Department of Homeland Security Daily Open Source Infrastructure Report for 12 December 2006

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

Daily Highlights

- The HeraldNet reports thieves, in a quest for copper wire, carted off thousands of feet of downed power lines during the recent snowstorm that struck Snohomish County, Washington, slowing efforts to restore electricity and endangering their lives. (See item 3)
- The Department of State's Bureau of Diplomatic Security in partnership with the Department of Homeland Security is distributing hundreds of wanted terrorist posters −− identifying 26 known terrorists −− at U.S. airports during the holiday season. (See item 15)
- The Department of Homeland Security has announced the results of the national interoperability baseline survey of first responders and law enforcement officials that assesses progress in achieving interoperable communications; approximately two−thirds of emergency response agencies across the nation use interoperable communications in varying degrees. (See item 30)

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. *December 11, New York Times* — **Arab nations plan to start joint nuclear energy program.** Arab leaders, meeting in the Saudi capital, Riyadh, on Sunday, December 10, said they

intended to start a joint nuclear energy development program, a move certain to heighten concerns over a possible race for nuclear power in the oil−rich Persian Gulf. Leaders of the Gulf Cooperation Council concluded a two−day summit meeting in Riyadh on Sunday, agreeing to study how to proceed with development of such capacity. Publicly, officials of the gulf council said the development of a nuclear energy program would help meet their rising demand for electricity, despite the huge oil reserves. At least six Arab countries have reportedly sought to develop nuclear power programs, including Saudi Arabia, Egypt, Morocco and Algeria.
Source: http://www.nytimes.com/2006/12/11/world/middleeast/11nuke.html?_r=1&oref=slogin

2. *December 10, Boston Globe* — **KeySpan fined $250,000 for security problems.** Massachusetts has fined KeySpan $250,000 for alleged security breaches when two people broke into its liquefied natural gas storage facility in Lynn last summer. Five days elapsed before the energy firm discovered and reported the intrusion last August, raising fears about the facility's vulnerability to terrorist attack. Company officials explained that no one had reviewed the surveillance tape, which captured the intruders using wire cutters to cut through a fence and climbing on top of the storage tank. The state Department of Telecommunications and Energy on Friday, December 8, cited KeySpan for alleged security violations and ordered the company to beef up its monitoring to prevent future break−ins. Alleged violations include not adequately maintaining the Lynn plant's security system and portions of surrounding enclosures, not conducting security patrols required under its own procedures, and not consistently training employees on security procedures. While there was no evidence the intruders were terrorists and no damage was done to the tanks, the breach raised questions of perimeter security and surveillance monitoring. Private firms that run LNG facilities are responsible for developing a security plan, which are reviewed by the Department of Telecommunications and Energy.
Source: http://www.boston.com/news/local/articles/2006/12/10/keyspan_fined_250000_for_security_problems/

3. *December 10, HeraldNet (WA)* — **Downed power lines stolen.** Thieves carted off thousands of feet of downed power lines during the snowstorm that struck Snohomish County, WA, on November 26, slowing efforts to restore electricity and endangering their lives. The theft of copper from power lines is an example of a worldwide trend of copper−wire theft that is occurring as copper prices have skyrocketed. Thieves recently stole more than 800 feet of wire from new light poles being installed in south Everett. The thieves knew what they were doing because the wires were live, said Jeret Garcia of Valley Electric. The thieves also had to be organized enough to appear as if they were a work crew that belonged in the freeway median, he said. During the snowstorm, the Public Utilities Department had more than 2,000 feet of wire taken from at least three separate locations. Another recent incident occured when a thief cut into an energized 12,000−volt primary cable at an abandoned industrial site in Maltby.
Source: http://www.heraldnet.com/stories/06/12/10/100loc_a1pud001.cf m

4. *December 08, U.S. Department of Energy* — **DOE takes next steps to expand SPR to one billion barrels.** U.S. Department of Energy (DOE) Secretary Samuel W. Bodman Friday, December 8, announced that DOE has identified the salt domes at Richton, in Mississippi, as the preferred alternative to lead the expansion of the U.S. Strategic Petroleum Reserve (SPR) to one billion barrels. This site selection adds to the SPR's geographic diversity. In addition to

Richton, DOE also proposes to expand capacity at three existing SPR sites: Big Hill in Texas, and Bayou Choctaw and West Hackberry in Louisiana. As an inland site, Richton will have less vulnerability to hurricane impacts and will be connected by pipeline to the Capline pipeline system and to refiners and marine facilities in Pascagoula for oil distribution. This new site, coupled with additional storage at the existing three SPR sites, will ensure an adequate crude oil emergency reserve. The SPR has been used a number of times as an emergency response tool, including during Operation Desert Storm in 1991, the aftermath of Hurricanes Katrina and Rita 2005, in January 2006 when the Sabine Neches shipping channel was blocked, and in June when the Calcasieu ship channel near Lake Charles, LA, was closed due to release of storm water and oil into the channel.
Source: http://www.energy.gov/news/4517.htm

5. *December 08, CBS News/Associated Press* — **Power company taken to task over outage.** Missouri and Illinois officials are calling on Ameren to explain why thousands of customers remained without power a week after a harsh winter storm and offer solutions to prevent another extended mass outage. Missouri Governor Matt Blunt on Thursday, December 7, asked his state's Public Service Commission to hold public hearings and for St. Louis−based Ameren Corp. to provide a "clear" plan for preventing a recurrence. Heading into Friday, some 19,000 Ameren customers still were without power. At the peak, more than 500,000 Ameren customers in both states were without power. Illinois Lt. Governor Pat Quinn also pressed utility regulators to investigate, calling the lingering power disruptions a "systemic failure" despite the efforts of thousands of repair workers from 14 states. On Wednesday, the Illinois Commerce Commission said it would review plans for an investigation into Ameren's preparedness and response to the storm. Ameren said it welcomed the scrutiny. "We believe we've thrown every possible resource into this," Ameren spokesperson Susan Gallagher said. She noted that repair crews trying to fix the latest outages had installed 391 miles of wire as of Thursday morning −− more than Ameren normally uses in six months.
Source: http://www.cbsnews.com/stories/2006/12/08/national/main22401 53.shtml

[Return to top]

Chemical Industry and Hazardous Materials Sector

6. *December 11, Associated Press* — **Green Bay apartment evacuated after gasoline leak.** A car leaking gasoline resulted in the evacuation of the Willow Park Apartments complex in Green Bay, WI, Monday morning, December 11. Residents were asked to remove vehicles from garages as firefighters looked for the source of the smell. It was eventually determined that a vehicle had leaked gasoline. Fire officials used a high power electrical fan to remove the smell from the building.
Source: http://www.wbay.com/Global/story.asp?S=5798186

[Return to top]

Defense Industrial Base Sector

Nothing to report.

[Return to top]

Banking and Finance Sector

7. *December 12, Arizona Daily Star* — **Four arrested in ID theft ring.** Four people have been arrested this month in connection with an identification theft ring that has victimized at least 40 people in Pima County, AZ, officials said Friday, December 8. A number of computers, fraud and identification documents, including personal IDs, Social Security cards and other documentation were seized during the service of six search warrants during the last week, said Deputy Dawn Barkman, a Pima County Sheriff's Department spokesperson. The potential loss as a result of the identity theft is more than $100,000, she said. The ring is mostly made up of heavy methamphetamine users.
Source: http://www.azstarnet.com/sn/hourlyupdate/159579.php

8. *December 11, Associated Press* — **Chinese government states eight banks have applied for retail licenses.** Eight foreign banks have applied to become the first foreign institutions licensed to handle retail business in Chinese currency, the government said, as a World Trade Organization (WTO) deadline for opening its banking market passed on Monday, December 11. Some 71 foreign banks are represented in China but most were limited until now to handling foreign currency business. Beijing agreed to open the market as part of its WTO membership. Its own banks have been racing to modernize in preparation for facing foreign competitors. Banks that have applied for retail licenses are Citigroup Inc. of the United States, Japan's Mizuho Corporate Bank, Britain's HSBC Corp. and Standard Chartered PLC, Dutch bank ABN Amro Holdings NV, Singapore's DBS Bank and Hong Kong's Bank of East Asia and Hang Seng Bank, according to the Website of the China Banking Regulatory Commission. Rules that took effect Monday give foreign banks access to the local currency retail banking business, in theory lifting all geographic and client restrictions on operations. Previously foreign banks were allowed to offer such services on a limited scale in 20 major cities.
Source: http://www.nytimes.com/aponline/business/AP−China−WTO−Banks. html

9. *December 11, Reuters* — **Internet criminals to step up "cyberwar" in 2007.** Computer hackers will open a new front in the multi−billion dollar "cyberwar" in 2007, targeting mobile phones, instant messaging, and community Websites such as MySpace, security experts predict. As people grow wise to e−mail scams, criminal gangs will find new ways to commit online fraud, sell fake goods, or steal corporate secrets. "The attacks are becoming more sophisticated," said Dave Rand of Internet security firm Trend Micro. "It's all about making money. And they're making a lot of it," he told Reuters. In 2007, hackers will be scouring social networking sites such as MySpace to gather information for more focused attacks on people's computers. "It is definitely an area that is ripe for more exploitation by malware (malicious software)," said Ed English, Trend Micro's chief technology officer for anti−spyware. Identity theft fraudsters will trawl through sites which allow people to leave their pictures and personal details, finding targets for "phishing" attacks −− fraudulent e−mails aimed at tricking people into revealing credit card numbers. Powerful new mobile phones and portable computers will also be targets as thieves try to bypass tight security to steal e−mails, documents or contacts, security firm McAfee said.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=ITFSTTOGEXS5QQSNDLPCKH0CJUNN2JVN?articleID=196602930

[Return to top]

Transportation and Border Security Sector

10. *December 11, Los Angeles Times* — **LAX radar upgrades are delayed.** Several radar upgrades that air traffic controllers say are essential to help identify potential collisions on the ground at Los Angeles International Airport (LAX) are months behind schedule. In one case, equipment that eliminates blind spots and false alarms that plague an existing collision−alert system will not be operational until 2009. Originally, the Federal Aviation Administration (FAA) slated the user−friendly system for installation this year. In another, a system that would colorize airplanes on radarscopes to distinguish whether aircraft are approaching the correct runway has yet to be installed in the air traffic control tower because of software glitches. News of the delays comes on the heels of two high−profile close calls at LAX in the last four months. The new collision−alert equipment, known as Airport Surface Detection Equipment Model X, or ASDE−X, helps controllers avert close calls on the ground by displaying a detailed picture of the 3,600−acre airfield. The FAA attributed the delays in the ASDE−X system at LAX to construction at other airports that required the agency to install the equipment at those facilities first. The existing ground radar system at LAX shows objects as blobs on a monochromatic screen and doesn't distinguish between a person, a vehicle, or an aircraft.
Source: http://www.latimes.com/news/local/la−me−lax11dec11,0,1271494.story?coll=la−home−local

11. *December 11, Associated Press* — **NJ Transit rolls out new multi−level rail cars.** The first of NJ Transit's new multilevel train cars featuring wider aisles, more leg room and no unpopular middle seats made its maiden voyage Monday, December 11. The new cars, which replace aging ones that are at least 25−years old, offer commuters more room. Each features an upper and lower seating level, as well open areas at each end equipped for wheelchairs, strollers and luggage. Seats are arranged two−by−two on the upper and lower levels, allowing more room in the aisles but no more middle seats that often serve as rest areas for briefcases and jackets. However, only commuters on the Northeast Corridor line will get to try out the cars over the next few months. More trains will appear next spring, first on the busiest lines, such as North Jersey Coast Line, Midtown Direct Service on the Morris and Essex lines and the Montclair Boonton line, said Dan Stessel, a spokesperson for NJ Transit.
Source: http://www.thnt.com/apps/pbcs.dll/article?AID=/20061211/NEWS /61211004

12. *December 09, New York Times* — **Billions later, plan to remake the Coast Guard fleet stumbles.** Four years ago the Coast Guard launched what is now a 24−billion dollar program to replace or rebuild nearly its entire fleet of planes, helicopters, and large ships. The modernization effort was a bold experiment, called Deepwater, to build 91 new ships, 124 small boats, 195 new or rebuilt helicopters and planes, and 49 unmanned aerial vehicles. The initial venture −− converting rusting 110−foot patrol boats, the workhorses of the Coast Guard, into more versatile 123−foot cutters −− has been canceled after hull cracks and engine failures made the first eight boats unseaworthy. And, plans to build a new class of 147−foot ships with an innovative hull were halted after the design was found to be flawed. The many problems delayed the arrival of any new ships or aircraft, which has compromised the Coast Guard's ability to fulfill its mission. Instead of doing it piecemeal, the Coast Guard decided to package

everything, in hopes that its multibillion price would command attention from a Congress and White House. And instead of managing the project itself, the Coast Guard hired Lockheed Martin and Northrop Grumman to plan, supervise and deliver the new vessels and helicopters. Some retired Coast Guard officials, former company executives, and government auditors fault that privatization model, saying it allowed the contractors to put their interests ahead of the Guard's.
Source: http://www.nytimes.com/2006/12/09/us/09ship.html?hp&ex=1165726800&en=bc5ef1a21f802ae9&ei=5094&partner=homepage

13. *December 08, Department of Transportation* — **DOT calls on nation's most congested cities to join fight against congestion.** Department of Transportation (DOT) Secretary Mary E. Peters on Friday, December 8, urged state and city transportation officials to respond to a request for proposals to partner with the Department of Transportation to fight traffic congestion in the nation's major metropolitan areas. Through the "Urban Partnership Agreement," the Department would provide qualified states and metropolitan areas, known as "Urban Partners," with a combination of grants, loans, credit support, regulatory relief and technical assistance to operationally test advanced technologies, such as ramp metering and real−time travel information systems, designed to reduce traffic congestion. In return, the Department's Urban Partners would be expected to research, develop and showcase strategies believed to be effective on a combined basis in actually reducing traffic congestion in the near term. Those strategies include implementation of variable rush hour pricing, otherwise known as "congestion pricing"; expanded transit services for commuters; employer commitments to expand telecommuting and/or flexible scheduling options for employees; and an expanded focus on reducing the impact of incidents, like crashing, on causing traffic tie ups. The program is part of DOT's National Strategy to Reduce Congestion on America's Transportation Network.
Highway Statistics 2005: Source: http://www.dot.gov/affairs/fhwa1406.htm
Source: http://www.dot.gov/affairs/dot11206.htm

14. *December 04, Houston Business Journal* — **Continental, New York helicopter shuttle to begin.** Continental Airlines and US Helicopter Corp. have partnered to provide shuttle service between Manhattan and its Newark hub beginning December 18. US Helicopter customers traveling on the Houston−based airline will be able to check in, receive boarding passes for US Helicopter and Continental Airlines, and complete security screening at the Manhattan heliport near Wall Street. Following the eight−minute flight to Newark Liberty International Airport, customers will arrive at Terminal C for connection to their Continental flight. A one−way ticket costs $159, plus security fees.
Source: http://houston.bizjournals.com/houston/stories/2006/12/04/da ily1.html

15. *December 04, U.S. Department of State* — **Pictures of most−wanted terrorists posted at U.S. airports.** Hundreds of wanted terrorist posters are being distributed during the holiday season to U.S. airports by the Department of State's Bureau of Diplomatic Security in partnership with the Department of Homeland Security. The poster, "The Faces of Global Terrorism," identifies 26 known terrorists with reward offers of up to $25 million as part of the Rewards For Justice program. Posters are on their way to major airports in New York City, Houston, Kansas City, Newark, Sacramento, and Washington, DC. Smaller airports across the country also requesting posters include those in Guam, Fairbanks, several cities in the Hawaiian Islands, Dayton,

Myrtle Beach, Little Rock, San Antonio, and Londonderry, NH. Over 500 English language posters have been requested by more than 30 airports with additional posters in Spanish, Japanese, Chinese, German and Korean also being sought. "Ensuring the security of our airports from terrorists requires many partnerships," said Kip Hawley, Administrator, Transportation Security Administration. "We're pleased to be teaming with the U.S. State Department and Diplomatic Security's Rewards For Justice in this vital national effort."
More information about the Rewards for Justice Program may be obtained at
http://www.rewardsforjustice.net
Tip information can be sent via e−mail to RFJ@State.gov.
Source: http://www.state.gov/m/ds/rls/77350.htm

[Return to top]

Postal and Shipping Sector

16. *December 10, Congress Daily* — **House, Senate pass landmark postal reform measure.** By voice votes in both chambers, the Senate and House approved legislation overhauling the U.S. Postal Service's rate−making operation and retirement program in the final hours of this year's session. House Government Reform Committee drafted the legislation to help satisfy Senate objections to the bills originally passed, particularly in ensuring that a new rate cap will not allow the Postal Service from raising its rates by more than the rate of inflation over the next decade. One major element of the bill is that the Postal Service will be relieved from paying retirement benefits earned by its employees during the years they were in military service. Those costs will be paid by the Treasury, lifting a burden that could have contributed to higher postal costs. "This, combined with release of escrow funds, will be used for retiree health benefits," said Postmaster General John Potter in a statement.
USPS statement on Passage of the Postal Accountability and Enhancement Act:
http://www.usps.com/communications/news/press/2006/pr06_pmg1 209.htm
Source: http://www.govexec.com/story_page.cfm?articleid=35671&dcn=to daysnews

[Return to top]

Agriculture Sector

17. *December 11, Agricultural Research Service* — **Queen bees shown to pass viruses to their offspring.** The first evidence that viruses can be transmitted vertically from mother queens to their offspring in honeybee colonies has been discovered by Agricultural Research Service (ARS) scientists. According to the researchers, this information could be used to predict bee colonies at risk of virus infection, which, in turn, would contribute to the development of effective disease−control strategies. Honeybees pollinate an estimated $15 billion worth of U.S. crops each year. The health of honeybee colonies is continuously threatened by various pathogens, with viruses posing an unknown risk because of lack of information concerning transmission and outbreaks.
Source: http://www.ars.usda.gov/is/pr/2006/061211.htm

[Return to top]

Food Sector

18. *December 11, New York Times* — **Stronger rules on produce likely after outbreaks of E. coli.** With processed produce like bagged salads and baby carrots growing in popularity in the past decade, the Food and Drug Administration (FDA) realized as long ago as 2000 that recommendations for safe handling of the products were needed. The agency went so far as to draft guidelines and kept the issue high on its priority list, but pressed by budget cuts and competing demands like drug testing, the proposal languished. Now, with the recent outbreaks of E. coli related to processed vegetables, the FDA's oversight of produce is likely to be treated with new urgency. The problems are so acute that the produce industry, long wary of regulation but stung more recently by a decline in sales, is now asking for more government oversight. No one believes that the FDA would eliminate all cases of E. coli, salmonella or other food−borne illnesses. Farmers cannot prevent wild animals from polluting their fields, for instance. But some observers believe that stronger FDA oversight of produce could reduce the number of outbreaks.
Source: http://www.nytimes.com/2006/12/11/washington/11fda.html?hp&ex=1165813200&en=a213bee893934f1a&ei=5094&partner=homepage

19. *December 11, Associated Press* — **Iowa illnesses tied to E. coli outbreak.** Nearly three−dozen people fell ill, including 14 who were hospitalized, with symptoms consistent with infection by the E. coli bacteria after eating at a Taco John's restaurant in Black Hawk County, IA, a local health department said. Test results were expected Monday, December 11. Brian Dixon, vice president of marketing for Taco John's, said the company had sent a representative to review cooking and food storage procedures, and to examine cleaning reports and employee health records.
Source: http://health.yahoo.com/news/169790;_ylt=Ano6QQBVlwTUXxVC6Gf dPKemxbAB

20. *December 10, Reuters* — **Another E. coli outbreak rattles California farmers.** California's farming industry is girding for another potential black eye after a second outbreak this year of a potentially deadly E. coli strain linked to its crops. Green onions served in Taco Bell restaurants are suspected as the source of dozens of illnesses in the Eastern U.S. and the fast−food chain has called for an industry review of the produce supply chain stretching to California. The onions came from the seaside region around Oxnard in Southern California. The latest E. coli outbreak followed a similar scare in supermarkets in September that was eventually tied to spinach grown in California's Salinas Valley. Oxnard's Boskovich Farms supplied the onions to Ready Pac Foods, a food processor for Yum Brands Inc. unit Taco Bell. Responding to food poisoning cases in recent weeks traced to its restaurants, Taco Bell tested the onions, found three samples were "presumptive positive" for E. coli O157:H7, and is no longer serving green onions at its 5,800 U.S. restaurants. While the findings are not conclusive −− Taco Bell is conducting more tests −− and Ready Pac's daily safety tests of produce it handles for Taco Bell did not show contamination, California farmers are concerned.
Source: http://today.reuters.com/news/articleinvesting.aspx?type=bondsNews&storyID=2006−12−10T165601Z_01_N10356752_RTRIDST_0_ECOLI−CALIFORNIA.XML

[Return to top]

Water Sector

21. *December 11, Associated Press* — **Main break leaves nearly 5,000 without water in Bucks County, Pennsylvania.** A water main break left nearly 5,000 residents without water for part of the weekend. Residents of Sellersville, PA, and some in adjacent West Rockhill Township, PA, were advised to boil their drinking and cooking water until early Monday afternoon, December 11, said Craig Wilhelm, Sellersville's water supply technician. Wilhelm said he received a call around 1:15 p.m. Saturday alerting him to the water main break. By the time the appropriate valves were sealed, one million gallons of water had escaped, Wilhelm said. Residents began to regain water pressure by 1 p.m. Sunday. He attributed the break to the age of the eight−inch−wide cast iron pipe. "It happens in any water system, usually when the weather changes," he said. "Older pipes get brittle in the cold."
Source: http://www.timesleader.com/mld/timesleader/16214162.htm

[Return to top]

Public Health Sector

22. *December 11, Reuters* — **South Korea says third bird flu case confirmed.** A third case of bird flu has been discovered in southwestern South Korea just as officials have completed culling hundreds of thousands of poultry from two earlier outbreaks. Last month South Korea confirmed its first cases of the H5N1 strain in about three years, saying the virus had been found at two poultry farms close to each other in the North Cholla province. The fresh case emerged after South Korea completed culling all 760,000 poultry near the two farms, raising concerns that quarantine measures had failed to control the outbreak. The third case was discovered at a quail farm in the same province about 100 miles south of Seoul. The farm has 290,000 quail and about three thousand had died over the past four days.
Source: http://health.yahoo.com/news/169786;_ylt=Aukc0t26WOCeXskgZl7 sEUamxbAB

23. *December 11, Reuters* — **Keep small birds out of chicken farms, expert says.** Poultry farms must be properly screened and protected from small birds such as sparrows, starlings and pigeons which are capable of passing the H5N1 bird flu virus to chickens, an expert said on Monday, December 11. These small birds are resident in many countries and small numbers of them have been found infected in recent years with the H5N1 virus. Leading virologist Robert Webster told Reuters his laboratory infected sparrows, starlings and pigeons with strains of the H5N1 virus isolated in Vietnam, Thailand and Hong Kong recently. His team confirmed the birds shed the virus in their stools and can therefore infect poultry. The virus replicated very well in the starling and less well in the pigeon, he added. Although all three species did not transmit the virus to their own kind, the fact that the infected starlings and pigeons did not succumb to the virus meant they could be dangerous to poultry.
Source: http://www.alertnet.org/thenews/newsdesk/SP217609.htm

24. *December 11, Canadian Broadcasting Corporation* — **Thirteenth person dies from C. difficile outbreak near Montreal.** A thirteenth person has died from a C. difficile infection at a hospital in Saint−Hyacinthe near Montreal, Canada, officials said on the weekend. More than

30 patients at the Honoré−Mercier hospital have been diagnosed with the bacterial infection since the start of July. Hospital staff said the latest victim died Friday, December 8. The hospital said it did not represent a new outbreak of C. difficile in the city. Three more patients there remain under observation, they said.
Source: http://www.cbc.ca/health/story/2006/12/10/c−difficile.html

25. *December 11, Associated Press* — **World's largest cruise ship docked after virus scare.** The world's largest cruise ship was held in port Monday, December 11, for intensive cleaning after a second outbreak of gastrointestinal illness in two voyages sickened 106 people. More than 380 passengers and crewmembers aboard Royal Caribbean's Freedom of the Seas were sickened by norovirus during a November 26−December 3 Caribbean cruise. The ship was cleaned before its next cruise, but 97 passengers and 11 crewmembers became sick with the same illness last week, officials at the Miami−based cruise line said.
Source: http://www.theglobeandmail.com/servlet/story/RTGAM.20061211.wcruisedock1211/BNStory/International/home

26. *December 07, Government Technology* — **Pandemic and All−Hazards Preparedness Act passes Senate.** Tuesday, December 5, the Senate passed S. 3678, the Pandemic and All−Hazards Preparedness Act. As part of this bill, the Secretary of Health and Human Services will be required to use information technology to create and establish a "nationwide public health situational awareness network." This network would be used for early detection and response to infectious disease outbreaks −− such as pandemic flu −− and other public health emergencies. This bill outlines several areas of importance such as increasing public awareness and vaccine tracking and distribution. The Secretary must submit a National Health Security Strategy in which federal, state and local governments are to coordinate efforts to protect public health and biosafety. This report would also include an assessment of the preparedness of federal, State, and local public health and medical capabilities.
Source: http://www.govtech.net/news/news.php?id=102760

27. *December 07, Center for Infectious Disease Research & Policy (MN)* — **Gene chip test can identify wide range of pathogens.** A new diagnostic tool that involves thousands of fragments of genetic material on a glass slide can identify a vast range of different pathogens, including viruses, bacteria, fungi, and parasites, according to a report from an international team of researchers. The "GreeneChip system" was successfully tested on samples from patients with respiratory disease, hemorrhagic fever, tuberculosis, and urinary tract infections, researchers from Columbia University and several World Health Organization reference laboratories reported last week in Emerging Infectious Diseases. The study's lead author is Gustavo Palacios of Columbia's Mailman School of Public Health in New York City. The GreeneChip is a slide with more than 29,000 probes, or short strips of genetic material, attached. "When human fluid and tissue samples are applied to the chip, these probes will stick to any closely related genetic material in the samples," the National Institute of Allergy and Infectious Diseases, which supported the research, said in a news release. "This allows the rapid and specific identification of any pathogens therein −− even those related to but genetically distinct from the ones represented on the chip."
Report: http://www.cdc.gov/ncidod/EID/13/1/73.htm
Source: http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/news/dec 0706chip.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

28. *December 10, Boston Globe* — **Boston's new chief urges review of 911 calls.** Boston's newly appointed police commissioner said Saturday, December 9, that the department's response times to 911 calls should be constantly reviewed and the deployment of officers "tweaked" to ensure callers from one neighborhood are not kept waiting longer than those in other neighborhoods. Commissioner Edward F. Davis said he had not spoken with the police supervisor in charge of deployment. But in coming weeks, he will work to decrease the amount of time it takes for officers to arrive at emergency scenes across the city, he said. Besides reviewing the numbers of officers assigned to each district, Davis said he planned to work on improving communication with 911 callers by having dispatchers let them know how long they'll have to wait before officers arrive.
Source: http://www.boston.com/news/local/articles/2006/12/10/chief_urges_review_of_911_calls/

29. *December 08, Federal Emergency Management Agency* — **President declares major disaster for Alaska.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced Friday, December 8, that federal disaster aid has been made available for Alaska to supplement state and local recovery efforts in the area struck by severe storms, flooding, landslides, and mudslides during the period of October 8−13. FEMA Director David Paulison said federal funding is available to state and eligible local governments and certain private nonprofit organizations on a cost−sharing basis for emergency work and the repair or replacement of facilities damaged by the severe storms, flooding, landslides, and mudslides in the Chugach Regional Educational Attendance Area, the Copper River Regional Educational Attendance Area, and the Kenai Peninsula Borough.
Source: http://www.fema.gov/news/newsrelease.fema?id=32046

30. *December 08, Department of Homeland Security* — **National baseline survey findings show significant levels of interoperability across the nation.** The Department of Homeland Security (DHS) announced Friday, December 8, the results of a nationwide survey of first responders and law enforcement that assesses progress in achieving interoperable communications. The national interoperability baseline survey was issued to 22,400 randomly selected law enforcement, fire response, and emergency medical services agencies, and confirms that roughly two−thirds of emergency response agencies across the nation use interoperable communications at varying degrees. Since 9/11, DHS has provided more than $2.1 billion to state and local governments for interoperable communications. Through its SAFECOM program, DHS provides research, development, testing and evaluation, guidance, tools, and templates on communications−related issues that improve emergency response

through more effective and efficient interoperable wireless communications. Additional baseline survey findings are available on the SAFECOM Website at http://www.safecomprogram.gov
DHS Fact Sheet: http://www.dhs.gov/xnews/releases/pr_1165603330445.shtm
Source: http://www.dhs.gov/xnews/releases/pr_1165602262541.shtm

[Return to top]

Information Technology and Telecommunications Sector

31. *December 11, IDG News Service* — **Project checks Java code for security bugs.** Fortify Software and the FindBugs project have launched a free service that will scan open−source Java software for bugs in the code. The Java Open Review project (JOR) lets open−source projects run audits of their source code using Fortify's source code analysis software and the University of Maryland's FindBugs tool. With developers focusing on more secure software development practices, the Java community needs more advanced bug−finding tools like JOR, said Barmak Meftah, vice president of product and services, with Fortify. "Everybody understands that the cheapest and easiest point to find and fix security bugs is at the time of implementation," he said.
JOR Project Website: http://opensource.fortifysoftware.com/welcome.html;jsessionid=ECB74504E47DB4531F9EAEF9F34ECC46
Source: http://www.infoworld.com/article/06/12/11/HNcheckjavacode_1. html

32. *December 11, CNET News* — **Second zero−day flaw found in Word.** A second security vulnerability has been discovered in Microsoft Word in less than a week. The zero−day flaw, which is could let an attacker gain remote access to a person's system, affects Word 2000, Word 2002, Word 2003 and Word Viewer 2003, according to a Microsoft security advisory posted Sunday night, December 10. Word 2007 is not affected, Microsoft said. Security provider Secunia said Monday that it is rating this latest Word security flaw as "extremely critical" because it is unpatched and because malicious attackers are currently exploiting the vulnerability.
Microsoft security advisory: http://blogs.technet.com/msrc/archive/2006/12/10/new−report−of−a−word−zero−day.aspx
Secunia advisory: http://secunia.com/advisories/23205/
Source: http://news.com.com/Second+zero−day+flaw+found+in+Word/2100−1002_3−6142531.html?tag=nefd.top

33. *December 11, CNET News* — **Microsoft pitching Vista security feature.** Microsoft is pitching a security feature in Windows Vista as a boon for consumer online safety, but others think its benefits lie elsewhere. The software maker is promoting the use of Windows Security Center, a feature in the long−awaited operating system, as a way for Websites and third−party software programs to gauge the security status of customer PCs. This could be used to deny computers that aren't fully protected access to online services, which ultimately is good for user safety, Microsoft said. Microsoft is actively pitching the possibility of the PC security checks to banks and online retailers. The feature was actually introduced in Windows XP Service Pack 2, in August 2004, but Microsoft hasn't talked about it much. Though they say Microsoft's goal is noble, others don't expect many consumer Websites or online services to start conducting PC

security checks. According to Microsoft's own data, about 70 percent of consumers aren't running up−to−date anti−virus protection. That's a large number of potential customers a business could lose, analysts said.
Source: http://news.com.com/Playing+it+safe+with+Windows+Vista/2100−7355_3−6142265.html?tag=nefd.top

34. *December 11, VNUNet* — **Mobile phone security attacks on the rise.** The number of security attacks against mobile phones is increasing dramatically, according to new data from Juniper Research. The analyst firm has identified a raft of risks that can affect mobile users, including viruses and malware. These dangers, combined with ever−tightening corporate governance rules and the increasing use of mobiles to store critical data, will prompt mobile users to install security products on 247 million mobile phones, nearly eight percent of the total, by 2011. Juniper's latest report also forecasts that mobile phone theft will continue to rise, despite initiatives by mobile operators and police forces. The analyst firm expects that nearly four percent of mobile phones will be stolen annually by 2011.
Source: http://www.vnunet.com/vnunet/news/2170690/mobile−phone−secur ity−attacks

35. *December 11, Tech Web* — **How to spot insider−attack risks in the IT department.** Nearly two−thirds of the 616 security pros surveyed this year by the Computer Security Institute say insiders account for some portion of the financial losses their organizations experience because of breaches. Insider attacks against IT infrastructure are among the security breaches most feared by both government and corporate security pros, says Eric Shaw, a psychologist and former CIA intelligence officer. The risks can be lessened first by doing background checks on potential IT employees −− something far more companies are doing this year, according to Carnegie Mellon University's CERT. If an employee is terminated, it's crucial that all system access be revoked immediately. About half of all insider attacks take place between the time an IT employee is dismissed and his or her user privileges are taken away. When it comes to current employees, IT managers must do something they might not have a taste for: Keep an eye out for insubordination, anger over perceived mistreatment, or resistance to sharing responsibility or training colleagues −− all warning signs someone may be capable of system sabotage or data theft. IT managers must be watchful any time someone with access to sensitive systems has a falling out with his or her bosses.
Source: http://www.techweb.com/news/showArticle.jhtml;jsessionid=WZ124W1VMDU5KQSNDLPCKHSCJUNN2JVN?articleID=196602853

36. *December 11, VNUNet* — **Trio convicted of $60 million software fraud.** The Department of Justice (DoJ) has won its case against three U.S. individuals accused of defrauding Microsoft of more than $60 million. A California couple was convicted on 30 counts of conspiracy, mail fraud, wire fraud and money laundering. An accomplice from Oregon was convicted on nine counts of conspiracy, mail fraud, wire fraud and money laundering. According to the DoJ, Mirza and Sameena Ali of Freemont, CA, along with Keith Griffen of Oregon City, set up and purchased a number of software distributors between 1997 and 2001 for the purpose of reselling educational software. The group used the satellite companies to participate in Microsoft's Authorized Education Reseller program, which allows academic institutions to purchase software at discounted rates. The software was then resold commercially to non−academic buyers, netting a profit of over $29 million. The DoJ said that much of the money was then laundered through estate purchases, some made in the name of Ali's son, and

over $300,000 was wired to Pakistan.
Source: http://www.vnunet.com/vnunet/news/2170606/trio−convicted−60m −software

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	31621 (−−−), 4207 (vrml−multi−use), 6881 (bittorrent), 1026 (win−rpc), 37384 (−−−), 4662 (eDonkey2000), 44113 (−−−), 1027 (icq), 1028 (−−−), 2234 (directplay) 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. *December 11, Associated Press* — **Seattle synagogues warned to increase security.** The Anti−Defamation League is sending a letter to some Seattle, WA, synagogues, asking them to increase security in light of hate e−mails the group has received after a decision by Seattle−Tacoma Airport officials to take down Christmas trees. Crews took down Christmas trees at the airport early Saturday, December 9, because a rabbi had threatened a lawsuit unless a menorah was added to the display. Robert Jacobs of the Anti−Defamation League's Pacific Northwest Regional office said the group has received hundreds of hate e−mails and forwarded the most serious threats to police. Fifteen local Jewish organizations that were threatened will be asked to boost security.
Source: http://www.kirotv.com/news/10510805/detail.html

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

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

Department of Homeland Security Disclaimer