Department of Homeland Security Daily Open Source Infrastructure Report for 01 November 2006

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

Daily Highlights

- The Associated Press reports federal authorities are investigating how a jetliner carrying more than 160 people landed on a taxiway instead of an adjacent runway at Newark's Liberty Airport on Saturday night, October 28. (See item 15)
- The U.S. Centers for Disease Control and Prevention and the U.S. Food and Drug Administration are investigating a salmonella outbreak potentially linked to produce that has sickened at least 172 people in 18 states. (See item 22)
- United Press International reports the FBI is investigating how a hacker, tapping into an employee's laptop, bypassed security and compromised the computer of a Harrisburg, Pennsylvania, water filtration plant. (See item 24)

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. *October 31, Washington Post* — **Cost−cutting led to blast at BP plant, probe finds.** BP PLC's cost−cutting efforts contributed to a Texas refinery explosion that killed 15 workers and injured 180 others in March 2005, the Chemical Safety Board (CSB) said Monday, October 30. Carolyn W. Merritt, chairman of CSB, said that BP senior management knew of "significant

safety problems" at the Texas plant and 34 other BP facilities months or years before the explosion. Budget cuts contributed to the March 2005 explosion at BP's Texas City, TX, refinery, CSB said. Merritt said that "BP implemented a 25 percent cut on fixed costs from 1998 to 2000 that adversely impacted maintenance expenditures and infrastructure at the refinery." Maintenance spending had declined throughout the 1990s, when the refinery belonged to Amoco. Once Amoco merged with BP, further cuts were imposed. BP disputed Merritt's conclusions. Company spokesperson Ronnie Chappell said that BP had boosted maintenance spending by 40 percent in the five years before the accident. Don Holmstrom of CSB said that BP's safety initiatives had "focused largely on improving personnel safety −− such as slips, trips and falls −− rather than management systems, equipment design, and preventative maintenance programs to help prevent the growing risk of major process accidents."
CSB investigation documents: http://www.csb.gov/index.cfm?folder=current_investigations&page=info&INV_ID=52
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/30/AR2006103001154.html

2. *October 30, Associated Press* — **Small fire at nuclear plant.** A small fire broke out at the Entergy nuclear power plant near Russellville, AR, Monday, October 30. The brief blaze posed no danger to the community. Entergy says the fire at Arkansas Nuclear One broke out in an auxiliary building that did not contain any radioactive material. Entergy Nuclear spokesperson Phil Fisher says an employee with a hand−held fire extinguisher put out the fire within ten minutes of its start. Nuclear Regulatory Commission officials are working with Entergy to determine the cause of the fire. Fisher says the fire, which began in an electrical panel, affected the plant's backup for its primary safety system. One of the two units at the steam electric plant continues to operate at 100 percent power. The other continues to run at 60 percent.
Source: http://www.todaysthv.com/news/news.aspx?storyid=36180

3. *October 30, Reuters* — **Columbia Gulf reports Gulf Coast natural gas line leak.** Columbia Gulf Transmission on Monday, October 30, said that a natural gas pipeline leak in the Gulf of Mexico had caused production platforms to be shut in until further notice. The leak on the Bluewater West Leg between Vermilion 245 and Pecan Island off the Louisiana Coast had shut in Columbia Gulf Transmission and El Paso Tennessee Gas Pipeline platforms. A Colombia Gulf spokesperson said there was no immediate information as to the cause of the leak, but the company was reducing pressure on the line to isolate it, shutting it down and sending a diver to check on the leak probably on Tuesday. The 4,200−mile Columbia Gulf Transmission system connects supply found in deepwater areas of the Gulf of Mexico with virtually every major producer in the Gulf, as well as to most major intrastate and interstate pipelines, serving customers throughout much of the southern U.S. Columbia Gulf also serves markets in the Midwest, East, Northeast, and Mid−Atlantic states. The 14,200−mile Tennessee Gas Pipeline system serves markets across the Midwest and mid−Atlantic regions, including major cities of Chicago, New York, and Boston.
Source: http://today.reuters.com/news/articleinvesting.aspx?view=CN&storyID=2006−10−30T200306Z_01_N30411514_RTRIDST_0_ENERGY−NISOURCE−LEAK−UPDATE−1.XML&rpc=66&type=qcna

4.

October 30, EA Technology — **IEA project to improve power transmission networks.** A new five year international collaboration program, supported by the International Energy Agency (IEA), has been launched to help countries across the world develop more energy−efficient and resilient electricity transmission and distribution (T and D) networks. The new IEA Implementing Agreement, called ENARD (Electricity Networks Analysis, Research and Development), will develop and share new technologies and best practices to help tackle challenges including replacing the aging network asset base. John Baker of EA Technology said, "Our vision is to help operators and governments across the world improve the performance of their T and D networks, with new technologies, architectures, methodologies, and operating procedures". The results will include enhanced energy efficiency, reduced environmental impact, lower costs, and greater reliability and availability of electricity to end users. ENARD will act as an authoritative source of information, expertise and advice for governments, policy makers, and industry stakeholders.
Source: http://www.processingtalk.com/news/eat/eat104.html

5. *October 30, BBC* — **Substation copper thieves hunted.** Criminals who steal copper from electricity substations across the UK are being targeted by Crimestoppers. CE Electric said the crime had cost it over $1 million over the last six months. CE Electric is now using a type of liquid to code copper in its substations. Each batch of the liquid, which is odorless and colorless, has a unique chemical formula so the rightful owner of property can be identified. CE Electric said each time thieves ransacked a substation up to 30,000 homes and businesses could be left without power. Det. Con. Kevin Mosley said, "Despite our work with the police −− installing electric fences at larger sites, monitoring CCTV, increasing security measures and regular patrols −− and thieves being badly burnt, they are still targeting our sites."
Source: http://news.bbc.co.uk/2/hi/uk_news/england/south_yorkshire/6 098686.stm

6. *October 30, Technology Review* — **More reliable power grids.** To try to make a better grid, researchers at the University at Buffalo (UB), in New York, are investigating ways to retrofit the present−day infrastructure with some new technology and communication systems. They suspect that the recent advances in nano−sensor technology and wireless networks could be key to providing an efficient way to monitor grid health and help repair damage more quickly. The idea is to disperse sensors with integrated processors and wireless capabilities throughout the grid, says W. James Sarjeant of UB. As the sensors collect information, the onboard processor would churn through the data, and transceivers would send and receive data to and from other sensor nodes. The researchers are testing if their nano−scale circuits can effectively filter out the junk signals to help detect the signatures that precede the breakdown of insulating materials in grid components. Another type of sensor undergoing exploration is called a nano hall−effect transducer. This device could sensitively detect variations in the magnetic fields generated by the system. When electric current runs through a power line, a magnetic field is produced near the line. Fluctuations detected by the sensor in the magnetic field near a power line could detect a problem.
Source: http://www.technologyreview.com/read_article.aspx?id=17673&c h=infotech

7. *October 27, Daily Nonpareil (IA)* — **Cause of Stern Oil blaze still unknown.** Fire officials and the U.S Bureau of Alcohol, Tobacco, and Firearm are investigating whether foul play was involved in a massive blaze at the Stern Oil Company, in Council Bluffs, IA, on Thursday, October 26, that took more than eight hours and a dozen fire departments to extinguish. The site

was a warehouse distribution plant used to store motor oil, cleaning solvents, and hydraulic fluids in a total of 21 storage tanks that ranged in size from 1,100 to 7,400 gallons. The fire destroyed four tanks and the loading dock. Owner Scott Stern said the blaze threatened between 125,000 and 150,000 gallons of oil that was stored on site, but the majority of the oil was not destroyed by the fire. Stern estimated the damage to the company would be in excess of $1 million.
Source: http://www.zwire.com/site/news.cfm?newsid=17386519&BRD=2703&PAG=461&dept_id=555106&rfi=6

[Return to top]

Chemical Industry and Hazardous Materials Sector

8. *October 31, WCVB−TV Boston* — **Acid spill prompts business evacuations.** In South Hadley, MA, at least eight businesses were evacuated Tuesday morning, October 31, because of a sulfuric acid spill. The accident happened on Ludlow Road in an industrial area. The road had been shut down for more than 10 hours by early Tuesday. School has been canceled in the town because the bus yard is located near the spill site.
Source: http://www.thebostonchannel.com/news/10197840/detail.html

9. *October 31, Associated Press* — **Collision between tanker and train causes kerosene spill.** A tanker truck carrying thousands of gallons of kerosene was hit by a train in Newark, NJ, as it was crossing a railroad track Tuesday morning, October 31. The truck, carrying about 7,500 gallons of the fuel, was leaving the Sunoco Oil and Gas terminal when it was hit by a Conrail engine. About half of the fuel spilled, and the Department of Environmental Protection was called in to supervise the cleanup. Officials for a short time evacuated a nearby drug treatment facility and the Sunoco terminal as a precaution. A nearby street was also closed as a result of the accident.
Source: http://www.newsday.com/news/local/wire/newjersey/ny−bc−nj−−trainaccident1031oct31,0,571595.story?coll=ny−region−apnewjer sey

[Return to top]

Defense Industrial Base Sector

10. *October 30, Federal Computer Week* — **DISA, Navy seek new approach to commercial satcom.** The Defense Information Systems Agency (DISA) wants to move to a mobile leasing approach for acquiring commercial satellite communications services for the Navy. This would be a wholesale change from the current method of purchasing individual rights to commercial satellite bandwidth. DISA issued a request for information Friday, October 27, that asks industry to come up with innovative ways to manage commercial satcom capabilities to maximize available resources and minimize cost. The Navy's new approach should pool available satcom resources across an area of coverage rather than reserving satellite capacity in advance. Currently, the Department of Defense leases transponders and reserves guaranteed numbers of links at specified data rates. This provides static capability but does efficiently manage the available resources.

Source: http://www.fcw.com/article96633−10−30−06−Web

11. *October 30, GovExec* — **IG: Iraq contractor abused rules to limit release of data.** A major Iraq reconstruction supplier has abused contracting rules by routinely marking documents as "proprietary" to shield them from public disclosure, government auditors said Friday, October 27. In a new report requested by the U.S. Embassy in Iraq (SIGIR−06−035), the Special Inspector General (IG) for Iraq Reconstruction found that KBR Inc., a subsidiary of Halliburton, has marked almost all documents produced under a contract for logistics support as "proprietary," limiting how government agencies can handle and share them. "In effect, KBR has turned [Federal Acquisition Regulation] provisions designed to protect truly proprietary information...into a mechanism to prevent the government from releasing normally transparent information, thus potentially hindering competition and oversight," the IG found. Auditors said the practice also increases the burden on contracting staff members, who must go through a challenge process to remove the label in cases where they think it is misapplied. The audit examined services provided under a cost−plus contract, in which the company is fully reimbursed for its expenses plus an additional percentage, to support military logistics at the embassy in Iraq.
IG Report: http://www.sigir.mil/reports/pdf/audits/06−035.pdf
Source: http://www.govexec.com/story_page.cfm?articleid=35373&dcn=to daysnews

[Return to top]

Banking and Finance Sector

12. *October 30, Sophos* — **Mass−spammed lottery e−mail uses BMW to dupe computer users.** IT security firm Sophos has warned Internet users of a new series of widely−distributed e−mail campaigns that pretends that the recipient has won a substantial cash prize and a new BMW car, in an attempt to steal confidential information and money. The e−mails state that recipients have won a BMW lottery and is entitled to nearly a million dollars and a brand new BMW 5 Series car. It advises recipients to contact the claims department and provides a fake corporate address, e−mail address and telephone number, to enhance the legitimacy of the message. Sophos researchers believe that the e−mails are a variant of the 419 Advanced Fee Fraud. Sophos notes that this is not the first time a major car manufacturer has been used in an email scam −− earlier in 2006, e−mails purporting to be from the Volkswagen lottery were spammed out to computer users worldwide.
Source: http://www.sophos.com/pressoffice/news/articles/2006/10/lott ery_bmw.html

13. *October 30, Sentinel (FL)* — **Fairwinds warns customers of phishing scam.** Scammers have been sending out fake "Fairwinds" e−mails, trying to trick people into disclosing their personal data. Like most modern e−mail frauds, the Fairwinds messages look very authentic, using the credit union's logo, other images, and official−sounding financial language. Ironically, one scam e−mail warns customers that Fairwinds Credit Union, an Orlando−based co−op, has discovered someone trying to hack into their online bank account. It urges customers to click on a Web link in the e−mail and follow directions to "re−validate" their account info. Another fake message alleges that someone has spent more than $2,000 using the customer's Fairwinds debit card and instructs the customer to click on a Web link to clear up the matter and protect the rest of the account. Yet another one tells people they need to "re−enroll" in Fairwinds'

online−banking system because the credit union has new security software. Each time, a cleverly constructed "spoof" Website asks for account numbers and other information that the scammers can use to clean out the customer's bank account, make unauthorized purchases, or set up fraudulent accounts using the customer's name.
Source: http://www.orlandosentinel.com/business/orl−banks3006oct30,0,1963743.story?track=rss

14. *October 27, VNUNet* — **Million−PC botnet threatens consumers.** Cyber criminals are assembling the biggest botnet for over two years −− already close to a million PCs −− according to online security experts. No one knows yet exactly what nefarious activity the army of captive PCs will be used for. But the chances are it will be a massive onslaught of phishing aimed at defrauding Web consumers in the run up to Christmas. The last time a botnet of nearly a million PCs was assembled was to launch the Netsky virus attacks in July and August 2004. Since then, botnets have been shrinking steadily to a maximum of around 20,000 PCs. This reduction is not due to better online security, but because the cyber criminals have learned that such large−scale attacks draw too much attention. "Fraud through spam and phishing is still very lucrative for cyber criminals," said Mark Sunner of MessageLabs. "We expect to see an increase in activity before Christmas when consumers are in a buying mood and more likely to be targets." Sunner says the super−size botnet is spread among computers across the globe. MessageLabs experts have watched it being assembled over the last few weeks, but don't know who is behind it.
Source: http://www.orlandosentinel.com/business/orl−banks3006oct30,0,1963743.story?coll=orl−business−headlines

[Return to top]

Transportation and Border Security Sector

15. *October 31, Associated Press* — **FAA examining why jet missed New Jersey runway.** Federal authorities are investigating how a jetliner carrying more than 160 people landed on a taxiway instead of an adjacent runway at Newark's Liberty Airport. No one was injured when the Continental Flight from Orlando, FL, landed in the wrong place Saturday night, October 28. The Boeing 757−200 should have landed on the shortest of the airport's three runways, but it instead touched down on a taxiway parallel to the runway, said Jim Peters, a spokesperson for the Federal Aviation Administration (FAA). The FAA had not interviewed the pilot and co−pilot as of Tuesday, October 31, but Continental Airlines Inc. said both pilots had been grounded. All navigational equipment and lights at the airport were working at the time, Peters said. The runways are edged in white lights, and have white lights down the center, while taxiways are bordered by blue lights, and have green lights down the center.
Source: http://www.nytimes.com/aponline/us/AP−Missed−Runway.html?hp&ex=1162357200&en=858151cf4e7fca20&ei=5094&partner=homepage

16. *October 31, Boston Globe* — **Passenger arrested after flight from Logan.** A 30−year−old man appeared in federal court in Florida on Monday, October 30, on a charge of threatening the flight crew Sunday night, October 29, on a plane with 156 passengers that took off from Boston's Logan airport and made an emergency landing in Orlando, FL. No one was hurt, but the flight crew had to wrestle with David Collyer, binding his wrists with plastic ties until the

plane could land, according to JetBlue spokesperson Todd Burke. The airliner was originally bound for Fort Lauderdale, FL. FBI agents arrested Collyer on a flight interference charge in Orlando.
Source: http://www.boston.com/news/local/articles/2006/10/31/passenger_arrested_after_flight_from_logan/

17. *October 30, Lancaster New Era (PA)* — **Pennsylvania Amtrak begins more frequent, faster service.** With music and speeches, Amtrak rolled out its faster and more frequent Keystone Corridor service on Monday, October 30. The improved service was made possible by a six−year, $145 million upgrade of the 104−mile Harrisburg−Philadelphia line. Changes include raising the number of weekday roundtrips from 11 to 14, and the number of Sunday roundtrips from six to seven, said Amtrak spokesperson Cliff Black. All of the trains will stop in Lancaster. With the track improvements, trains on the Keystone run will go as fast as 110 mph, compared to the previous top speed of 90 mph. To make the faster speeds possible, Amtrak (with funding from PennDOT and the Federal Transit Administration) made a host of improvements to the line. The work included: installing 200 miles of continuous welded rail, which provides for a smoother ride; installing 216,000 concrete ties, 48,000 wooden ties and 52 new switches; new track bed; and upgrading signal and electrification systems.
Source: http://local.lancasteronline.com/4/27275

18. *October 30, Department of Transportation* — **DOT: New approach is needed to finance air traffic controllers and safety equipment.** With Congress poised to consider Federal Aviation Administration (FAA) reauthorization legislation next year, Department of Transportation Secretary Mary E. Peters on Monday, October 30, said she will listen to all members of the aviation community as her agency grapples with how best to finance new air traffic controllers and equipment investments needed to keep pace with surging traffic in the system. During a visit to a FAA air traffic control facility in Olathe, KN, the Secretary said that the growth in air traffic was occurring just as thousands of air traffic controllers were getting set to retire. As a result, she said the federal government has plans in place to hire 11,800 new controllers over the next 10 years. New technology also is needed to ensure that incoming air traffic controllers can safely handle the increase in air traffic, Peters said. She noted that the FAA planned to install new satellite−based tracking equipment that would allow for greater precision, but that "the best plans and the most ambitious schedules won't mean a thing without a way to pay for it."
Source: http://www.dot.gov/affairs/dot10306.htm

[Return to top]

Postal and Shipping Sector

19. *October 30, Scripps Howard News Service* — **FedEx forecasts record holiday shipping season.** While retailers expect holiday spending will be up five percent, Memphis, TN−based FedEx Corp. expects it will ship 9.8 million packages, 10 percent more, on December 18, making it easily the busiest day in company history. The numbers, analysts say, prove that FedEx is stealing market share from UPS, the U.S. post office, DHL and others. On the larger front, it is also in line to pick up a windfall if now−nervous retailers start placing last−minute orders they will only be able to receive through expedited transportation companies. "Retailers

in particular and the market in general have been very careful about purchasing inventory this year," said Ted Scherck, president of Atlanta−based The Colography Group. "As a result, inventories are lean, both in warehouses and stores, and in the pipeline." If retailers need items at the last minute, they may be shipping directly to the consumer from the production facility, certainly one of FedEx's fortes. Most of that business is likely to go by FedEx Ground, which predicts a 12.5 percent increase in package volume on its busiest day. With Christmas on a Monday this year, customers will have to pay a premium for Saturday delivery, which will help boost company profits.
Source: http://www.jacksonholestartrib.com/articles/2006/10/30/news/business/a8f82ae4219fbb7a87257215002104e4.txt

[Return to top]

Agriculture Sector

20. *October 31, Agricultural Research Service* — **Chlorate compound found to quell microbes in meat animals.** A patented compound developed by Agricultural Research Service (ARS) scientists could help reduce the risk of Salmonella and Escherichia coli (E. coli) O157:H7 infection from meat or poultry products. Researchers mixed a chlorate−based compound into livestock feed or water two days before slaughter. When fed at roughly 0.5 to five percent of an animal's diet, this powder−like additive was very effective in reducing Salmonella and E. coli O157:H7 in the animal's gastrointestinal tract. To test the chlorate compound in poultry, microbiologists gave it to more than 200 market−age turkeys and 2,000 broiler chickens 48 hours before they went to processing. The incidence of Salmonella dropped from 35 percent to zero in turkeys, and from 37 percent to two percent in broilers.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

21. *October 30, Animal and Plant Health Inspection Service* — **USDA to regulate movement of articles from boll weevil quarantine areas.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service on Monday, October 30, announced a proposal to establish boll weevil regulations restricting the interstate movement of regulated articles into or through commercial cotton−producing areas. Under the proposed regulations, articles subject to the movement restrictions such as wild or ornamental cotton, seed cotton, gin trash and processing equipment must be accompanied by a permit when transiting through commercial cotton−producing states. These articles present a risk of spreading the pest because the boll weevil, if present, can survive in these materials and could possibly be transported to non−infested areas. States designated as commercial cotton−producing areas are Alabama, Arizona, Arkansas, California, Florida, Georgia, Kansas, Kentucky, Louisiana, Maryland, Mississippi, Missouri, New Mexico, North Carolina, Oklahoma, South Carolina, Tennessee, Texas and Virginia.
Source: http://www.aphis.usda.gov/newsroom/content/2006/10/bwmove.sh tml

[Return to top]

Food Sector

22. *October 30, Associated Press* — **CDC investigating salmonella outbreak.** A salmonella outbreak potentially linked to produce has sickened at least 172 people in 18 states, health officials said Monday, October 30. Health officials think the bacteria may have spread through some form of produce; the list of suspects includes lettuce and tomatoes. But the illnesses have not been tied to any specific product, chain, restaurants or supermarkets. No one has died in the outbreak, which stems from a common form of salmonella bacteria. Eleven people have been hospitalized, health officials said. The U.S. Centers for Disease Control and Prevention (CDC) detected the salmonella outbreak two weeks ago through a national computer lab system that looks for patterns and matches in reports of food−borne illness. The U.S. Food and Drug Administration has joined the investigation and will try to help trace the outbreak to its origin. Salmonella generally cause a nonfatal, diarrhea−causing illness. Other symptoms can include nausea, vomiting, abdominal cramps, fever, and headache. People can catch the infection from many different sources, including water, soil, insects, factory surfaces, kitchen surfaces, animal feces, and raw meats, poultry, and seafoods.
Source: http://www.chron.com/disp/story.mpl/ap/health/4298577.html

23. *October 30, USAgNet* — **Study warns of antibiotics used in poultry industry.** Antibiotics used to raise bigger poultry appear to increase the risk of resistance in humans who need similar drugs to treat serious infections. That's according to a study involving Marshfield Clinic researchers, who have been working with the Minnesota Health Department. The study found they could make strains of common, normally harmless bacteria resistant to antibiotics used to treat infections acquired in health care settings, such as hospitals and nursing homes. The same bacteria do not respond to other drugs. The researchers studied virginiamycin, an antibiotic that the poultry industry has long used to grow poultry to market weight faster. It is closely related to an antibiotic known as Synercid, which is used to treat health care−acquired bacterial infections.
Study abstract: http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=Pubmed&list_uids=17041845&dopt=Abstract
Source: http://www.usagnet.com/story−national.php?Id=2258&yr=2006

[Return to top]

Water Sector

24. *October 31, United Press International* — **Hacker hits Pennsylvania water system.** The FBI in Philadelphia is investigating how a hacker bypassed security and compromised the computer of a Harrisburg, PA, water filtration plant. FBI Special Agent Jerri Williams told ABC News the apparent motive in the October 9 attack wasn't to disrupt the plant's operation, but rather to use its computer to covertly distribute mass e−mails or pirated software. "The concern was high because it is a computer that controls an important infrastructure system," Williams said. The hacker originally gained access by tapping into an employee's laptop, officials said. Since the intrusion, the plant has changed all passwords to the system and eliminated home access to the system, ABC said. WaterISAC, an industry information sharing and analysis center with members from among more than 1,000 water and wastewater systems in the United States, said it was the fourth intrusion into a member's systems in the past four years. In one attack, the hacker announced entry into the system with the message: "I enter in your server like you in Iraq," the report said.

Source: http://www.upi.com/NewsTrack/view.php?StoryID=20061031−12501 1−5264r

[Return to top]

Public Health Sector

25. *October 31, Reuters* — **H5N1 strain could start wave of bird flu outbreaks.** Scientists in Hong Kong and the United States have detected a new strain of H5N1 bird flu virus in China and warned it might have started another wave of outbreaks in poultry in Southeast Asia and move deeper into Eurasia. The strain, called the "Fujian−like virus" because it was first isolated in China's southern Fujian province in March 2005, has increasingly been detected since October 2005 in poultry in six provinces in China, displacing other H5N1 strains. The strain might also have become resistant to vaccines, which China began using on a large scale from September 2005 to protect poultry from H5N1, said the scientists.
Source: http://www.alertnet.org/thenews/newsdesk/SP303161.htm

26. *October 31, Nepal News* — **Unknown disease claims 36 lives in Nepal.** Thirty−six people have died due to an unknown disease that has spread in four village development committees of the mid−western Banke district of Nepal in the last two weeks. The number of patients who are suffering from the disease has risen to 500. According to newspaper reports, most of those dead are children and the elderly. Over 36 people are in a critical condition. According to locals, viral fever, body ache, shivering and sudden unconsciousness are some of the symptoms of the "mysterious ailment." Head of the epidemic control program in the District Public Health Office in Banke confirmed that 36 people have died due to the epidemic.
Source: http://www.nepalnews.com/archive/2006/oct/oct31/news05.php

27. *October 30, Toledo Blade (OH)* — **Despite recent mumps outbreak, some universities not planning changes in vaccination policies.** Despite college students' high vulnerability to infectious diseases, freshmen entering public universities in Ohio and Michigan aren't required to show proof they've received the mumps, measles, and rubella vaccines. An outbreak of mumps that began in Iowa in December has resulted in more than 5,700 cases of mumps reported this year, according to the federal Centers for Disease Control and Prevention (CDC). By comparison, 314 cases of mumps were reported last year. For the week ending October 20, the CDC's Morbidity and Mortality Weekly Report covering select diseases reported another 75 cases in the last four weeks nationwide −− an increase "beyond historical limits." In the eight states that reported significant outbreaks, the incidence rate was highest among people ages 18 to 24. Despite the outbreak, however, several regional universities said they do not plan any immediate changes in vaccination policies for their students to require the mumps, measles, and rubella vaccines (MMR). Most of the universities contacted pointed out that there aren't specific federal requirements regarding the MMR vaccines, but they strongly encourage students to get two doses before they start college.
Source: http://toledoblade.com/apps/pbcs.dll/article?AID=/20061030/N EWS21/61030011

28. *October 30, New Scientist* — **Vaccine protects mice against MRSA superbug.** A newly developed vaccine might serve as a useful weapon against the drug−resistant superbug methicillin−resistant Staphylococcus aureus (MRSA), researchers say. Olaf Schneewind at the

University of Chicago, Illinois, and his colleagues came up with the new vaccine by identifying the bits of genetic code that eight different S. aureus strains share. This genetic analysis revealed 19 proteins that can be found on the cell surface of all eight strains. Researchers then tested what type of immune response each of these proteins could trigger in mice by injecting the proteins individually into the animals. Of the 19 tested, they selected the four protein types that elicited the greatest immune system reaction and combined them into a single vaccine. Schneewind's team then injected this combination into mice. Three weeks later they exposed the mice to different types of MRSA. All mice that received the vaccine survived exposure to the virulent MRSA strain that causes community−acquired infections in humans. By comparison, 65 percent of the control mice exposed to the same strains died. Also, while all of the control mice exposed to the hospital−acquired MRSA strain "USA100" died within 36 hours, 60 percent of vaccinated mice survived this strain.
Source: http://www.newscientist.com/article/dn10409−vaccine−protects−mice−against−mrsa−superbug.html

29. *October 30, Associated Press* — **Deadly new TB strains expose drug need.** A deadly drug−resistant new strain of tuberculosis (TB) on the rise this year has forced scientists to confront a new problem: old drugs and a more than century−old TB test that takes weeks to get laboratory confirmation. Scientists, doctors and public health specialists met in Paris on Monday, October 30, to discuss the urgent need for better tests, new drugs and a broadly effective vaccine. The TB drugs prescribed today are more than 40 years old, and they require patients to undergo a six− to nine−month treatment regimen. The U.S. Centers for Disease Control and Prevention and the World Health Organization surveyed laboratories on six continents from 2000 to 2004 and found that one in 50 TB cases around the world is resistant not only to the usual first−choice TB treatments, but also to many medications that represent the last line of defense. That classifies the disease as extensively drug resistant TB, or XDR. XDR−TB is virtually incurable with existing antibiotics. The French aid group Medecins Sans Frontieres (MSF) released an analysis Monday suggesting that none of the drugs currently in development will bring dramatic and rapid improvement to fighting TB.
MSF study: http://www.accessmed−msf.org/documents/TBPipeline.pdf
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/10/30/AR2006103000614.html

30. *October 30, Associated Press* — **Second outbreak of flu−like virus drydocks Mississippi River cruise.** Following the second outbreak in a week of a flu−like disease on board a riverboat, a Mississippi River cruise from St. Louis, MO, to St. Paul, MN, was canceled. The Delta Queen Steamboat Co. nixed its fall foliage cruise on the 520−passenger Mississippi Queen after about 12 people were treated Friday, October 27, at a Hannibal, MO, hospital. The previous weekend about 35 passengers became sick and were treated in Henderson, KY, as the boat was cruising on the upper Ohio River from Cincinnati to St. Louis. Health officials believe the gastrointestinal illness is a form of Norwalk virus.
Source: http://wcco.com/local/local_story_303222250.html

[Return to top]

Government Sector

31. *October 30, Federal Computer Week* — **Reality of HSPD−12 settles in.** The deadline for federal agencies to begin issuing computer−readable identity cards has come and gone, but it was only one step on the road to making federal buildings and information systems more secure. The October 27 deadline for complying with Homeland Security Presidential Directive 12 (HSPD−12) required agencies −− at a minimum −− to issue a standards−compliant personal identity verification (PIV) card to one agency employee. Agencies must issue the cards to all their employees and many contractor employees by October 27, 2008. Agencies must begin using the advanced capabilities of the cards by the 2008 date, too. But agencies face monumental cost and implementation hurdles. The PIV program will remain a management challenge even after the rush to distribute the cards is complete, HSPD−12 experts say. Agencies that track the HSPD−12 program said they could not reliably estimate how many PIV cards agencies have issued so far. HSPD−12 program costs will include establishing card and certificate management processes and providing building and information systems access. The October 27 deadline does not require agencies to install card readers for access to buildings.
Source: http://www.fcw.com/article96615−10−30−06−Print

32. *September 29, Government Accountability Office* — **GAO−06−1076: Homeland Security: Federal Protective Service Could Better Measure the Performance of Its Control Centers (Report).** The Department of Homeland Security's (DHS) Federal Protective Service (FPS) through its control centers (MegaCenters) helps provide for the security and protection of federally owned and leased facilities. This report (1) identifies the services MegaCenters provide, (2) determines how FPS assesses MegaCenter performance and whether FPS links MegaCenter performance measures to FPS−wide measures, and (3) examines how MegaCenters and selected organizations compare in the services they provide. To address these issues, GAO reviewed FPS's performance measures and past MegaCenter assessments, assessed the MegaCenters' performance measures, and interviewed officials and collected relevant information at FPS, the four MegaCenters, and nine selected security organizations. The Government Accountability Office (GAO) recommends that the Secretary of Homeland Security direct FPS to (1) establish MegaCenter performance measures that meet the attributes of successful performance measures, (2) develop a performance measure for the MegaCenters that corresponds to the FPS−wide performance measure of response time, and (3) routinely assess the extent to which MegaCenters meet established performance measures. DHS generally agreed with the findings and recommendations in this report.
Highlights: http://www.gao.gov/highlights/d061076high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−1076

[Return to top]

Emergency Services Sector

33. *October 30, Associated Press* — **Audit: Massachusetts' homeland security plans still inadequate.** Massachusetts' homeland security response plans are still woefully inadequate five years after the terrorist attacks of 2001, according to a report released Monday, October 30, by the state's Senate Post Audit and Oversight Committee. Committee Chairman Massachusetts Senator Marc Pacheco (D−Taunton) said the report paints a stark picture of the state's security plans. "Overall, the state must work harder to provide first responders with adequate equipment and training so that they are prepared to respond to a homeland security emergency," Pacheco

said. "We are still ill−prepared." In one of the report's key findings, Pacheco said Massachusetts has 1,124 fewer police, firefighters and emergency workers now than on September 10, 2001. Pacheco said the state must also work to improve the ability of firefighters and police officers from different cities and towns to communicate with each other quickly in the event of a major disaster. During last year's flooding when a dam in Pacheco's hometown threatened to burst, police from different communities resorted to using cellular phones to communicate, rather than reaching each other through a central command, he said.
Source: http://www.boston.com/news/local/massachusetts/articles/2006/10/30/audit_states_homeland_security_plans_still_inadequate /

34. *October 29, Intelligencer (WV)* — **Shortage of emergency personnel leads to innovative training.** In a 2002 needs assessment completed in conjunction with the Federal Emergency Management Agency, the National Fire Protection Association found that more than a quarter of volunteer fire department personnel who deliver EMS services lack formal training in those duties. The majority of those EMS personnel were not certified to the level of Basic Life Support and almost no departments had all their EMS personnel certified to the level of Advanced Life Support, according to the NFPA. This means most EMS personnel lack the ability to provide advanced airway management and intubation, manual defibrillation, intravenous access and drug therapy. But Jay Clevenger, coordinator of the Belmont Emergency Medical Services Training Program, and other local educators are working to change all that in the Upper Ohio Valley. The program offers training in the areas of Fire/EMS Heart saver (layman) plus Health Care CPR. It is the only training center between Cleveland and Athens and as far west as Columbus to offer training in Advanced Stroke Life Support. The program also provides first aid and CPR training for the counties in West Virginia's Northern Panhandle.
Source: http://www.theintelligencer.net/community/articles.asp?artic leID=12195

[Return to top]

Information Technology and Telecommunications Sector

35. *October 31, Security Focus* — **HP OpenView Storage Data Protector Backup Agent remote arbitrary command execution vulnerability.** HP OpenView Storage Data Protector Backup Agent is prone to an arbitrary command execution vulnerability. Attackers can exploit this vulnerability to execute arbitrary commands in the context of the affected process. This may aid attackers in the compromise of the underlying system; other attacks are also possible.
Vulnerable: HP OpenView Storage Data Protector 5.5 and HP OpenView Storage Data Protector 5.1.
Solution: The vendor has released an advisory along with fixes to address this issue. For further information on obtaining and applying fixes:
Source: http://www.securityfocus.com/bid/19495/references

36. *October 31, VNUNet* — **Security firm warns of Halloween malware.** Web filtering and security firm Websense has warned Internet users to be aware of online scammers seeking to exploit this year's Halloween celebrations. Users may encounter one of these malicious sites when searching Google for Halloween items. Websense has described one instance of these scams as the classic "typo−attack" in which cyber−criminals create links to Webpages that host

malware. The sites take advantage of commonly mistyped word searches such as "halkoween" instead of "halloween." These Websites often advertise Halloween−related details in their titles, but actually contain dangerous spyware which could log user activity on the Web.
Source: http://www.vnunet.com/vnunet/news/2167612/websense−halloween −malware

37. *October 31, Reuters* — **Microsoft sues counterfeit software dealers.** Microsoft Corp. said on Tuesday, October 31, it had started 55 legal actions around the world against dealers it accuses of selling counterfeit software online, its largest enforcement effort to date. "Today's announcement marks...the first time the company has focused its efforts worldwide to bring legal action against online dealers," the U.S.−based software company said in a statement. "Counterfeit software is defective and dangerous because counterfeiters tamper with the genuine software code, which leaves the door open to identity theft and other serious security breaches," Matt Lundy, a senior attorney at Microsoft, said in a statement. Microsoft analyzed counterfeit Windows XP programs in June this year and said it found that 34 percent of the disks could not be installed on a computer, and another 43 percent contained additional programs, or binary code, that are not part of the operating system.
Source: http://www.eweek.com/article2/0,1895,2047861,00.asp

38. *October 31, Sophos* — **Stration worm cracks Sophos' top 10 malware threat list for October.** Sophos has revealed the most prevalent malware threats and hoaxes causing problems for computer users around the world during October 2006. The report shows that while the well−known Netsky−P has proved once again to be the most prevalent piece of malware in circulation, variants of the Stratio worm (also known as Stration or Warezov) have entered the top ten for the first time. Several hundred variants of the worm were widely spammed out during the month, on some days accounting for more than 50 percent of all reported malware. The proportion of infected e−mail continues to remain low, at just one in 300 (0.34 percent), while during October Sophos identified 3,076 new threats, bringing the total number of malware protected against to 193,821.
Source: http://www.sophos.com/pressoffice/news/articles/2006/10/top−ten−virus−october−2006.html

39. *October 30, IDG News Service* — **New attack can disable XP firewall.** Hackers have published code that could let an attacker disable Windows Firewall on certain Windows XP machines. The code, which was posted on the Internet early Sunday morning, October 29, could be used to disable Windows Firewall on a fully patched Windows XP PC running Windows' Internet Connection Service (ICS). This service allows Windows users to essentially turn their PCs into routers and share their Internet connections with other computers on a LAN. It is typically used by home and small−business users. The attacker could send a malicious data packet to another PC using ICS that would cause the service to terminate. Because this service is connected to the Windows firewall, this packet would also cause the firewall to stop working, said Tyler Reguly, a research engineer at nCircle Network Security Inc.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9004616&taxonomy Id=17&intsrc=kc_top

40. *October 30, IDG News Service* — **Laptop vendors seek better battery standard.** A group of laptop vendors and battery manufacturers plan to announce a standard for making safer lithium ion batteries by June 15, 2007, in an attempt to recover from a massive series of battery recalls

in recent months. The new standard will cover "process requirements, quality control and assurance" for all forms of rechargeable lithium ion battery cells, from prismatic to cylindrical and pouch, according to the Association Connecting Electronics Industries.
Source: http://www.infoworld.com/article/06/10/30/HNbatterystandard_1.html

41. *September 29, Government Accountability Office* — **GAO−06−811: Information Security: Coordination of Federal Cyber Security Research and Development (Report).** Research and development (R&D) of cyber security technology is essential to creating a broader range of choices and more robust tools for building secure, networked computer systems in the federal government and in the private sector. The National Strategy to Secure Cyberspace identifies national priorities to secure cyberspace, including a federal R&D agenda. The Government Accountability Office (GAO) was asked to identify the (1) federal entities involved in cyber security R&D; (2) actions taken to improve oversight and coordination of federal cyber security R&D, including developing a federal research agenda; and (3) methods used for technology transfer at agencies with significant activities in this area. To do this, GAO examined relevant laws, policies, budget documents, plans, and reports. GAO recommends that the Office of Science and Technology Policy establish timelines for developing a federal agenda for cyber security research. GAO also recommends that the Office of Management and Budget (OMB) issue guidance to agencies for providing cyber security research data to repositories. In commenting on a draft of this report, OMB stated that it would review the need for such guidance.
Highlights: http://www.gao.gov/highlights/d06811high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−811

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	4662 (eDonkey2000), 6881 (bittorrent), 1026 (win−rpc), 4672 (eMule), 15281 (−−−), 25530 (−−−), 50001 (−−−), 445 (microsoft−ds), 6346 (gnutella−svc), 65530 (WindowsMite) 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

42. *October 31, USA TODAY* — **Government to mandate sprinkler systems.** The federal government wants to fill a gap in fire safety at nursing homes by requiring that about 3,500 older homes install sprinkler systems. A rule proposed by the Centers for Medicare and Medicaid Services would end an exemption in existing law that mandates sprinklers for new nursing homes but not older facilities. The exemption has left about one in five facilities nationwide without full sprinkler coverage, federal data show. Patient advocacy groups and fire officials, including the National Association of State Fire Marshals, have increased their calls

for a universal sprinkler requirement since 2003, when 31 patients died in two fires at nursing homes without sprinklers in Hartford, CT, and Nashville, TN. Since then, at least a dozen other patients have died in nursing home fires around the country, according to a USA TODAY analysis of federal statistics. In an investigation last year, the newspaper reported that about 2,300 fires are reported in nursing homes annually. Of the 18 worst nursing home fires since 1970, every one happened in a facility that lacked sprinklers in patient rooms and corridors, USA TODAY found. Those fires killed more than 200 patients.
Source: http://www.usatoday.com/news/nation/2006−10−30−sprinkler_x.h tm

43. *October 30, Associated Press* — **Man charged in Utah library explosion.** Authorities have arrested a man in connection with an explosion that damaged Salt Lake City's main library last month after finding his fingerprints on remnants of a rocket igniter. Thomas James Zajac is charged with possessing an unregistered destructive device, according to court documents unsealed Monday, October 30. He was arrested Friday in Oakbrook Terrace, IL, and remained in custody Monday, said a spokesperson for the U.S. attorney's office, Melodie Rydalch. The September 15 explosion blew a hole in a third−floor window and damaged a chair. There were no injuries, but 400 people were evacuated from the library. Authorities said a hobby shop−type rocket igniter was used to detonate a pipe bomb. Zajac's fingerprints were on file because of arrests in Ohio and Illinois, said Michael Minichino, a federal firearms agent.
Source: http://hosted.ap.org/dynamic/stories/L/LIBRARY_EXPLOSION_ARREST?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

[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