or boarding pass. His ability to board the plane after showing only an itinerary represents a breach of security at several

critical points, according to officials familiar with the incident.
Source: http://www.nj.com/news/ledger/jersey/index.ssf?/base/news−1/113125745672070.xml&coll=1

13. *November 04, Denver Post* — **Security checks may ease .** Airport security checks may get a little less strict in coming months as the Transportation Security Administration (TSA) considers shortening its list of contraband items. The agency said it will focus more on detecting explosives than on confiscating scissors, pocketknives and other less dangerous items. The list was drawn up after the September 11, 2001, terrorist attacks, when security was significantly tightened. It includes meat cleavers, ice picks, ski poles and hammers, among other things. Under the new rules being considered by TSA, passengers may be allowed to carry small knives and scissors onto the plane, according to TSA chief Kip Hawley. Such changes could speed security lines and change the way millions of travelers pack their bags.
Source: http://www.denverpost.com/business/ci_3180829

14. *November 04, Department of Transportation* — **Train derailments lead to more detailed and frequent inspections of railroad track joint bars.** The U.S. Department of Transportation will require railroads to inspect certain types of track joint bars more frequently using new uniform standards to help prevent train derailments, U.S. Secretary of Transportation Norman Y. Mineta announced Friday, November 4. Noting that better inspection of continuous welded rail (CWR) joint bars is essential to improving rail safety, Mineta detailed the new joint bar inspection standards that railroads must incorporate into their track maintenance plans. Specifically, the interim final rule, which takes effect December 2, 2005, states that railroads must inspect CWR joint bars for visible or detectable cracks, loose or missing bolts, other damage and evidence of any rail movement. In addition, special on−the−ground visual inspections of the joint bars must be conducted on a regular schedule. Failure of CWR joint bars was identified by the National Transportation Safety Board (NTSB) as the probable cause of three serious train accidents, which resulted in two fatalities, more than 350 injuries, and the release of hazardous materials in Minot, ND, Flora, MD, and Pico Rivera, CA.
Source: http://www.dot.gov/affairs/fra2805.htm

15. *November 04, Record Net (CA)* — **California's Altamont Commuter Express installing security cameras.** Transit officials are installing new security cameras to improve safety on board California's Altamont Commuter Express (ACE). The San Joaquin Regional Rail Commission, which owns and operates ACE trains, on Thursday, November 3, hired a firm to put 110 digital security cameras throughout the ACE trains. The installation should be completed within the next 30 to 45 days. Each train car will have four security cameras that will record passengers as they enter and exit the train, said Brian Schmidt, rail program manager for ACE. There will also be cameras on the control car. Schmidt said the cameras are meant to help law enforcement officers investigate crimes that might happen aboard the train. Only police and ACE officials will view the video footage as needed. "If something occurs, you have video footage," Schmidt said. "You can transmit those photographs to other agencies." ACE operates three daily round−trip commuter trains between Stockton and San Jose, CA, with stops in Lathrop, Tracy, Livermore, Pleasanton, Fremont and Santa Clara. The train carries about 1,300 daily commuters.
Source: http://www.recordnet.com/apps/pbcs.dll/article?AID=/20051104/NEWS01/511040324/1003

16. *November 03, The Intelligencer Wheeling News− Register (WV)* — **Ohio River barge traffic locked up.** An unforeseen problem with the large chamber at the Hannibal Locks and Dam on the Ohio River on Wednesday, November 2, shut down all river traffic in the area until at least 11 p.m. EST Sunday, November 6. Jim Fregiato, a shift leader at the locks and dam, said Thursday, November 3, there were 25 tows with more than 300 barges stacked up along the river waiting to travel through the locks. He explained that the small chamber at the locks and dam had been shut down for planned maintenance when the large chamber "went out." The U.S. Army Corps of Engineers attributes this to "a failure in the miter gates" at the locks and dam.
Source: http://www.news−register.net/news/story/113202005_new03.asp

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

17. *November 05, Ledger (FL)* — **Florida crop losses at $2.2 billion.** The 2005 hurricane season dealt a $2.2 billion blow to Florida's agricultural industry, state officials reported Friday, November 4. Agricultural Commissioner Charles Bronson will meet with Congressional leaders in Washington, DC, to discuss federal relief funding for state producers. Hurricanes Dennis, Katrina, Rita, and Wilma each inflicted significant agricultural damage. Ornamental nurseries suffered the worst, with approximately $1.1 billion in crop and structural losses. Damage to the state's citrus industry totaled about $180 million; vegetable growers lost $311 million; sugar cane losses were $370 million; and aquaculture and shellfish losses totaled about $107 million.
Source: http://www.theledger.com/apps/pbcs.dll/article?AID=/20051105/NEWS/511050442/1039

18. *November 04, Animal and Plant Health Inspection Service* — **Emeral ash borer quarantined areas amended.** The U.S. Department of Agriculture’s Animal and Plant Health Inspection Service (APHIS) Friday, November 4, announced it is amending its existing emerald ash borer (EAB) regulations by adding areas in Indiana, Michigan, and Ohio to the list of quarantined areas, and is restricting the interstate movement of regulated articles from these quarantined areas. Intensive surveys conducted by APHIS, along with state, county, and city inspectors, have confirmed infestations of EAB outside the quarantined areas, specifically in parts of the Grand Traverse and Montcalm counties, MI; Lima and Newbury townships in LaGrange County, IN; and Auglaize, Fulton, Hancock, Henry, Lucas, Ottawa, Sandusky, and Wood counties, OH, prompting the need to expand the quarantine to include these areas. This action is necessary to prevent the artificial spread of EAB from infested areas in Indiana, Michigan, and Ohio to noninfested areas of the U.S. EAB is an invasive species of wood−boring beetles that targets ash trees in North America. It was first detected in July of 2002 in southeastern Michigan and has since been found in Ohio, Indiana, Maryland, and Virginia. EAB quarantines

restrict the movement of all hardwood species of firewood, nursery stock, and green lumber, among other items.
EAB information: http://www.emeraldashborer.info/
Source: http://www.aphis.usda.gov/lpa/news/2005/11/EASHBORE.html

19. *November 03, Daily Democrat (CA)* — **Salinity threatens agriculture in California.** The long−term viability of irrigated agriculture in California's highly productive San Joaquin Valley is threatened by the accumulation of salt in soils and groundwater, reports a team of researchers at the University of California, Davis. The researchers found that irrigated agriculture on the west side of the San Joaquin Valley is at risk due to the lack of fresh water, inadequate natural drainage and high water tables. The study focused on 540 square miles in western Fresno County on the west side of the San Joaquin Valley. "Our analysis shows the impacts of droughts and changes in water management on water levels and salinity, and provides insight into the long−term behavior of this irrigated agricultural system and its sustainability," Jan Hopmans, a soil hydrologist and co−investigator on the study. Salt build−up in soils and groundwater is a global problem that affects 20 to 30 percent of the world's 642 million acres of irrigated land, thus limiting world global food production. Salt is problematic for crop production because it upsets a plant's ability to take in water by its roots.
Study: Sustainability of irrigated agriculture in the San Joaquin Valley, California: http://www.pnas.org/cgi/content/full/102/43/15352?maxtoshow=&HITS=10&hits=10&RESULTFORMAT=1&andorexacttitle=and&andorexacttitleabs=and&fulltext=San+Joaquin+Valley+salinity&andorexactfulltext=and&searchid=1131291526827_1681&stored_search=&FIRSTINDEX=0&sortspec=relevance&fdate=9/1/2005&journalcode=pna s
Source: http://www.dailydemocrat.com/agriculture/ci_3178780

[Return to top]

Food Sector

20. *November 03, Food Safety and Inspection Service* — **Agencies work together to examine the jurisdiction of certain food categories.** The Food Safety and Inspection Service (FSIS) and the Food and Drug Administration (FDA) Thursday, November 3, announced a joint public meeting to discuss and solicit public comment on a consistent regulatory approach concerning the jurisdiction over certain food products. The meeting will be held December 15, 2005 in Rosemont, IL. By law, FSIS has authority over meat and poultry products. FDA has authority over all foods not under FSIS' jurisdiction. As the principal regulators, FSIS and FDA formed a working group to examine jurisdictional issues for food categories that contain meat and poultry ingredients. The group concluded that past decisions involving certain product categories are no longer consistent. For example, FSIS regulates corn dogs, while FDA regulates bagel dogs. The working group has recommended an approach that will utilize defined conditions and factors when making jurisdictional decisions for existing and future food products containing meat and poultry. Food products that primarily contain meat and poultry ingredients, such as bagel dogs, meat, and poultry−based sandwiches, and natural casings, are recommended to be regulated by FSIS. Those food products that contain meat and/or poultry as ingredients for the purpose of accentuating flavor only and do not contribute to the identity of the food product are recommended to be under FDA’s jurisdiction.

Source: http://www.fsis.usda.gov/News_&_Events/NR_110305_01/index.as p

21. *November 03, Food Safety and Inspection Service* — **Ground beef recalled.** American Fresh Foods, a Thomasville, GA, firm, is voluntarily recalling approximately 6,200 pounds of ground beef that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Thursday, November 3. The ground beef was produced on October 28, 2005 and was shipped to retail stores in Florida. The problem was discovered through company testing. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with E. coli O157:H7, a potentially deadly bacterium, can cause bloody diarrhea, and dehydration.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_047_2005_Relea se/index.asp

22. *November 02, Food and Drug Administration* — **Smoked salmon recalled.** Golden Eagle Smoked Foods of Hialeah, FL, is recalling 3672 lbs of Smoked Salmon because it has the potential to be contaminated with Listeria Monocytogenes, an organism which can call serious and sometimes fatal infections. The recalled salmon was distributed to FL, MN, NY, GA, and CA, through wholesales and distributors. No illnesses have been reported in conjunction this problem. The potential for contamination was noted after routine testing by the Florida Department of Agriculture revealed the presence of listeria monocytogenes.
Source: http://www.fda.gov/oc/po/firmrecalls/goldeneagle11_05.html

[Return to top]

Water Sector

23. *November 05, Bloomberg* — **RWE plans to sell two water utilities.** RWE, Europe's third−largest utility, plans to sell Thames Water of London, England, and the American Water Works Company of New Jersey, abandoning a five−year, $17 billion expansion that drew investments away from growing energy markets. RWE said it would start the sale of American Water first and then divest itself of Thames Water. The company, based in Essen, Germany, said it hoped to complete the sale by 2007. RWE's chairman, Harry Roels, said he had already received interest for the businesses. He said RWE would put American Water up for sale first because a deal would need approval from 10 states. RWE bought Thames Water for $9.8 billion in 2000 and acquired American Water Works for $7.5 billion in 2001.
Source: http://www.nytimes.com/2005/11/05/business/05utility.html

[Return to top]

Public Health Sector

24. *November 06, Associated Press* — **China turns to World Health Organization for bird flu help.** China said Sunday, November 6, it had asked the World Health Organization (WHO) to help it determine whether the death of a 12−year−old girl in October was caused by bird flu. If it is confirmed, it would be China's first known human death from the H5N1 strain of bird flu. Three people living in China's Hunan province came down with pneumonia from unknown causes in October following an outbreak of the H5N1 strain among local poultry, the official

Xinhua News Agency reported. The girl died three days after developing a high fever on October 13. She had had close contact with sick birds. Her 9−year−old brother was also hospitalized with similar symptoms but recovered. The third victim was a 36−year−old middle school teacher who reportedly cut raw chicken while he had a minor injury on his hand and later fell ill. All three lived in or near Wantang, a village where the government says 545 chickens and ducks died of bird flu last month. Roy Wadia, a WHO spokesperson, confirmed that China had asked the organization for help.
Source: http://news.yahoo.com/s/ap/20051106/ap_on_he_me/china_bird_f lu

25. *November 05, Associated Press* — **FEMA assessing damage to Louisiana hospitals.** The head of Louisiana's charity hospital system says both of New Orleans' public hospitals were destroyed by Hurricane Katrina and need to be replaced. A central question is how much damage was caused by the storm and how much came earlier. "We don't address the deficiencies that existed before the disaster," said David Fukutomi, the Federal Emergency Management Agency's (FEMA) infrastructure coordinator for Louisiana. FEMA decides how much the federal government will pay, whether it will pay for repairs to the aging hospital buildings or whether the facilities are damaged beyond repair and it will pay for a replacement. FEMA's payment would be the largest source of money since the hospital system, which runs nine hospitals around the state, already had been cutting services and paring its budget for years, and now has no income from the two New Orleans facilities. Engineers who assessed the damage determined that Charity was 65 percent ruined and University was 68 percent ruined. Fukutomi said a multistory facility that had several feet of water on one floor would more likely be eligible for repair rather than replacement. Fukutomi said teams have done some preliminary assessments and are still at work.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/11 /05/AR2005110500959.html

26. *November 05, Agence France Presse* — **Indonesia confirms bird flu deaths.** Indonesia has confirmed its fifth death from the H5N1 bird flu strain after tests by the World Health Organization (WHO), a hospital spokesperson said. Ilham Patu, a spokesperson for the Sulianti Saroso hospital for infectious diseases, confirmed Saturday, November 5, the death as well as another case about which he could not reveal any details. Both were confirmed by the WHO, Patu said. He said one of the two new confirmed cases was a woman, who died at a hospital in suburban Tanggerang on October 28. Before the two new cases, at least four other people had died of avian influenza in Indonesia. Three others have been confirmed as infected but have either recovered or are still being treated. Doctors at Patu's hospital were also treating as a suspected case of bird flu a nurse who had cared for the latest victim, Solati.
Source: http://news.yahoo.com/s/afp/20051105/hl_afp/healthfluindones ia_051105155914;_ylt=AkE02kcMFFxByL0VRESyKMiJOrgF;_ylu=X3oDM TBiMW04NW9mBHNlYwMlJVRPUCUl

27. *November 04, Honolulu Star Bulletin (HI)* — **Hawai`i begins first program to detect avian flu at airport.** Hawai`i is the first state to establish airport surveillance of avian flu or other viruses that may be introduced by travelers, health officials report. The program is expected to improve the state's ability to rapidly detect, characterize and respond to the threat of pandemic flu, said Catherine Chow, U.S. Centers for Disease Control and Prevention medical officer assigned to the state Health Department. Enhanced airport surveillance was initiated through an

agreement October 31 between the state Department of Health and the Queen's Medical Center, said Janice Okubo, Health Department spokesperson. The program will enable public health officials to collect nose or throat specimens from sick passengers for influenza testing, with detailed passenger information to trace contacts and begin disease control/containment activities if warranted, Chow said.
Source: http://starbulletin.com/2005/11/04/news/story05.html

28. *September 30, Government Accountability Office* — **GAO−05−984: Influenza vaccine: shortages in 2004−05 season underscore need for better preparation.** In early October 2004, the U.S. lost about half its expected influenza vaccine supply when one of two major manufacturers announced it would not release any vaccine for the 2004−05 season because of potential contamination. Although health officials took actions to distribute the limited supply of influenza vaccine, reports persisted of high−risk individuals and others in priority groups who could not find a vaccination. The Government Accountability Office (GAO) was asked to examine actions taken to ensure that high−risk individuals had access to influenza vaccine during the shortage. Health officials took several actions to help ensure that individuals at high risk of severe complications from influenza had access to vaccine. Federal officials quickly revised vaccination recommendations to target available vaccine to high−risk individuals and to other priority groups. Additional actions were aimed to distribute vaccine expeditiously and to communicate with providers and the public as events unfolded and vaccine supplies changed. Several lessons emerged. First, unless planning for problems is already in place, action is delayed. Second, when actions occur late in the influenza season, they are likely to have little effect. Third, effective response requires communication that is both clear and consistent.
Highlights: http://www.gao.gov/highlights/d05984high.pdf
Source: http://www.gao.gov/new.items/d05984.pdf

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

29. *November 05, Associated Press* — **Chertoff pushes emergency response upgrades.** Speaking to a national fire chief's leadership summit on Friday, November 4, Homeland Security Secretary Michael Chertoff said that the government should look to the private sector as a model for improving its response methods for emergencies. He said "We ought to be able to do what, you know, UPS does, or DHL, or Fed−Ex, or any other airfreight agency…in order to make sure we get things to people who need them quick." He said the Federal Emergency Management Agency (FEMA) is consulting with both government and private experts to determine how to "manage the flow of people and supplies that our first responders have a right to expect." Calling FEMA a 20th century organization, Chertoff said, "We need to be able to get information out to people and be interactive with them in a 21st century way." Chertoff said his agency has looked for new solutions to communications difficulties, such as aircraft

carrying equipment to amplify weak signals. He said "Although we have done a fair bit to prepare ourselves, we're not where we need to be…if there's an offseason for emergency management, we ought to use that."
Remarks by Secretary Michael Chertoff at the International Association of Fire Chiefs Leadership Summit: http://www.dhs.gov/dhspublic/interapp/speech/speech_0262.xml
Source: http://news.yahoo.com/s/ap/20051105/ap_on_go_ca_st_pe/cherto ff_improvements_4

30. *November 05, Associated Press* — **Spitzer lays out program to prepare New York state for dealing with terrorism.** State Attorney General Eliot Spitzer said in a speech to the Association of Fire Districts of New York on Friday, November 4, that the state needs to bolster its anti−terrorism network and better inform the public and firefighters about threats and disaster plans. He said "It's not being alarmist −− just realistic −− to say that New York can do more to protect its citizens…You can't anticipate everything, but you can develop the capability to respond to anything." Spitzer specifically called for: sharing more information on threats and disaster planning for specific events with first responders and the public; establishing a "firm chain of command" among federal, state, and local leaders before disaster hits; improving regional coordination with neighboring states; giving teachers disaster training; increasing use of the Statewide Wireless Network; ending rivalries between police and fire departments; redoubling efforts to recruit and retain first responders; working with the federal government to stockpile vaccines; engaging the public with concrete information about credible threats; expanding the Emergency Broadcast System to include a government channel for television, radio, and the Internet; seeking federalization of security at nuclear plants; establishing a comprehensive approach to securing ports; and upgrading the regional power grid.
Source: http://www.buffalonews.com/editorial/20051105/1046841.asp

31. *November 05, Associated Press* — **Illinois ready for disaster, but drill will find any weak spots.** Police and fire officials in Chicago, IL, are planning an exercise next spring that would simulate such disasters as an aerial release of chemicals in Chicago and an earthquake in southern Illinois. Officials are scouting locations for emergency shelters that can be stocked with food, water and back−up power, and experimenting with highway gates to clear lanes for emergency vehicles or give residents a way out. A method of informing the public if an evacuation was needed has not been identified. Officials say the most likely large−scale disasters are some kind of dangerous chemical release −− whether by accident or by terrorists −− in Chicago, an earthquake along the New Madrid fault in southern Illinois, or a major outbreak of disease. Carol Adams, director of the Illinois Department of Human Services, said the department has established a database of people who volunteered to help after Hurricane Katrina to call on if Illinois disaster teams need help. Illinois officials are working with neighboring states to create shelters to transfer residents, and the city of Chicago is working on an evacuation plan to help at−risk populations evacuate. The city will provide buses for those who have no means of transportation.
Source: http://www.belleville.com/mld/belleville/news/local/13091436 .htm

32. *November 03, Daily Barometer (OR)* — **Oregon State University tests emergency response.** Coordinating with other local agencies, the Oregon State University's (OSU) triage center tested its emergency preparedness and response capabilities if a disaster led to 100 students needing emergency care. The drill split up personnel into seven teams, each with its own unique set of responsibilities. One team set up signs around campus directing people to help. Another

team coordinated medical records. A triage area was staffed by a third team, where test patients were “tagged” based on the severity of their injuries. Red tag patients were sent to another team, responsible for emergency care and possible transport to the hospital. Other tag colors were offered for different levels of injury or priority, including psychological support and medicine distribution. In an emergency, a satellite system would be setup for communication with a command center located in the Alumni Center from which information would be relayed to different departments on campus in the county. The center would also aim to alleviate the call load for the hospital or Student Health Services. Steve LeBoeuf, OSU’s biological safety officer, said “This is a way to make sure things run well for the community…both in Corvallis and at OSU.”
Source: http://barometer.orst.edu/vnews/display.v/ART/2005/11/03/436 9b65d882ed

[Return to top]

Information Technology and Telecommunications Sector

33. *November 04, Security Focus* — **IBM Lotus domino multiple vulnerabilities.** IBM Lotus Domino is vulnerabile to multiple vulnerabilities. These issues can be exploited to trigger a In addition, there have also been issues with unknown impacts. These issues affect Lotus Domino versions prior to 6.5.4 Fix Pack 2. Security Focus stated that IBM has released Lotus Domino 6.5.4 Fix Pack 2 to address these issues.
Source: http://www.securityfocus.com/bid/15321/info

34. *November 04, Secunia* — **Apple QuickTime multiple vulnerabilities.** Vulnerabilities have been reported in Apple QuickTime. These can be exploited by malicious attackers to cause a Denial of Service and a compromise of a user's system. The vulnerabilites are interger overflows, a NULL pointer dereferencing error, a boundary error exists. Secunia is reporting a solution has been developed for QuickTime version 7.0.3.
Source: http://secunia.com/advisories/17428/

35. *November 04, eSecurityPlanet* — **Insider threats giving IT execs nightmares.** Sixty−nine percent of 110 senior executives at Fortune 1,000 companies say they are 'very concerned' about insider network attacks or data theft, according to a study by Caymas Systems, a network security technology firm. Only 13 percent says they are not worried at all. Sanjay Uppal, a vice president at Caymas Systems, claims 30 percent of people who come in and work on your average network every day are temporary workers. And that brings up specific threat concerns. But he also says that IT and security administrators should not forget about permanent workers and the havoc they can wreak. Uppal says insider security threats definitely need to be dealt with quickly. Uppal recommends that workers should be limited as to what parts of the network they can access. Someone working in production shouldn't be able to access financials. And someone working in the financial department, should be able to access personnel records and reviews.
Source: http://www.esecurityplanet.com/prevention/article.php/356176 1

36. *November 03, Security Focus* — **Man accused of selling bot software to compromise computers.** Federal authorities have arrested an accused man of creating bot software to

compromise nearly 400,000 Windows computers and then using his control of the systems to garner more than $60,000 in profits. James Aquilina, Assistant U.S. Attorney for the Central District of California and the prosecutor on the case stated, "This is the first case to charge someone for using bots for generating profits. On the one hand, he is selling bots to other people so that they can (perform) denial−of−service attacks and spam to make money. And on the other hand, he is using bots to make affiliate income." Over nearly a year, the man allegedly used automated software to infect Windows systems, advertised and sold access to the compromised PCs, and used the software to perpetrate click fraud, garnering tens of thousands of dollars in affiliate fees.
Source: http://www.securityfocus.com/news/11353

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available proof of concept code for an Oracle worm. Currently, US−CERT cannot confirm if this code works. We are working with Oracle to determine the threat posed by this code.

Although there is limited information concerning this potential threat, US−CERT strongly encourages Oracle system administrators to implement the following workarounds:

* Change default user credentials for Oracle installations
* Change the default port for the TNS listener
* Restrict Oracle network access to trusted hosts only
* Revoke CREATE DATABASE LINK privileges from the CONNECT role

US−CERT will continue to investigate the issue and provide updates as they become available.

For more information please review URL:
http://www.us−cert.gov/current/current_activity.htmloraclewm

Phishing Alert / Malicious Code: PayPal Traffic Redirection

US−CERT has received reports of a new attack that targets users of PayPal. The attack begins with a spoofed email phishing message that provides a link to download the executable PayPal security tool file. The executable, named PayPal−2.5.200−MSWin32−x86−2005.exe, is a Trojan Horse which modifies the DNS server of the local workstation and then deletes itself. All future requests for paypal.com will be transparently redirected to a phishing website. This same DNS

server could also be used to redirect requests for additional websites, but it currently appears to only redirect paypal.com.

For more information please see:
http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =329

XML−RPC for PHP Vulnerability Attack (NEW)

SANS is reporting, " We have received a few reports on an attack exploiting xml−rpc for php vulnerability." xml−rpc for php is used in a large number of popular web applications such as PostNuke, Drupal, b2evolution, Xoops, WordPress, PHPGroupWare and TikiWiki. When exploited, this could compromise a vulnerable system. From the submitted logs, it attempts to wget a remote access Trojan from one system and using the Trojan to try to connect to another site via port 8080. SANS has posted new information and analysis on this attack.

For more information, please see http://isc.sans.org//diary.php?storyid=823

Current Port Attacks

Top 10 Target Ports	35885 (−−−), 1026 (win−rpc), 445 (microsoft−ds), 6881 (bittorrent), 40000 (−−−), 135 (epmap), 25 (smtp), 80 (www), 27015 (halflife), 32789 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

37. *November 03, National Institute of Standards and Technology* — **'Smart' buildings to guide first responders.** The National Institute of Standards and Technology (NIST) is working with the building industry and the public safety and information technology communities to learn how "intelligent" building systems can be used by firefighters, police, and other first responders to accurately assess emergency conditions in real−time. NIST plans to develop standards to allow manufacturers to create intelligent building systems that use various types of communication networks (including wireless networks). The systems would send information such as building floor plans and data from motion, heat, biochemical, and other sensors and video cameras directly to fire and police dispatchers who then can communicate detailed information about the scene to first responders. Recently, NIST released video presentations that demonstrate how an "Intelligent Building Response" program would work. Firefighters are shown using laptops to track the spread of a developing fire on a floor plan even before reaching the scene. Other real−time building sensor information includes status information concerning a specific building's mechanical systems, elevators, lighting, security system and fire systems, the locations of building occupants, and temperature and smoke conditions. Intelligent Building Response video presentations: http://www.bfrl.nist.gov/ibr.

Source: http://www.nist.gov/public_affairs/techbeat/tb2005_1103.htm# smart

[Return to top]

General Sector

Nothing to report.
[Return to top]