



Department of Homeland Security Daily Open Source Infrastructure Report for 31 October 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 Associated Press reports children may be the fastest growing segment of ID theft victims; in one case a thief used a seven-year-old's name, Social Security number, and clean credit history to purchase a \$40,000 houseboat. (See item [8](#))
- A new study names St. Louis, Missouri, as the most dangerous city in the country, leading a trend of violent crimes rising much faster in the Midwest than in the rest of the nation; the study considered crime only within St. Louis city limits, with a population of about 330,000. (See item [29](#))

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. *October 28, Associated Press* — **Bolivia to sign nationalization deals with foreign oil companies.** President Evo Morales' government completed an ambitious oil and gas nationalization plan Saturday, October 28, by signing contracts allowing international companies to continue operating in Bolivia under state controls. The government signed deals with Brazilian state energy giant Petroleo Brasileiro SA and several foreign energy companies, including French company Total SA and U.S.-based Vintage Petroleum. Morales nationalized Bolivia's oil and gas industry on May 1, giving foreign companies 180 days to sign new deals

ceding majority control of their Bolivian operations or leave the country. The deals guarantee investment for the natural gas industry in Bolivia, that contains South America's second largest reserves after Venezuela but in dire need of foreign investment to boost exploration and production capacity.

Source: <http://www.chron.com/disp/story.mpl/business/4295278.html>

2. *October 28, Associated Press* — **Many emergency gas shutoff valves inaccessible.** Most of the emergency valves used to shut off the flow of explosive gas to Massachusetts homes and businesses are inaccessible, according to the Boston Globe. Nearly 70 percent of the 1.1 million valves in Massachusetts are inaccessible, the newspaper reported, citing industry records filed with state regulators. Many valves may have been paved over or blocked by debris. The natural gas pipeline system has several types of valves, including those that control gas flowing to large sections of communities and others that control service to parts of neighborhoods, such as a street or a group of streets. The service valves, which control gas flowing to individual buildings, are the ones most often buried or blocked. Gas companies are required by federal and state regulations to ensure that all shut-off valves are accessible. DTE executive director Timothy Shevlin Jr. said the agency is investigating compliance issues with the service valves controlling flow to individual buildings. Gas companies say that the system is safe because they can turn off gas to entire areas with critical or main valve shutoffs.

Source: <http://www.thebostonchannel.com/news/10181954/detail.html?rs=s=bos&psp=news>

3. *October 27, Medill News Service* — **Utility first in U.S. to burn paint solids to produce electricity.** Ameren Corp.'s Meramec facility in South Saint Louis County, MO, will be the first power plant in the U.S. to burn paint solids to produce electricity, the company said. Through a partnership with DaimlerChrysler AG, Ameren, a major electricity provider in Illinois and Missouri, plans to reuse 1,000 tons of leftover paint solids from car production to offset coal purchases at the plant. In its first trial year, paint solids are expected to replace roughly 570 tons of coal and produce enough energy to power 70 homes annually, according to Ameren. Though that is a small portion of the four million tons of coal burned by the facility annually, paint solids may represent one of a number of possible alternative substances used for power generation. Many of these alternative substances actually burn more efficiently than coal, Fox said. When the paint solids are completely dry, they can produce more British Thermal Units, or BTUs, than coal alone.

Source: <http://www.nwintimes.com/articles/2006/10/28/business/business/dc91dab78ce23b99862572130001f92e.txt>

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

Chemical Industry and Hazardous Materials Sector

4. *October 29, Oakland Press (MI)* — **Acid spill at Michigan plant prompts evacuation.** Families living along two short streets were evacuated from their homes Saturday, October 28, after an acid spill inside a Hazel Park, MI, plant. The spill of about 300 gallons of nitric acid happened inside the K.C. Jones plating company. Officers initially warned near-by residents, those living within a half-mile, to stay indoors, but air-testing confirmed the spill was contained within the building and the air was clean. However, residents on one block each of West Mahan and West Brickley, which both dead end to the west due to Interstate 75, were

evacuated as a precaution.

Source: http://www.theoaklandpress.com/stories/102906/loc_2006102929.shtml

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

Defense Industrial Base Sector

5. *October 28, Aviation Week* — **Small aircraft may become large sensors.** An emerging arena for new competition in the defense industry will involve the melding of airframes and what they traditionally have carried internally. The debate about whether platforms or payloads are more important will soon shift fundamentally as systems — particularly sensors, communications and weaponry as they merge into one — move to the outside of platforms and become their skins. Moreover, there are moves afoot to integrate the two more closely, even on more traditional designs. Conformal arrays are being eyed for manned and unmanned aircraft, ships and ground vehicles. But they seem to have a special niche in unmanned aircraft. There the operational and low-cost advantages of small, stealthy, missile-size unmanned combat aircraft can be fused with the benefits of a sensor that uses the whole exterior of the platform as an aperture to communicate, image, jam or function as a weapon that fires high-power spikes of energy into enemy electronics.

Source: http://www.aviationnow.com/avnow/news/channel_defense_story.jsp?id=news/aw103006p1.xml

6. *October 27, Reuters* — **U.S. hails airborne laser as weapons milestone.** The head of the Pentagon's Missile Defense Agency on Friday, October 27, hailed what he described as epochal progress toward putting a high-energy laser aboard a modified Boeing Co. 747 to zap ballistic missiles that could be fired by North Korea and Iran. But the Pentagon's former top weapons tester cast doubt on project, calling it far from militarily effective and perhaps easily defeated by a simple countermeasure. The so-called Airborne Laser has been developed at a cost so far of about \$3.5 billion with the aim of destroying, at the speed of light, all classes of ballistic missiles shortly after their launch. If successful in flight testing and deployed, it would become part of an emerging U.S. anti-missile shield that also includes land- and sea-based interceptor missiles. Philip Coyle, the Pentagon's chief weapons tester under former President Bill Clinton, told Reuters that its real effectiveness appeared doubtful. "If a laser can be developed with enough power to penetrate the atmosphere and still be lethal once it reaches a target, an enemy would only need to put a reflective coating on the outside of its missiles to bounce off the laser beam, making it harmless," he said.

Source: http://today.reuters.com/news/articlenews.aspx?type=topNews&storyid=2006-10-27T211842Z_01_N27431705_RTRUKOC_0_US-ARMS-US-A-LASER.xml&src=rss&rpc=22

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

Banking and Finance Sector

7. *October 30, TechWeb* — **Phishing domain resale market booms.** Internet addresses that appeal to identity thieves eager to rip off consumers are being posted by major domain

resellers, F-Secure said Friday, October 27. F-Secure has identified more than 30 registered domain names for resale on Sedo that would be of interest only to the legitimate holder of the trademark or to phishers, criminals who try to dupe consumers into divulging personal information by enticing them to fake Websites. Among the domains: citi-bank.com, bankofamerica.com, americanexpresscard.com, mastercard.com, and visacredit.com. "Why would anybody want to buy these domains unless they are the bank themselves -- or a phishing scammer?" wrote Mikko Hypponen, F-Secure's chief research officer. In its search of Sedo, F-Secure also found domain names for resale that use the accent characters " and " in place of the normal "a" or "i" to create "highly deceptive" URLs like vsa.com, p'ypal.com, and payp'l.com. Sedo said that while it has a process in place to pull domain sales that violated trademarks, it was the trademark holder's responsibility to file a request. Last March F-Secure identified nearly 500 domain names on variations of "citibank" and over 400 on versions of "bankofamerica."

Source: <http://www.itnews.com.au/newsstory.aspx?CIaNID=41386&src=sit e-marq>

8. *October 30, Associated Press* — **Childrens' identities being stolen.** Identity theft is a growing problem and kids aren't immune. New York Senator Hillary Rodham Clinton (D) says as many as 400,000 children may be victims of identity theft. She says the number of complaints has grown by 78 percent, making it the fastest growing segment of ID theft victims. Clinton says she's heard of one story in which a thief used a seven-year-old's name, Social Security number, and clean credit history to purchase a 40-thousand-dollar houseboat.

Source: <http://www.wstm.com/global/story.asp?s=5605501&ClientType=Pr intable>

9. *October 29, Daily Mail (UK)* — **ID thieves infiltrate call centers.** As more businesses move away from direct customer contact, call centers have become the latest front in the war on identity theft as criminals search for new ways of accessing secret customer information and stealing from accounts. Up to a tenth of call centers in one UK city alone have already been targeted. There are some 5,700 call centers in the UK, meaning nearly 600 could potentially have been infiltrated. Call centers are not used just by banks, but by other groups such as insurers, shops, and catalogue companies. Criminals have tapped into call centers after recognizing how easy it is to operate in such a large industry with a high staff turnover. The scammers recruit volunteers to work in the centers who supply them financial information in return for a fee. Employees leaving the call centers are also being approached and coerced into providing data. Disgruntled employees may also turn their hand to fraud. They target large accounts, with sums of money stolen ranging from a few thousand to hundreds of thousands.

Source: http://www.thisismoney.co.uk/credit-and-loans/idfraud/article.e.html?in_article_id=414157&in_page_id=159

10. *October 28, Agence France-Press* — **Banks dispose of customer account information in trash receptacles.** Some banks have been using garbage bags to dispose of customer information in "wholly unacceptable" breaches of data protection rules, Britain's information commissioner has said. Richard Thomas said that his office was investigating branches of HSBC, Halifax, NatWest, and Royal Bank of Scotland as well as a post office. "A number of banks have been very careless with people's personal information," he told the Times newspaper, adding he had seen rubbish bags full of bank statements and details of a \$948,000 bank transfer. "...if the banks themselves are being careless with the information, that seems to me to be wholly unacceptable." The banks could face unlimited fines if the information

commissioner's office was to take them to court but the spokesperson said Thomas wanted banks to "sort this out" themselves. Ian Mullen of the British Bankers' Association told BBC radio that instances of documents being found in dustbin bags were isolated and it was not clear whether banks were at fault.

Source: http://news.yahoo.com/s/afp/20061028/wl_uk_afp/britainmoneybanking_061028121036

11. *October 27, IDG News Service* — **Phishing attack targets MySpace users.** Netcraft reports that a MySpace user was e-mailing potential victims inviting them to visit a fraudulent log-in page, where they were asked to enter their e-mail address and password. The attack, which was shut down by MySpace around 10 a.m. PDT Friday, October 27, took advantage of the way MySpace organizes URLs in order to give the fake log-in page a believable Web address, something that could confuse even security-conscious users, according to Netcraft analyst Rich Miller. The attack is not unprecedented, but it shows "one more interesting way that phishers are trying to trick people out of their account details," Miller said. Typically, sites like MySpace have a database of user names that are off-limits, in order to prevent this type of attack, Miller said. "What this kind of attack suggests is that sites have to expand that list."

Source: <http://www.pcworld.com/article/id.127688-pg.1-RSS.RSS/article.html>

12. *October 27, National Nine News MSN (Australia)* — **Money laundering ring apprehended.**

Police believe they have apprehended the biggest money laundering racket in Australian history, arresting 57 people in the past three weeks for laundering more than \$93 million. Four arrests were made Thursday, October 26. A Melbourne woman has been charged with laundering \$1.4 million while a Sydney man has been charged with laundering over \$1.5 million. The operation targeting money launderers, known as Taskforce Gordian, came about following an investigation into drug trafficking. The Australian Crime Commission alleges that drug syndicates have been rapidly shipping their profits offshore through the use of money laundering groups. The money has been heading to Vietnam, Cambodia, and Hong Kong — a known base for triad gangs.

Source: <http://news.ninemsn.com.au/article.aspx?id=156229>

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

Transportation and Border Security Sector

13. *October 30, Associated Press* — **Nigerian crash pilot ignored storm advice.** The pilot of a Nigerian airliner that crashed on Sunday, October 29, did not heed air traffic controllers' advice to wait for stormy weather to clear before taking off, the minister of aviation said Monday, October 30. The pilot was among 96 people killed in the crash; nine people survived. While Aviation Minister Babalola Borishade did not directly blame pilot error in the third mass-casualty jet crash to hit this West African nation in less than a year, he said officials would move to try to curb pilots' power to ignore advice from the control tower. Late Sunday, investigators found one of two black boxes from the Boeing 737 owned by a private Nigerian airline, Aviation Development Co. (ADC). Borishade said all of ADC's planes were grounded indefinitely and its flying license was suspended. "The pilot of the unfortunate accident refused to take advantage of the weather advice and the opinion of the (control) tower to exercise patience and allow the weather to clear for a safe take off," Borishade said at a news

conference. Nigeria's air industry is notoriously unsafe. Last year, two planes flying domestic routes crashed within seven weeks of each other, killing 224 people.

Source: <http://www.cnn.com/2006/WORLD/africa/10/30/nigeria.crash.ap/index.html>

14. *October 30, Associated Press* — **Mesaba, flight attendants reach agreement.** Mesaba Aviation Inc. and the union that represents its flight attendants reached a tentative agreement on labor concessions on Sunday, October 29, one day after doing the same with its pilots, said the airline, which is in bankruptcy protection. On Saturday, the airline and its pilots agreed on concessions, five days after a bankruptcy judge blocked a potential strike by pilots, flight attendants and mechanics at the regional carrier, based in suburban Eagan, MN. Flight attendants have the right to accept or reject it. If a deal had not been reached, Mesaba had the authority from the judge to impose labor cost cuts of 17.5 percent. This leaves only the mechanics who have yet to work out a deal.

Source: http://biz.yahoo.com/ap/061029/mesaba_flight_attendants.html?.v=3

15. *October 30, Department of Homeland Security* — **Fact Sheet: ICE Accomplishments in Fiscal Year 2006.** Under the leadership of Assistant Secretary Julie Myers, U.S. Immigration and Customs Enforcement (ICE) achieved historic results in FY 2006. ICE set new records for enforcement activity, ended the long-standing practice of “catch-and-release” along the nation’s borders, launched major new initiatives, transformed its detention and removal process, and improved its intelligence functions. Two of these milestones: (1) Set New Records for Worksite Enforcement: Total arrests made in ICE worksite enforcement cases during FY 2006 reached a level that was more than seven times greater than in 2002, the last full year of operations for U.S. Immigration and Naturalization Service; and (2) Created a National Center to Coordinate Deportation of Aliens Upon Release from Prison: ICE created a national center that reviews aliens at all 119 federal detention facilities (as opposed to only 30 federal facilities in 2005), to ensure that criminal aliens are deported rather than released into society upon the completion of their sentences. U.S. Immigration and Customs Enforcement (ICE) was established in March 2003 as the largest investigative arm of the Department of Homeland Security. ICE is comprised of four integrated divisions that form a 21st century law enforcement agency with broad responsibilities for a number of key homeland security priorities.

Source: http://www.dhs.gov/xnews/releases/pr_1162228690102.shtm

16. *October 30, Department of Homeland Security* — **Fact Sheet: Securing America’s Borders.** During fiscal year 2006, U.S. Customs and Border Protection (CBP) made significant progress toward securing the nation’s border at and between the ports of entry. Through operations, increases in staffing, additional infrastructure and better technology, and the support of the President and Congress, CBP’s frontline personnel were better equipped in fiscal year 2006 than any period in the nation’s history. Among other achievements, CBP Border Patrol agents improved border security, reducing the number of apprehensions at the borders by 8.4 percent compared with fiscal year 2005. Tucson Sector saw a reduction in apprehensions by 11 percent (392,074 apprehensions) and El Paso Sector saw a nine percent reduction (122,256 apprehensions) in fiscal year 2006 compared with 2005. San Diego Sector saw an increase of three percent (142,104 apprehensions). Also, significant progress has been made with denying illegal entry to aliens from countries other-than-Mexico (OTMs). In fiscal year 2005, OTMs made up approximately 20 percent of border apprehensions. In fiscal year 2006, working

closely with Immigration and Customs Enforcement, CBP Border Patrol agents reduced the percentage of OTM apprehensions at the Southwest border to 98,153 or nine percent of total border apprehensions.

Source: http://www.dhs.gov/xnews/releases/pr_1162226345208.shtm

17. *October 30, Department of Transportation* — **FMCSA fines Fung Wah for violating federal safety regulations.** The Department of Transportation's Federal Motor Carriers Safety Administration (FMCSA) announced on Monday, October 30, that it has fined Fung Wah Bus Transportation Inc. \$31,110 for violating federal safety regulations. In September, a bus operated by Fung Wah overturned on a freeway ramp outside Boston, MA. Forty-eight people were injured, some seriously. Following the crash, as is standard procedure when a motorcoach incident of this nature occurs, FMCSA investigated Fung Wah and found the company to be in violation of multiple federal regulations and has initiated enforcement action for two specific violations: 1) using drivers unable to speak the English language and 2) drivers exceeding the posted speed limit. The agency noted that this is not the first time it has reviewed Fung Wah's operations. Federal authorities visited the company eight times over the past three years, including a May 2006 review that resulted in a \$12,950 fine for safety and traffic violations. Source: <http://www.dot.gov/affairs/fmcsa0706.htm>

18. *October 29, USA TODAY* — **Boston explores Wi-Fi options.** The Federal Communications Commission (FCC) will soon issue a ruling that could broaden airlines' wireless Internet (Wi-Fi) service at Boston Logan airport. In 2005, the Massachusetts Port Authority (Massport), which runs Logan, banned airlines from offering wireless Internet service at their clubs in the airport. Soon after the Massport decision, Continental Airlines, which provided free Wi-Fi at its clubs, petitioned the FCC to overturn the ban. In banning the service, Massport cited security concerns. It said private Wi-Fi networks could interfere with the wireless transmissions used by the airport for operations, and by federal officials for security. Massport's decision came one year after Logan launched its own \$8-a-day wireless Internet service, prompting its critics to complain that the airport was creating a monopoly. Source: http://www.usatoday.com/travel/flights/2006-10-29-check-in-boston-wi-fi-usat_x.htm

19. *October 27, Department of Transportation* — **Working conditions for train crews to improve with federal regulations to help prevent hearing loss.** Train crews will be less likely to suffer problems with hearing loss as the result of revised federal standards aimed to enhance the safety and well being of railroad employees by limiting locomotive cab noise, announced Federal Railroad Administrator (FRA) Joseph H. Boardman. He explained that the final rule will directly affect approximately 80,000 rail employees and amends existing federal noise standards to require that railroads perform routine noise monitoring and provide training to employees in hearing loss prevention. In addition, train crews are required to use hearing protection. The final rule also requires the integration of noise reduction features into the design, manufacturing and maintenance of locomotives, Boardman said. This includes standards for better insulation, relocation of air brake exhaust piping, and a reduction in vibration from cab equipment. Some of these features are already being incorporated into newer locomotives. The FRA strongly believes these changes will reduce the incidence of noise-induced hearing loss, which may improve train crew communication as well as reduce the risk of accidents caused by occupational stress and fatigue, said Boardman. In developing

the final rule, FRA incorporated comments from many interested parties, including locomotive engineers, audiologists, and rail labor organizations.

Source: <http://www.dot.gov/affairs/fra1706.htm>

20. *September 29, Government Accountability Office* — **GAO-06-973: Aviation Finance: Observations on Potential FAA Funding Options (Report).** The Federal Aviation Administration (FAA), the Airport and Airway Trust Fund (Trust Fund), and the excise taxes that support the Trust Fund are scheduled for reauthorization at the end of fiscal year 2007. FAA is primarily supported by the Trust Fund, which receives revenues from a series of excise taxes paid by users of the national airspace system (NAS). The Trust Fund's uncommitted balance decreased by more than 70 percent from the end of fiscal year 2001 through the end of fiscal year 2005. The remaining funding is derived from the General Fund. This report focuses on the portion of revenues generated from users of the NAS and addresses the following key questions: (1) What advantages and concerns have been raised about the current approach to collecting revenues from NAS users to fund FAA, and to what extent does available evidence support the concerns? (2) What are the implications of adopting alternative funding options to collect the revenues contributed by users that fund FAA's budget? (3) What are the advantages and disadvantages of authorizing FAA to use debt financing for capital projects? The Government Accountability Office (GAO) obtained documents from relevant agencies, key stakeholders, and academic and financial experts.
Highlights: <http://www.gao.gov/highlights/d06973high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-973>

[[Return to top](#)]

Postal and Shipping Sector

21. *October 30, DM News* — **DHL offers shipment transparency with new online tool.** Express delivery and logistics company DHL is giving customers full control over their country-to-country shipments through a Web-based tool called DHL Import Express Online, which will enable customers to securely prepare and manage shipments from their personal computers. The tool can support shipping transactions from 46 countries to anywhere in the DHL network. Subsequent rollout is planned to more trade routes throughout DHL's network to provide customers with full visibility and control during the shipment process.
Source: <http://www.dmnews.com/cms/dm-news/direct-mail/38792.html>

[[Return to top](#)]

Agriculture Sector

22. *October 30, Associated Press* — **Nebraska leading in identification program.** Nebraska leads the nation in voluntary registration of livestock operations. State agriculture officials say more than 13,000 of an estimated 31,000 known locations have been assigned a number. Premise ID began in Nebraska in September 2004 as the first step toward a national animal identification system. The national directive calls for voluntary participation. Indiana and Wisconsin have exercised their option to make premise identification mandatory. Missouri has had difficulty

getting producers to participate. Steve Goff, head of Missouri's Animal Identification Program, said his state has assigned only about 10,000 of a possible 104,000 numbers.

Source: <http://www.nebraska.tv/news/local/4514866.html>

23. *October 24, Horse Magazine* — Guidelines for equine infectious disease outbreaks issued.

The Infectious Disease Task Force of the American Association of Equine Practitioners (AAEP) has developed guidelines for the control of contagious infectious disease within the horse population. Recommendations are provided for the control of suspected cases of infectious respiratory, neurologic, diarrheal, and vesicular disease. The symptom-based guidelines provide a detailed action plan for veterinarians as they address a possible infectious disease outbreak. From the point at which a case of infectious disease is suspected, the guidelines offer measures to control the spread of infection, diagnostic testing options and communication considerations. The guidelines are available to veterinarians.

Source: <http://www.thehorse.com/viewarticle.aspx?ID=7958>

[[Return to top](#)]

Food Sector

24. *October 30, Agricultural Research Service* — Irradiation for healthier food. Low levels of irradiation can help ensure that U.S. beef producers are providing the safest, highest-quality ground beef products possible. That's the conclusion of Agricultural Research Service (ARS) scientists at the Roman L. Hruska U.S. Meat Animal Research Center (USMARC) in Clay Center, NE. Ground beef can pose a serious threat to human health if contaminated by a disease-causing microbe, or pathogen, during grinding. USMARC Director Mohammad Koohmaraie and his colleagues examined the effectiveness of using low levels of radiation on beef carcasses before cutting, to reduce pathogens in ground beef. The researchers discovered that the low-penetration E-beam reached approximately 15 millimeters (about 1/2 inch) below the surface of the carcass. Because pathogens are most prevalent on the surface, this technology can significantly lower their numbers. Research also showed that E-beam irradiation effectively reduced pathogens on the carcass surface with little to no influence on the flavor of beef that was used to make stir fry and ground beef products.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

[[Return to top](#)]

Water Sector

25. *October 30, Reuters* — Spain looks to penalize heavy water use. Spaniards who use "excessive" amounts of water may have to pay more for it in future, the government said on Monday, October 30, seeking ways to curb water use after two years of drought. After the worst drought on record in 2005 and below average rainfall again in the year ended on September 30, the country's reservoir levels dropped to their lowest in a decade. Environment Minister Cristina Narbona said she was planning to guarantee a minimum amount of clean water for everyone and would raise prices above that limit. Narbona did not say how the reform would affect farmers, who use 77 percent of Spain's water. Urban consumption accounts for 18

percent and industry the remaining five percent.

Source: http://today.reuters.co.uk/news/articlenews.aspx?type=scienceNews&storyID=2006-10-30T153316Z_01_L27395543_RTRIDST_0_SCIE_NCE-ENVIRONMENT-SPAIN-WATER-DC.XML

[[Return to top](#)]

Public Health Sector

26. *October 30, Reuters* — **Seventh Egyptian dies of bird flu.** An Egyptian woman died of bird flu on Monday, October 30, bringing the total number of human deaths in Egypt to seven, the state news agency MENA said. The victim was a woman from the Nile Delta town of Samanoud who had slaughtered and handled domestic poultry, it said. It was the first human death in Egypt from the virus since May. With 15 infections, Egypt has had the largest cluster of human bird flu cases outside Asia, and the latest case came a month after authorities found a cluster of new cases in birds following a two-month lull in detected poultry cases.

Source: http://today.reuters.com/News/CrisesArticle.aspx?storyId=L30_68642

27. *October 30, Agence France-Presse* — **World Health Organization launches global anti-corruption drive on medicines.** The World Health Organization (WHO) launched an anti-corruption drive to tackle bribery in medical procurement, which is thought to affect up to a quarter of the drugs governments buy. The total global market for pharmaceuticals is worth up to \$50 billion a year. Recent estimates showed that as much as 25 percent of medicines procured by governments can be lost to fraud, bribery and other corrupt practices, the WHO said. The initiative to help governments was launched at a first meeting of a new WHO group of international anti-corruption and pharmaceutical experts on Monday, October 30.

Source: http://news.yahoo.com/s/afp/20061030/hl_afp/whohealthcorruption_061030173050

28. *October 28, CTV (Canada)* — **C. difficile outbreak kills nine at Quebec hospital.** Doctors are investigating whether a more virulent strain of the C. difficile bacterium is to blame for an outbreak at a Quebec, Canada, hospital that killed nine people. Health officials have identified a total of 22 cases at Honore-Mercier Hospital in St-Hyacinthe since late July. Most of the nine patients who died were elderly and suffered from other ailments. Another 13 patients who have fallen ill are now isolated in single-patient rooms at the hospital.

C. Difficile information: http://www.cdc.gov/ncidod/dhqp/id_Cdiff.html

Source: http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20061027/difficile_hospital_061027/20061027?hub=TopStories

[[Return to top](#)]

Government Sector

29. *October 30, Associated Press* — **St. Louis named most dangerous U.S. city.** A surge in violence has made St. Louis, MO, the most dangerous city in the country, leading a trend of violent crimes rising much faster in the Midwest than in the rest of nation, according to an annual list. The city has long fared poorly in the rankings of the safest and most dangerous

American cities compiled by Morgan Quitno Press. Violent crime surged nearly 20 percent in St. Louis from 2004 to last year, when the rate of such crimes rose most dramatically in the Midwest, according to FBI figures released in June. The ranking, released Monday, October 30, came as the city was still celebrating Friday's World Series victory at the new Busch Stadium. St. Louis has been spending millions of dollars on urban renewal even as the crime rate climbs. The study looks at crime only within St. Louis city limits, with a population of about 330,000, Morgan said. Visiting St. Louis on Thursday, FBI director Robert Mueller said the FBI is working harder to form partnerships with police departments to launch programs like St. Louis' Safe Streets task force, which focuses police efforts on problematic neighborhoods. The second most dangerous city was Detroit, followed by Flint, MI, and Compton, CA.

Morgan Quitno Report Website: <http://www.morganquitno.com/>

Source: <http://www.cnn.com/2006/US/10/30/city.crime.ap/index.html>

30. *October 30, Associated Press* — **Bus vandals shut down school system.** In Waterbury, CT, vandals damaged a third of the buses used to bring about 18,000 students to public schools, leading officials to give children an unexpected day off from school Monday, October 30. The city's schools were closed because vandals sprayed fire extinguishers, spray-painted graffiti, smashed first aid kits, damaged fuse boxes, and broke antennas on 40 buses. A worker for the bus company discovered the damage Sunday night, police Lt. Chris Corbett said. Safety equipment must be replaced before the buses can be used again, he said. No arrests had been made but authorities thought juveniles may be involved because the damage came shortly before Halloween.

Source: http://hosted.ap.org/dynamic/stories/S/SCHOOL_BUSES_VANDALIZED?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

31. *October 28, Morning Call Online (PA)* — **Explosion at Pennsylvania school mars day of pride.** In Allentown, PA, a Liberty High School student set off a "soda bottle bomb" in the school's foyer on Thursday, October 26, sending an adult hall monitor to the hospital and dismaying district officials who had been celebrating another school's acceptance into a national NASA program. The student's exploding bottle of soda and hydrochloric acid injured the hall monitor as classes dismissed at 2:30 p.m. EDT. The incident came at the same time Bethlehem Area administrators, teachers and students were gathered at Broughal Middle School to mark the beginning of the NASA program. According to a Bethlehem police report, Vice Principal Joanne Durante said a soda bottle bomb was set off in the foyer on the south side of the school building. Ronnel Ford, 54, a hall monitor, told police she breathed in some of the mist and vapors and her eyes and nose were irritated. Police have not charged anyone with constructing or setting off the bomb, which exploded from a 16-ounce plastic soda bottle containing aluminum foil and hydrochloric acid. But police say they are close.

Source: http://www.mcall.com/news/local/all-b1_4sodabomboct28.0.7554009.story?coll=all-newslocal-hed

[[Return to top](#)]

Emergency Services Sector

32. *October 30, Silver City Sun-News (NM)* — **New Mexico State University to start dirty-bomb training.** New Mexico State University's Institute for Energy and the

Environment has implemented a first-responder training program targeted toward "dirty bomb" attacks. Dirty bombs, a class of weapons also known as radiological dispersal devices, are viewed as one of the gravest anticipated terrorist threats facing the United States and other nations. In training first-responders such as firefighters and emergency medical personnel, Jim Conca, Director of the Carlsbad Environmental Monitoring and Research Center, stresses the criticality of risk, perception and education. He also trains emergency personnel to assume that all bombs are dirty and to follow the first priority at the scene — defining the hot zone. "This is the most important first response, and a simple alarming dosimeter is the most useful piece of equipment for a dirty bomb attack," Conca said. A dosimeter is a device used to measure an individual's exposure to radiation.

Source: http://www.scsun-news.com/news/ci_4572927

33. *October 29, Star-Bulletin (HI)* — **Most Hawaiians do not know how to respond in the event of a tsunami.** If the tsunami warning sirens had sounded on October 15, about 100 might not have gone off, because they are dependent on the electrical power grid, state officials in Hawaii acknowledged. In addition, about 148 more emergency sirens are needed on the four main Hawaiian Islands to cover "gap areas." However, scientists say a bigger issue, overshadowing criticism over communications issues on October 15, is that most people apparently do not know what to do if the sirens sound to signal a real tsunami. Dan Walker, a tsunami adviser to the Oahu Civil Defense Agency, noted how people desperately called radio stations long after the magnitude-6.7 quake had struck to ask why the sirens didn't go off. "If they are calling four hours later and asking if there's any chance of a tsunami, that shows that they haven't been properly educated," said Walker. Walker, the civil defense adviser, is chairing a Science Advisory Working Group going over all communication glitches experienced during the earthquake, as well as the public's response to it. By January, the group will make a number of recommendations to the state about how it could improve alert systems and boost public education.

Source: <http://starbulletin.com/2006/10/29/news/story03.html>

34. *October 28, KETV 7 (NE)* — **Three Nebraska counties put to the test.** Federal, state, and local agencies responded to three different scenarios on Saturday, October 28, in Nebraska to test what would happen during a real disaster, and late in the day officials were calling the test a success. The preparedness drill tested Douglas, Washington, and Sarpy Counties. In Rosenblatt stadium, the simulation was an explosion during the national anthem of a Yankees-Royals baseball game. At the Sarpy County Fairgrounds, agents responded to radioactive material hidden by terrorists. The University of Nebraska Medical Center Biocontainment unit, was another location. Officials there had to handle a small pox outbreak. The drill was also an opportunity to test equipment, like the Sarpy county mobile command center or communication tools at the United Way. "Our goal is to make sure the team effort works, to make sure each person knows what their roles and responsibilities are," said spokesperson Jamie Moore.

Source: <http://www.ketv.com/news/10181109/detail.html>

35. *October 27, Government Computer News* — **Chertoff lays out plan for fusion centers.** As the United States faces threats from weapons of mass destruction, as well as high-consequence international and homegrown plots, the Department of Homeland Security (DHS) is working with state, local, federal and international law enforcement to defend the country from terrorism. DHS Secretary Michael Chertoff said stopping domestic terrorism threats is best

done through shared intelligence, starting at the local level. To ensure that this coordination and collaboration happens, DHS will establish fusion centers, stocked with experts, and will work to grant clearance of classified information more quickly. Both initiatives are part of the department's effort to take its relationships with major city police chiefs and information sharing to the next level. The fusion centers will be made up of intelligence personnel from the federal intelligence community, subject matter experts and intelligence analysts and operators of local police departments. The goal is to "become more deeply embedded in one another's day-to-day intelligence analysis and operational activity," Chertoff said. DHS plans to have 20 fusion centers by the end of the fiscal year and up to 35 fusion centers by the end of the next fiscal year.

Source: http://www.gcn.com/online/vol1_no1/42432-1.html

- 36. *October 27, Federal Emergency Management Agency* — President declares major disaster for Alaska.** The head of the Department of Homeland Security's Federal Emergency Management Agency announced Friday, October 27, that federal disaster aid has been made available for Alaska to supplement state and local recovery efforts in the area struck by a fire during the period of August 3–4.

For further detail: <http://www.fema.gov/news/event.fema?id=7265>

Source: <http://www.fema.gov/news/newsrelease.fema?id=31118>

[[Return to top](#)]

Information Technology and Telecommunications Sector

- 37. *October 30, InfoWorld* — InfoWorld 2006 Security Survey: IT's confidence crisis.** This year's InfoWorld Security Survey shows an alarming and growing lack of confidence among IT security professionals — for the fourth year in a row. According to the survey, which polled 430 individuals responsible for their organization's security, 56 percent are at most "somewhat confident" in their enterprise's security system. And the rising tide of malware and phishing exploits is behind a great deal of that anxiety. If 2005 marked the year that playful teenage hacker hobbyists gave way to more criminally minded professionals, 2006 is showing just how lethal this better-funded and -disciplined breed of thugs can be.

Full text report: http://www.infoworld.com/pdf/special_report/2006/44SRsecurity.pdf

Source: http://www.infoworld.com/article/06/10/30/44FEsecsurvey_1.html

- 38. *October 30, IDG News Service* — Security researchers find another pop-up vulnerability in IE.** A security problem originally found in Microsoft Corp.'s Internet Explorer (IE) 6 browser has returned to haunt IE7, the new version of the browser launched two weeks ago, a security consultant said Monday, October 30. Danish security consultancy Secunia AsP posted an advisory regarding an issue where an attacker could potentially snare logins and passwords from an unsuspecting IE7 user. Over two years ago, security researchers reported the same fault in IE6. If a user visits a Website specially crafted by an attacker, and then opens a "trusted" site such as a bank or e-commerce site that has a pop-up window, the attacker can put new content into the pop-up, said Thomas Kristensen, Secunia's chief technology officer. This could enable the attacker to ask a user for financial information or passwords, he said. When the problem was revealed in June 2004, Microsoft gave instructions for a workaround for IE6: disable the setting "Navigate sub-frames across different domains." That setting is disabled by default in

IE7, but does not appear to prevent the attack, Kristensen said.

Source: http://www.infoworld.com/article/06/10/30/HNieflaws_1.html

39. *October 29, New York Times* — **U.S. investigates voting machines' Venezuela ties.** The federal government is investigating the takeover last year of a leading American manufacturer of electronic voting systems by a small software company that has been linked to the leftist Venezuelan government of President Hugo Chávez. A touch-screen machine by Sequoia Voting Systems was used this month during early balloting in Chicago. The inquiry is focusing on the Venezuelan owners of the software company, the Smartmatic Corporation, and is trying to determine whether the government in Caracas has any control or influence over the firm's operations. The inquiry on the eve of the midterm elections is being conducted by the Committee on Foreign Investment in the United States, or CFIUS, the same panel of 12 government agencies that reviewed the abortive attempt by a company in Dubai to take over operations at six American ports earlier this year. The concern over Smartmatic's purchase of Sequoia comes amid rising unease about the security of touch-screen voting machines and other electronic elections systems.

Source: <http://www.nytimes.com/2006/10/29/washington/29ballot.html?ei=5065&en=e0c8ab46eb7f870b&ex=1162789200&adxnnl=1&partner=MYWAY&adxnnlx=1162123697-fGdgFeTtCKTTCxcnenqAsQ>

40. *October 26, Secunia* — **Cisco Security Agent for Linux port scan denial-of-service.** A vulnerability has been reported in Cisco Security Agent for Linux, which can be exploited by malicious people to cause a denial-of-service. The vulnerability is caused due to an error within the detection of port scans. This can be exploited to stop the Cisco Security Agent (CSA) from responding due to excessive resource consumption by starting a port scan with certain options. The vulnerability is reported in CSA 4.5 for Linux prior to Hotfix 4.5.1.657, CSA 5.0 for Linux prior to Hotfix 5.0.0.193, and in the standalone CSA shipped with Cisco Unified CallManager (CUCM) 5.0 versions including 5.0(4), and Cisco Unified Presence Server (CUPS) 1.0 versions including 1.0(2).

Affected Software: CSA 4.x; CSA 5.x; Cisco Unified CallManager 5.x; Cisco Unified Presence Server 1.x.

Solution: Apply Hotfixes: <http://www.cisco.com/cgi-bin/tablebuild.pl/cups-10?psrtdcat 20e2>
CSA version 4.5 for Linux: Apply Hotfix 4.5.1.657. CSA version 5.0 for Linux: Apply Hotfix 5.0.0.193. CUCM 5.0 version including 5.0(4): Apply COS COP upgrade. CUPS 1.0 version including 1.0(2): Apply COS COP upgrade.

Source: <http://secunia.com/advisories/22574/>

41. *October 26, Secunia* — **AOL YGPPDownload ActiveX control buffer overflows.** Two vulnerabilities have been reported in AOL, which can be exploited by malicious people to compromise a user's system. 1) A boundary error in the YGPPDownload ActiveX control (YGPPicDownload.dll) when processing input passed to the "AddPictureNoAlbum()" method can be exploited to cause a heap-based buffer overflow. 2) A boundary error in the YGPPDownload ActiveX control (YGPPicDownload.dll) when processing input passed to the "downloadFileDirectory" property can be exploited to cause a heap-based buffer overflow. Successful exploitation of the vulnerabilities allows execution of arbitrary code.

Affected Software: AOL 8.x and AOL 9.x.

Solution: Updates are automatically available for AOL 9.x users when logging into the AOL

service.

Source: <http://secunia.com/advisories/22567/>

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	[fetch Target Ports (auto)] [fetch Target Ports (manual)]
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 29, KCAL-TV (CA)* — **Deputies detonate suspicious package on sidewalk in California.** Several lanes of traffic on Highway 111 were closed early Sunday, October 29, while sheriff's deputies detonated a suspicious package found outside a Blockbuster Video Store on the corner of Fred Waring Drive and Highway 111 in Palm Desert, CA. A video store employee saw a small carry-on suitcase on the sidewalk near the store and called police. No explosives or dangerous substances were found inside, according to Riverside County Sheriff's Sergeant Terrence Tingle.

Source: http://cbs2.com/topstories/local_story_302154521.html

43. *October 28, WCBS-TV (NY)* — **Homemade bomb explodes in Queens, New York.** Police say an 18-year-old man who lives at 85-30 75th Street in Queens, NY, set off a homemade pipe bomb in his driveway on Friday, October 27. The man was taken into custody after police found a second explosive device inside the man's home. They evacuated a two-block area around the scene for several hours while to remove the device safely. There were no injuries and there was no major damage caused by the bomb.

Source: http://wcbstv.com/topstories/local_story_301084050.html

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

General Sector

Nothing to report.

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

DHS Daily Open Source Infrastructure Report Contact Information

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

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

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

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

Department of Homeland Security Disclaimer

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.