



# Department of Homeland Security Daily Open Source Infrastructure Report for 03 November 2006

Current  
Nationwide  
Threat Level is

**ELEVATED**  
SIGNIFICANT RISK OF  
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

## Daily Highlights

- The Department of Health and Human Services' Agency for Healthcare Research and Quality, in partnership with the American Academy of Pediatrics, has released a report entitled Pediatric Terrorism and Disaster Preparedness: A Resource for Pediatricians. (See item [28](#))
- The Pittsburgh Post–Gazette reports bronze flag holders, some with plaques that designate military service during America's wars, have disappeared during the past few months at cemeteries in rural southwestern Pennsylvania counties; many are being sold for the scrap metal value. (See item [38](#))
- The Associated Press reports that led by the U.S. Marshals Service, a weeklong sting code–named Operation Falcon III has arrested nearly 11,000 sex offenders, gang members, and other fugitives in 24 states east of the Mississippi River. (See item [40](#))

## DHS Daily Open Source Infrastructure Report *Fast Jump*

**Production Industries:** [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

**Service Industries:** [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

**Sustenance and Health:** [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

**Federal and State:** [Government](#); [Emergency Services](#)

**IT and Cyber:** [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

**Other:** [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – <http://www.esisac.com>]

1. *November 02, Computing* — **British Energy to boost user password security.** British Energy is installing a single sign–on system to increase security and reduce password confusion among staff. The system, which allows access to all the electricity producer's systems via one

password, will be used by all 5,500 employees when it goes live in early 2007. "People will also now stop writing down their five or six different passwords. If someone from outside the company got hold of any of those they could use them to do all kinds of damage," IT director Ian Campbell. Campbell says the system will also help British Energy when it deploys secure mobile computer systems.

Source: <http://www.vnunet.com/computing/news/2167722/british-energy-boost-user>

2. *November 02, Washington Post* — **Dominion to sell off production assets.** Dominion Resources, the nation's second largest utility owner, said Wednesday, November 1, that it would put most of its oil and natural gas production assets up for sale, and industry analysts said they could fetch more than \$15 billion. The sale would include about 5.5 trillion cubic feet of proven natural gas reserves as well as extensive prospects in the Gulf of Mexico — an unusually large amount of U.S. oil and gas reserves to be put up for sale in one chunk. Richmond-based Dominion said it would keep its older Appalachian gas holdings, 17 percent of its proven reserves and eight percent of its production, and its large natural-gas storage system. The restructuring would leave behind a firm more focused on its electric utility in Virginia, a natural gas distribution company in Ohio and electric power plants in New England, Wisconsin and other parts of the country. Dominion said it would use the cash to buy back shares, invest in power generation and transmission, and trim its \$14.4 billion in long-term debt.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/11/01/AR2006110103113.html>

3. *November 01, Reuters* — **Study: Arctic reserves won't replace OPEC crude.** There isn't enough oil under the Arctic Circle to replace crude from the Organization of the Petroleum Exporting Countries (OPEC), according to a study released on Wednesday, November 1, by analyst group Wood MacKenzie and seismic research firm Fubro Robertson. Under the circle, 233 billion barrels of oil equivalent in crude and natural gas have been discovered and 166 billion barrels of oil equivalent are thought to remain undiscovered, said the study's lead author, Andrew Latham of Wood McKenzie. Eighty-five percent of discovered reserves and 74 percent of expected reserves is made up of natural gas, Latham said. "The oil-gas mix is not ideal because remote gas is often harder to transport to markets," Latham said. "In addition, export and technology constraints are expected to delay production as a large portion of the communal gas until 2050," he said. OPEC's 11 member countries hold about two-thirds of the world's oil reserves.

Source: [http://news.yahoo.com/s/nm/20061101/sc\\_nm/energy\\_arctic\\_study\\_dc\\_1](http://news.yahoo.com/s/nm/20061101/sc_nm/energy_arctic_study_dc_1)

4. *November 01, Caribbean 360 (Barbados)* — **Barbados blackout shows utility vulnerabilities.** Barbados experienced a cross-island power failure just after daybreak Tuesday, October 31. It is believed to have been caused by a monkey climbing a high voltage pole while the backup systems failed. The blackout threw light on several aspects of the operation and vulnerabilities of the Barbados Light and Power Company (BL&P), the sole seller of electricity in the Eastern Caribbean island. Managing Director, Peter Williams, explained that the blackout occurred due to a fault on the 24,000 volt cable between the main generating plant and the central substation. Backup services which were to be provided by two 69,000 volt underground cables recently installed failed. Williams said that the cables were not operational as they were damaged during excavation associated with construction of a highway

extension. The company said that in the area where the power outage appeared to have originated there were reports of a monkey climbing a pole which carried the older high voltage cables — a 24,000 and 11,000 volt cable. The blackout severely affected businesses and has strengthened the resolve of some in the manufacturing sector to forge ahead with plans to start generating their own power.

Source: <http://www.caribbean360.com/News/Business/Stories/2006/11/01/NEWS0000003703.html>

5. *October 31, Reuters* — **Canada has enough energy for winter: regulator.** Canada's National Energy Board said on Tuesday, October 31, that it isn't expecting shortages of fuel or electricity this winter. The board said in its Winter Energy Outlook that uncertain forecasts for winter temperatures have been responsible in part for recently volatile oil, natural gas, and electricity prices. In natural gas markets, the board expects more balanced conditions to emerge. However, the board said gas costs for users could rise as lower temperatures bring higher demand. The National Energy Board also said supplies of heating oil and propane are adequate to meet winter's call on both fuels. Electricity supplies are also expected to meet winter demand but prices will depend on the cost of fuels.

Source: [http://ca.today.reuters.com/news/newsArticle.aspx?type=busin  
essNews&storyID=2006-10-31T222753Z\\_01\\_N31252515\\_RTRIDST\\_0 BU  
SINESS-ENERGY-CANADA-FORECAST-COL.XML&archived=False](http://ca.today.reuters.com/news/newsArticle.aspx?type=busin essNews&storyID=2006-10-31T222753Z_01_N31252515_RTRIDST_0_BU SINESS-ENERGY-CANADA-FORECAST-COL.XML&archived=False)

[[Return to top](#)]

## **Chemical Industry and Hazardous Materials Sector**

6. *November 02, Post-Standard (NY)* — **Mall evacuated after gas line break.** A break in a natural gas line Thursday, November 2, forced the evacuation of DeWitt, NY's ShoppingTown Mall. A two-inch gas main ruptured during renovation work. A 15-mph wind blew the gas into the building. Fearing an explosion, firefighters evacuated the building and area police officers blocked the entrances to the building. There is no fire or report of injuries.

Source: [http://www.syracuse.com/news/updates/index.ssf/?mtlogs/syr\\_p  
oststandard/archives/2006\\_11.html#200393](http://www.syracuse.com/news/updates/index.ssf/?mtlogs/syr_p oststandard/archives/2006_11.html#200393)

[[Return to top](#)]

## **Defense Industrial Base Sector**

7. *November 02, Aviation Week* — **Satellites and UAVs should collaborate, not compete: Air Force general.** Collection and transportation of data in the military's future net-centric domain is a job that both space-based satellites and unmanned aerial vehicles (UAVs) can lay claim to — but the two platforms should collaborate for equipment and technology instead of competing for missions, says Lt. Gen. Michael Hamel, commander of the U.S. Air Force Space Command's Space and Missile Systems Center. The two should be looking for ways to complement one another, he said. The priority should be to make sure sensors, antennas and other equipment are applicable for both space and air platforms, he said. Those working on the programs need to make sure they find complementary ways to process and fuse data. That will

become increasingly important as the multitude of sensors grows and the net-centric military future takes hold. Collecting and moving data will be the wave of the future for unmanned systems and the space community, Hamel said.

Source: [http://www.aviationnow.com/avnow/news/channel\\_netdefense\\_story.jsp?id=news/SATU11026.xml](http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/SATU11026.xml)

8. *November 02, Reuters* — **Air Force to create cyberspace command.** The U.S. Air Force plans to set up what could become a major command aimed at safeguarding U.S. military and civilian cyberspace, Air Force Secretary Michael Wynne said on Thursday, November 2. Wynne said the new command would be part of the 8th Air Force based at Barksdale Air Force Base in Louisiana. The mission of bombers now within the 8th Air Force would remain, and the new cyber-command reflects the Air Force's growing reliance on computer networks, data and electronic warfare. Wynne said he hoped the new command would eventually be on par with such major Air Force units as the Space Command and the Air Combat Command. In creating what could become a unit led by a four-star Air Force general, the Air Force would set the stage for significant budget resources and congressional interest. The Air Force will seek funding for the cyber-command in fiscal 2009, which begins October 1, 2008, he said.
- Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/11/02/AR2006110200613.html>

[[Return to top](#)]

## **Banking and Finance Sector**

9. *November 02, Associated Press* — **Area veterans' personal data reported lost.** Three computer disks containing the Social Security numbers and other personal information of about 1,400 veterans treated at a McAlester, OK, clinic are missing, federal officials said. The Veterans Affairs Hospital in Muskogee, OK, confirmed the loss in a letter mailed Tuesday, October 31, to patients of the McAlester clinic. The lost information includes patients' names, Social Security numbers, amount billed, and amount paid for services they received at the outpatient clinic, which operated through a contract with the Choctaw Nation. The hospital says there is no information to indicate this personal information has been misused. The disks were mailed May 10, June 10, and July 10. The hospital did not notify veterans earlier because it had to wait for officials in Washington to approve the wording of the letter, she said, which didn't come until October 26.
- Source: [http://www.tulsaworld.com/NewsStory.asp?ID=061102\\_Ne\\_A6\\_Area\\_v63279](http://www.tulsaworld.com/NewsStory.asp?ID=061102_Ne_A6_Area_v63279)
10. *November 01, Associated Press* — **Study: One in four say financial, personal information stolen.** More than one in four Americans say their financial or personal information has been stolen, sometimes by someone they knew, according to a survey released Tuesday, October 31. The study done for Experian, the credit rating agency, found that about 19 percent of consumers report that financial information, including a bank or credit card number, has been misused. About 14 percent say they've had personal information such as a Social Security number or birth certificate taken. The survey, conducted by The Gallup Organization, also found that some consumers were more likely to be victimized than others. Among the prime targets were college graduates, those with annual household income of \$75,000 or more, people residing in the West, and Americans between the age of 30 and 49. The study also found that about one-fifth

of those who suffered the theft of financial or personal data knew the person who stole their information.

Source: <http://www.nasdaq.com/aspxcontent/NewsStory.aspx?cpath=20061031%5cACQDJON200610311911DOWJONESDJONLINE000948.htm&>

11. *November 01, Daily Press (VA)* — **Data-rich computer stolen from Fort Monroe.** A laptop containing personal information about 4,600 high school seniors from across the country was stolen last week from the U.S. Army Cadet Command's headquarters at Fort Monroe, VA, a spokesperson confirmed Tuesday, October 31. The students are applicants for the Army's four-year ROTC college scholarship. Their applications included their Social Security numbers, birth dates, home addresses, phone numbers, parents' names, and mother's maiden names. A database containing that information was on the missing computer. Military police are investigating the incident. It's unlikely that anyone will be able to access the personal information to exploit it, due to security measures installed on the laptop, said command spokesperson Paul Kotakis. While there were no indications that the information had been tampered with as of Tuesday, the command has notified the 4,600 students and their families of the theft.

Source: <http://www.dailypress.com/news/local/dp-67405sy0nov01.0.3737661.story?coll=dp-news-local-final>

12. *November 01, Computerworld* — **MasterCard tackles PIN-based debit card fraud.** MasterCard Worldwide will introduce in the first quarter of 2007 a new service to help banks and other card issuers detect and stop PIN-based debit card fraud in real time. The service is the company's first offering designed to help card issuers detect debit card fraud at ATMs and point-of-sale systems during the authorization process. MasterCard's new service addresses a definite need, said Avivah Litan, an analyst at Gartner Inc. Even so, it is unclear how successful the company will be in getting banks and other issuers to sign up for the service, she said. "But MasterCard, along with Visa, is in a better position to see networkwide transactions," which can be an advantage in detecting fraud, Litan said. MasterCard's Online Fraud Monitor service will use a proprietary risk-scoring model that will look at factors such as account spending, transaction histories, and device-level activity to calculate the likelihood of fraud on an individual ATM transaction. For instance, if a card that in the past has been used only domestically were to be used in a large transaction in a foreign country, the transaction would automatically be flagged as high-risk for follow-up action.

Source: <http://www.computerworld.com/action/article.do?command=printArticleBasic&articleId=9004681>

13. *November 01, Times Online (UK)* — **Visa voucher to combat Internet fraud.** Shoppers are set to bamboozle Internet scammers with a new Visa voucher which allows them to change their card details every time they spend money online. Each 3V voucher comes with its own 16-digit number. Once a shopper buys a voucher, a matching expiration date and security code is texted to their mobile phone. These details will be accepted by online retailers as a Visa credit or debit card payment. Kieron Guilfoyle, of 3V Transaction Services, the Irish firm which created the vouchers in association with Visa, said: "The launch of 3V vouchers is great new for people in the UK who want to shop online but don't want to because of the fear of fraud or going into the red." More than 60,000 customers signed up for the vouchers during a yearlong pilot in Ireland and they are to be launched in Europe next year.



Source: <http://technology.timesonline.co.uk/article/0,,20411-2432121,00.html>

[\[Return to top\]](#)

## **Transportation and Border Security Sector**

14. *November 02, USA TODAY* — **Bonuses don't stop turnover for TSA.** An ambitious program that paid the nation's airport screeners \$18 million in bonuses as an enticement to stay in their jobs did not reduce the turnover rate at the Transportation Security Administration (TSA), which still has one of the highest attrition rates in the U.S. government, according to agency data. The TSA has battled high turnover among screeners since the agency was formed after the September 11 attacks. It is looking for ways to curb a staffing problem that has lengthened lines at airport checkpoints. The TSA began paying 36,000 of its 45,000 screeners "retention bonuses" of \$500 or \$1,000 each in May. The turnover rate over the summer was unchanged from the winter and spring months, according to the TSA and the federal Office of Personnel Management. The TSA acknowledges the attrition problem and is taking additional steps such as creating screener jobs with salaries up to \$56,700 that will focus on detecting bombs or identifying suspicious passengers. TSA has maintained that screeners with more experience are better at finding weapons at checkpoints.

Source: [http://www.usatoday.com/travel/news/2006-11-01-screeners\\_x.htm](http://www.usatoday.com/travel/news/2006-11-01-screeners_x.htm)

15. *November 02, Boston Herald* — **Airline wins WiFi war at Logan: FCC sides with Continental.** The Federal Communications Commission (FCC) has sided with Continental Airlines in its battle to continue to offer its own WiFi Internet service at Boston's Logan International Airport. The FCC ruled on Wednesday, November 1, that the Massachusetts Port Authority's attempt to block other entities from offering wireless Internet service violated FCC rules that allow businesses and consumers to install WiFi antennas without landlord approval. "Today's decision ensures that the WiFi bands remain free and open to travelers, who can make productive use of their time while waiting to catch their next flight in an airport," FCC Commissioner Michael Copps said in a statement. Unless Massport appeals, the FCC ruling ends a two-year battle that pitted the agency against Continental and others that petitioned the FCC on its behalf, including American Airlines, T-Mobile, and the Media Access Project.

Ruling: [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-06-157\\_A1.doc](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-157_A1.doc)

Source: <http://business.bostonherald.com/businessNews/view.bg?articleid=165300&src=biz>

16. *November 02, Associated Press* — **Northwest discounts holiday tickets.** Northwest Airlines launched a holiday fare sale on Thursday, November 2, including a handful of "Super Bargain Days" aimed at filling its planes during November and December. It's the first time in two years Northwest has launched a domestic fare sale. The cheapest fares require travel on Thanksgiving or the day after, with a return trip the following Wednesday. The other "Super Bargain Day" falls on Christmas. Northwest runs some of the fullest planes in the business. In September, its mainline domestic flights ran 78.6 percent full. But spokesperson Kurt Ebenhoch said the airline believed it could improve its performance on some of its slower days. Airlines generally have been raising fares because of fuel prices.

Source: [http://www.usatoday.com/travel/flights/2006-11-02-nwa-fare-sale\\_x.htm](http://www.usatoday.com/travel/flights/2006-11-02-nwa-fare-sale_x.htm)

17. *November 01, Pacific Business News* — **Hawaiian Airlines reports profit.** Hawaiian Airlines said it earned \$7.8 million in the third quarter, despite a bruising fare war and continued high fuel prices. The earnings were roughly the same as in the third quarter of 2005, though operating revenue increased three percent to \$230 million, up from \$224 million in the previous year. The airline said a 19 percent increase in jet fuel costs cut sharply into earnings and resulted in operating expenses increasing to \$217 million for the quarter, up from \$206 million in the same period last year. Hawaiian also said that its efforts to improve fuel efficiency resulted in a one percent decrease in fuel consumption, even as its aircraft were flying more hours.

Source: <http://biz.yahoo.com/bizj/061102/1369756.html?.v=5>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

18. *November 02, Louisville Business First (KY)* — **UPS Trade Direct goes to Japan.** United Parcel Service Inc. (UPS) has begun its first inbound Trade Direct service in Asia. The Atlanta-based package shipper has debuted its UPS Trade Direct service inbound to Japan, making the service available from 50 origin countries in North America, Europe and Asia. The Japan service is the first Trade Direct inbound lane to be opened in Asia by UPS. UPS Trade Direct is an international freight service that combines air or ocean freight transportation and customs clearance with package and less-than-truckload service for final delivery. UPS said the service offers faster transit and the ability to bypass traditional warehouses and distribution centers because shipments can go directly from airplane or ship into the local UPS delivery network. UPS introduced the service in 2002.

Source: <http://louisville.bizjournals.com/louisville/stories/2006/10/30/daily33.html>

[\[Return to top\]](#)

## **Agriculture Sector**

19. *November 01, Purdue University* — **Purdue wrap-up says viable soybean rust spores can move long distances in a short period of time.** Asian Soybean Rust reached as far north as Indiana via the Mississippi Delta area. A weather-based spore dispersal and deposition model indicated that from September 22 through 24, spores from the Delta region were carried up the Mississippi Valley into southeastern Illinois and much of Indiana. Since late September, when the dispersal model predicted spores were being transported north from the Delta area, rust has been found in 26 counties in Arkansas, 17 in Tennessee, 18 in Kentucky, four in Missouri, eight in Illinois, and six in Indiana. The timing of discoveries of rust in the mid-South and Midwest indicates that all of these infections arose from a major dispersal event that originated in Louisiana. The events of this fall suggest that viable spores can move long distances in a short period of time. If rains that scrub spores out of the air accompany a long-distance dispersion, rust can appear simultaneously over a large area. If the events of late September 2006 were to occur several weeks earlier in a growing season, there could be a major outbreak of rust when the crop is still vulnerable.

Purdue Plant and Pest Diagnostic Lab: [http://www.ppd.l.purdue.edu/PPDL/soybean\\_rust.html](http://www.ppd.l.purdue.edu/PPDL/soybean_rust.html)

Source: [http://www.agry.purdue.edu/ext/coolbean/PDF-files/End\\_of\\_Season\\_2006\\_Soybean\\_Rust.pdf](http://www.agry.purdue.edu/ext/coolbean/PDF-files/End_of_Season_2006_Soybean_Rust.pdf)

20. *November 01, Associated Press* — **Pratt Livestock tests new cattle ID system.** Modern technology is invading the traditional cattle auction, as the industry tries to respond to concerns about an animal disease outbreak, or a terrorist attack on the nation's food supply. This week at the Pratt Livestock auction ring in Kansas, 500 of the 6,000 cattle auctioned off wore electronic identification tags in their ears, which emit radio signals. The cows also have a computer chip that stores the animal's 15-digit I-D number. It's part of a national effort to test a system that would allow the government to find millions of head of cattle within 48 hours of some type of disease outbreak or terrorist attack.

Source: <http://www.wibw.com/home/headlines/4539501.html>

[[Return to top](#)]

## **Food Sector**

21. *November 01, Associated Press* — **South Carolina salmonella outbreak linked to boiled peanuts.** Two-dozen people sickened with salmonella in South Carolina likely ate bad boiled peanuts from the mid-October Pumpkin Festival in Pickens County, state health officials say. "We never heard of salmonella in boiled peanuts before. It appears to be an isolated, very unusual event," Department of Health and Environmental Control spokesperson Adam Myrick said. While the boiling would have killed any of the bacteria on the peanuts, salmonella could have ended up back on the nuts during refrigeration, packaging or shipping, Myrick said.

Source: <http://www.wilmingtonstar.com/apps/pbcs.dll/article?AID=/20061101/APN/611012123>

[[Return to top](#)]

## **Water Sector**

22. *November 01, Associated Press* — **Toxic oil spill in north China river cuts water supplies.** An overturned truck spilled 33 tons of toxic oil into a river cutting water supplies to 28,000 people in northern China, state media said Wednesday, November 1. The overloaded truck was carrying wash oil, also known as creosote, when it overturned and dumped its contents into a river in Shanxi province, Xinhua News Agency reported. An investigation showed the truck overturned due to brake failure, the report said. The spill flowed into the Yangjiapo reservoir, contaminating 70 million cubic feet of water, the agency said, citing the provincial environmental bureau. The spill occurred October 26, Xinhua said, but did not say why it was reported a week later. Cleanup crews were using pumps, tons of activated carbon and other materials to absorb the spill. Authorities were trucking in drinking water to affected residents, and were trying to connect water pipes to a large well in the nearby village of Mahui, Xinhua said. Most of China's canals, rivers and lakes are severely tainted by agricultural and household pollution.

Source: <http://www.cbsnews.com/stories/2006/11/01/ap/world/mainD8L4DNVO1.shtml>



## **Public Health Sector**

23. *November 02, Reuters* — **China says no evidence of new bird flu strain, refuses to share virus samples.** China has found no evidence of a new strain of H5N1 bird flu in its southern provinces and said on Thursday, November 2, there was no need to share virus samples with the World Health Organization (WHO). Scientists in Hong Kong and the United States said in a report released this week they had detected a new strain of bird flu. But China rejected the report, saying there was no evidence of major changes to the virus since 2004. However, the WHO says its understanding of the virus and how it might be changing is being hampered by the fact China has not shared animal virus samples since 2004. "It's our understanding that there have been certainly changes in the virus and continual evolution in the virus since 2004 and the viruses that we requested from 2005 have still not been shared with WHO," said Julie Hall, the WHO's bird flu coordinator in Beijing. The point was not whether there were major differences in virus strains, she said: it was about being able to keep abreast of changes, however minute, to better understand how the virus is developing.  
Source: <http://www.alertnet.org/thenews/newsdesk/PEK282865.htm>
24. *November 02, Bloomberg* — **Bird flu–infected dog suggests human risk from pets: study.** Bird flu infected organs of a dog in Thailand before killing the animal, highlighting the potential for pets to contract the lethal virus and potentially spread it to humans, researchers in the country said. The dog probably picked up the H5N1 avian influenza strain from infected duck carcasses in the central Thai province of Suphanburi two years ago, the researchers said in a study published in this month's Emerging Infectious Diseases journal. Five days after feeding on the carcasses, the dog developed high fever, panting and lethargy, and died a day later. The virus was found in the dog's lung, liver, kidney and urine, providing more evidence of the ability of H5N1 to cross the species to infect mammals, the study said.  
Study: <http://www.cdc.gov/ncidod/EID/vol12no11/06-0542.htm>  
Source: <http://www.bloomberg.com/apps/news?pid=20601087&sid=aOLf4luHzaXA&refer=home>
25. *November 02, WCVB–TV Boston* — **Whooping cough reported at Boston hospital.** A patient and 15 workers at the Children's Hospital in Boston have been diagnosed with whooping cough. Sixty other Children's staff members are being tested to see if they also have the highly contagious bacterial disease, spread by coughing and sneezing, said Dr. Anita Barry of the Boston Public Health Commission. Those workers are staying home until they finish a five–day antibiotic treatment, said Dr. Thomas Sandora, an epidemiologist at Children's Hospital. Sandora also said the hospital has sent letters to the parents of about 1,000 patients who may have come in contact with the potentially infectious workers.  
Source: <http://www.thebostonchannel.com/health/10216655/detail.html>
26. *November 01, Ashley County Ledger (AR)* — **CDC investigating chicken pox outbreak in highly–immunized groups in Arkansas.** Representatives from the Centers for Disease Control and Prevention (CDC) in Atlanta have been in Ashley County, AR, in connection with an outbreak of chicken pox among highly–immunized groups. Ann Wright of the Arkansas

Department of Health said that as Monday morning, October 30, that there have been 118 cases of chicken pox in Ashley County, but could not provide additional details as to the location. Wright termed the situation a "very large outbreak." She also noted that the issue is of concern because it has been in a population that has been "highly vaccinated." The CDC is investigating the outbreak to help determine the reason for the spread of the disease in groups which have been vaccinated. She said that the CDC has determined that the local sickness is definitely varicella and that the problem was not the efficacy of the vaccine. The CDC is now looking at the issue of transmission.

Source: [http://www.ashleycountyledger.com/articles/2006/11/01/news/h\\_16f103t.txt](http://www.ashleycountyledger.com/articles/2006/11/01/news/h_16f103t.txt)

27. *October 31, Jackson Hole Star-Tribune (WY)* — **Wyoming health officials warn of tularemia outbreak.** Several outbreaks of tularemia around Wyoming have state health officials cautioning hunters and recreationists to take basic precautions. Tularemia, also known as rabbit fever or deer fly fever, typically infects rabbits, hares and rodents. People and domestic animals can become infected through contact with the bacteria or through bites from deer flies. Two people in Wyoming contracted tularemia this year, said Jamie Snow, a public health veterinarian for the Wyoming Department of Health. The first, a woman in Baggs, was bitten in the hand by a cat. The feline had likely been chewing on an infected rabbit and carried the disease on, Snow said. The second victim was a Big Horn County teenager who came down with a high fever, body ache and chills after skinning an infected rabbit. In most cases tularemia can be treated with antibiotics. If left untreated, however, the bacteria can be fatal.

Source: <http://www.jacksonholestartrib.com/articles/2006/10/31/features/health/6ae94a8b7ba356558725721700567360.txt>

28. *October 27, Agency for Healthcare Research and Quality* — **New pediatric terrorism and disaster preparedness resource released.** The Department of Health and Human Services' Agency for Healthcare Research and Quality, in partnership with the American Academy of Pediatrics, on Friday, October 27, released Pediatric Terrorism and Disaster Preparedness: A Resource for Pediatricians. The resource is intended to increase awareness about the unique needs of children and encourage collaboration among pediatricians, state and local emergency response planners, health care systems, and others involved in planning and response efforts for natural disasters and terrorism incidents.

Report summary: <http://www.ahrq.gov/research/pedprep/pedterrorism.pdf>

Full-text report: <http://www.ahrq.gov/research/pedprep/pedresource.pdf>

Source: <http://www.ahrq.gov/news/press/pr2006/pedterpr.htm>

[[Return to top](#)]

## **Government Sector**

29. *November 02, Associated Press* — **Fire forces North Carolina school to close for rest of year.** A fire that began in a chemistry lab destroyed a high school, leaving more than 1,000 students without a school building for the rest of the year. A teacher spotted the fire around 2 p.m. EST Wednesday, November 1, at Eastern Guilford High School in Gibsonville, NC, and tried to put it out with an extinguisher, but then pulled the alarm. The school, which has 1,060 students, was evacuated, with students, teachers and other employees going to a nearby church. The cause of the fire was under investigation. The building was a total loss. "Those kids will

not go back to school there this year, there's no question," said Guilford County schools Superintendent Terry Grier, who met Wednesday night with school officials to decide what to do. School administrators discussed space at other nearby high schools but did not decide where the students will go for the rest of the year. Gibsonville, 15 miles east of Greensboro, has about 4,600 residents. Its school district is the third largest in the state, with 116 schools, including about two dozen other high schools.

Source: [http://www.usatoday.com/news/nation/2006-11-02-school-fire\\_x.htm](http://www.usatoday.com/news/nation/2006-11-02-school-fire_x.htm)

[\[Return to top\]](#)

## **Emergency Services Sector**

### **30. *November 02, Pittsburgh Tribune-Review* — County starts emergency audit of 911 system.**

Allegheny County, PA, has begun an emergency audit of the county's 911 system in response to last week's call center failure, county Controller Mark Patrick Flaherty's office said Wednesday, November 1. "This is something that should be given priority," said the controller's spokesperson, Pam Goldsmith. "A glitch is just not acceptable as an explanation. We have to find the cause." The audit will examine whether the county is properly using state money to upgrade its emergency system. The county's emergency dispatch center in Point Breeze missed about 100 calls over six hours on October 25 because of a computer failure.

Source: [http://www.pittsburghlive.com/x/pittsburghtrib/news/today/s\\_477768.html](http://www.pittsburghlive.com/x/pittsburghtrib/news/today/s_477768.html)

### **31. *October 30, Associated Press* — Red Cross announces post-Katrina management overhaul.**

The American Red Cross announced plans Monday, October 30, for a major overhaul that would include slashing its 50-member board and reducing the influence of presidentially appointed overseers. The reforms are intended to ease recurring friction between board members and Red Cross management, and to address complaints that the organization was at times too bureaucratic and unaccountable after Katrina and the attacks. Highlights of the reforms that would need congressional approval include: 1) explicitly delegating responsibility for day-to-day operations to the Red Cross' full-time professional management, with the board focusing mainly on longer-term strategic oversight; 2) reducing the board of governors to between 12 and 20 members by March 31, 2012; 3) creating a single category of board members; 4) shifting seven of the presidentially appointed governors — all but the chairman — into a newly created Cabinet Council that will be merely advisory. To address fraud and other issues of financial accountability, the board is trying to recruit a new chief audit executive with more authority than any predecessors.

Source: <http://www.emsresponder.com/article/article.jsp?siteSection=1&id=4346>

[\[Return to top\]](#)

## **Information Technology and Telecommunications Sector**

### **32. *November 01, Security Focus* — Microsoft Windows NAT helper remote denial-of-service vulnerability.**

Microsoft Windows is prone to a remote denial-of-service vulnerability because the server service fails to properly handle unexpected network traffic. Exploiting this issue may cause affected computers to crash, denying service to legitimate users. Reports

indicate that this vulnerability can be used to disable the Windows firewall. To exploit this issue, an attacker must have the ability to send malformed network traffic from a network interface located in the LAN-side of an affected computer.

Vulnerable: Microsoft Windows XP Tablet PC Edition SP2; Microsoft Windows XP Tablet PC Edition SP1; Microsoft Windows XP Tablet PC Edition; Microsoft Windows XP Professional SP2; Microsoft Windows XP Professional SP1; Microsoft Windows XP Professional; Microsoft Windows XP Media Center Edition SP2; Microsoft Windows XP Media Center Edition SP1; Microsoft Windows XP Media Center Edition Microsoft Windows XP Home SP2; Microsoft Windows XP Home SP1; Microsoft Windows XP Home.

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/20804/references>

**33. *November 01, Network World* — New trick lures worried employees to visit malicious site.**

Last week, a handful of employees at Dekalb Medical Center in Decatur, GA, received e-mails saying they were being laid off. The subject line read "Urgent — employment issue," and the sender listed on the message was at dekalb.org, which is the domain the medical center uses. The e-mail contained a link to a Website that claimed to offer career-counseling information. And so a few employees, concerned about their employment status and no doubt miffed about being laid off via e-mail, clicked on the link to learn more and unwittingly downloaded a keylogger program that was lurking at the site. Called targeted spam or spear phishing, this type of spam that's currently on the rise is particularly vexing because the spammer is able to "spoof" the sending e-mail address to make it look like it's coming from within the organization of the recipient, making it difficult for spam filters to catch. And, unlike traditional spam that is sent in the thousands, spammers are sending just handfuls of these messages at a time, again making it difficult for anti-spam technology to detect.

Source: <http://www.networkworld.com/news/2006/110106-spam-spear-phishing.html>

**34. *November 01, CNET News* — Attack code out for new Apple Wi-Fi flaw.** Kicking off a "month of kernel bugs," a security researcher has released attack code that he claims exploits a new security hole in wireless software from Apple Computer. The vulnerability lies in the Apple AirPort driver, according to details on the flaw published by H.D. Moore, the developer of the Metasploit security tool. It affects only the AirPort driver provided with wireless cards shipped between 1999 and 2003 with PowerBooks and iMacs, the posting said. To launch an attempt, the hacker would have to be on the same wireless network as a vulnerable Mac. The attack entails trying to trigger a memory corruption flaw by sending a malformed data packet to the computer, according to Moore's advisory. But the process isn't easy, and Moore hasn't yet been able to gain complete control over a vulnerable Mac.

Details on the flaw: <http://projects.info-pull.com/mokb/MOKB-01-11-2006.html>

Source: [http://news.com.com/Attack+code+out+for+new+Apple+Wi-Fi+flaw/2100-1002\\_3-6131711.html?tag=cd.top](http://news.com.com/Attack+code+out+for+new+Apple+Wi-Fi+flaw/2100-1002_3-6131711.html?tag=cd.top)

**35. *November 01, CNET News* — Another denial-of-service bug found in Firefox 2.** A second security flaw that could cause the new Firefox 2 browser to crash has been publicly disclosed. The vulnerability lies in the way the open-source browser handles JavaScript code. Viewing a rigged Webpage will cause the browser to exit, a representative for Mozilla, the publisher of the software, said Wednesday, November 1. Contrary to claims on security mailing lists, the bug cannot be exploited to run arbitrary code on a PC running Firefox 2, the representative said.

This flaw in the JavaScript Range object is different from the denial-of-service vulnerability in Firefox 2 that was confirmed by Mozilla last week.

Source: [http://news.com.com/Another+denial-of-service+bug+found+in+Firefox+2/2100-1002\\_3-6131624.html?tag=cd.top](http://news.com.com/Another+denial-of-service+bug+found+in+Firefox+2/2100-1002_3-6131624.html?tag=cd.top)

36. *November 01, CNET News* — **McAfee: Watch out for 'island-hopping' spam.** McAfee's anti-spam researchers have been tracking a trend they've nicknamed "spam island-hopping." Some spammers are using the domain names of small islands for Website links in their junk e-mail campaigns, the security company said. By using top-level domains from small island countries, they attempt to avoid detection, as these domains are typically unknown to spam filters. Using a lesser-known top level domain makes it harder to distinguish spam from legitimate e-mail by examining the links in the messages, according to McAfee. The trend was discovered when McAfee researchers noticed a significant increase in the use of .st, the top-level domain for Sao Tome and Principe, an island off the west coast of Africa, the company said.

Source: [http://news.com.com/McAfee+Watch+out+for+island-hopping+spam/2100-7349\\_3-6131693.html?tag=cd.top](http://news.com.com/McAfee+Watch+out+for+island-hopping+spam/2100-7349_3-6131693.html?tag=cd.top)

37. *November 01, IDG News Service* — **Vista, Office 2007 to launch in U.S. November 30.** After years of waiting, U.S. business customers will finally have a chance to get their hands on Windows Vista and Office 2007 when Microsoft Corp. launches the products on Thursday, November 30, at an event in New York City. In addition to Vista and Office 2007, Microsoft Exchange Server 2007 also will be released to business customers at the event.

Source: [http://www.infoworld.com/article/06/11/01/HNvistaoffice2007nov30\\_1.html](http://www.infoworld.com/article/06/11/01/HNvistaoffice2007nov30_1.html)

### Internet Alert Dashboard

Current Port Attacks	
<b>Top 10 Target Ports</b>	15281 (---), 1026 (win-rpc), 4662 (eDonkey2000), 6881 (bittorrent), 1027 (icq), 4672 (eMule), 1028 (---), 50001 (---), 25 (smtp), 445 (microsoft-ds)
Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center	
To report cyber infrastructure incidents or to request information, please contact US-CERT at <a href="mailto:soc@us-cert.gov">soc@us-cert.gov</a> or visit their Website: <a href="http://www.us-cert.gov">www.us-cert.gov</a> .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <a href="https://www.it-isac.org/">https://www.it-isac.org/</a> .	

[[Return to top](#)]

## Commercial Facilities/Real Estate, Monument & Icons Sector

38. *November 02, Pittsburgh Post-Gazette* — **Police probing thefts of grave markers in southwestern Pennsylvania area.** Bronze flag holders with plaques that designate military service during America's wars and other bronze markers have disappeared during the past few months at cemeteries in rural southwestern Pennsylvania counties. Some of the items have been recovered, but many others have not. State police in Indiana County Tuesday, October 31, recovered 52 of the bronze markers in a wooded area about a mile from where some of the



plaques were stolen. Investigators located the plaques, contained in three buckets, after an interview with one of the suspected thieves, Trooper Tim Lipniskis said. That discovery followed the recovery two weeks ago of 114 of the bronze markers found at a scrap yard in White Township, Trooper Lipniskis said. The scrap yard owner told police he bought the flag holders for \$186. In Fayette County, thieves have struck at least two cemeteries in recent weeks. Also on Tuesday, state police in Uniontown arrested the owner of a Brownsville scrap yard on charges he bought 125 bronze vases stolen in September from a Redstone cemetery. They are valued at \$300 each About \$7,000 worth of bronze markers were stolen in mid-October from a Connellsville Township cemetery.

Source: <http://www.post-gazette.com/pg/06306/734949-85.stm>

[\[Return to top\]](#)

## **General Sector**

39. *November 02, Associated Press* — **Murder charges sought in deaths of California firefighters.** Investigators are seeking arson and murder charges against a man suspected of setting a Southern California wildfire that killed five firefighters. Raymond Oyler, 36, of Beaumont, CA, has been in custody in connection with two earlier fires, and had been described as a "person of interest" in the fire that began a week ago near Palm Springs. Investigators said they would seek to have Oyler tried on five counts of murder, 11 counts of arson, and 10 counts of using an incendiary device. Oyler was in custody in connection with two June fires in the Banning Pass area, a windy corridor that carries Interstate 10 between mountain ranges west of Palm Springs. The Esperanza fire was set on October 26 in Cabazon, a city 90 miles southeast of Los Angeles. Stoked by Santa Ana winds, it destroyed 34 homes and charred 40,200 acres — or about 60 square miles — before being contained Monday, October 30. The blaze was the deadliest for firefighters since 14 were killed in July 1994 near Glenwood Springs, Colorado, according to the National Interagency Fire Center statistics.

Source: <http://www.cnn.com/2006/US/11/02/socal.wildfire.ap/index.htm>

40. *November 02, Associated Press* — **More than 10,700 arrested in 24-state fugitive sting.** Led by the U.S. Marshals Service, nearly 11,000 sex offenders, gang members and other fugitives were swept up in what the Department of Justice on Thursday, November 2, called a sting targeting the "worst of the worst" criminals on the run. The weeklong sting, code-named Operation Falcon III, also led to the shooting death of a Georgia fugitive who was killed by authorities as he came out of his house, officials said. Additionally, the mother of a fugitive in Florida fired — but missed — police approaching her home. Both incidents are under investigation, said John F. Clark, director of the Marshals Service. The roundup, in 24 states east of the Mississippi River, targeted "the worst of the worst fugitive felons in the country," U.S. Attorney General Albert Gonzales said at a Washington news conference. In all, Gonzales said officials caught 10,733 fugitives — including 1,659 sex offenders, 364 gang members and thousands of others sought on kidnapping, robbery, burglary, carjacking and weapons charges. More than 230 weapons were seized.

Source: [http://www.usatoday.com/news/nation/2006-11-02-fugitive-swee p\\_x.htm](http://www.usatoday.com/news/nation/2006-11-02-fugitive-swee p_x.htm)

[\[Return to top\]](#)



## **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](mailto: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](mailto: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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.