



# Department of Homeland Security Daily Open Source Infrastructure Report for 30 December 2005

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 a New Jersey law that takes effect Sunday, January 1, is expected to curtail identity theft crimes by allowing residents to freeze access to their personal credit reports. (See item [6](#))
- The Associated Press reports Oregon police have zeroed in on a new front in the fight against drugs from Mexico and Canada: the small airports that dot the state's most rural regions. (See item [16](#))
- USA TODAY reports many of the nation's 50,000 public-safety agencies still can't communicate with each other in a crisis; incompatible radio equipment remains the main culprit. (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. *December 29, Lexington Herald-Leader (KY)* — **Coal mine deaths in 2005 could be record low.** Barring more accidents before January 1, 2005 could go down as perhaps the safest coal mining year in the history of the United States. As of Wednesday, December 28, 21 deaths related to coal mining had been posted this year by federal regulators. According to Suzy

Bohnert, a spokesperson for the U.S. Mine Safety and Health Administration, which compiles nationwide fatality statistics for all U.S. mining operations, the nation's coal mining states have six fewer deaths than in 2002, when there was a record low of 27. Four coal-mining deaths were reported this year in Alabama and Pennsylvania, Bohnert said, seven in Kentucky, three in West Virginia and one each in Ohio, Wyoming and Oklahoma. Meanwhile, several coal states, including Virginia and Tennessee, reported none, she said. Several factors — including fewer underground mines and miners, improved safety training and the proliferation of surface mining — have generally reduced mining accidents and deaths over the years, said Bill Caylor, president of the Kentucky Coal Association.

U.S. Mine Safety and Health Administration: <http://www.msha.gov/>

Source: <http://www.kentucky.com/mld/kentucky/13505489.htm>

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

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

### **2. *December 29, Associated Press* — Gas pipeline rupture triggers evacuations in Kentucky.**

About 300 residents of Allen County were allowed to return home Thursday morning, December 29, about seven hours after being evacuated because of a natural gas leak, officials said. There were no injuries when the ruptured Tennessee Gas pipeline began spewing out natural gas around 3 a.m. CST. The part of the line that ruptured had been previously welded, said Kentucky Division of Emergency Management spokesperson Gary Rogers. The scene of the 30-inch-diameter pipeline rupture happened in a rural section of southern Kentucky about 10 miles north of the Kentucky-Tennessee state line.

Source: <http://www.kentucky.com/mld/kentucky/news/13507904.htm>

### **3. *December 29, San Antonio Express-News (TX)* — Texas daycare evacuated after gas line break.** A Northwest Side daycare center was evacuated Wednesday morning, December 29, after construction workers cracked a nearby natural gas line leading into the building. No one was injured in the incident at Discovery World Learning Center in the 5400 block of Prue Road in San Antonio, TX. Officials said workers digging postholes to extend a fence along the side of the building struck the gas line at about 11:15 a.m. CST, causing a vapor leak. Teachers evacuated 62 children, ages six weeks to 12 years, to a nearby field. About an hour after the break, a utility company shut off the leak and teachers and children were allowed back into the building.

Source: <http://www.mysanantonio.com/news/metro/stories/MYSA122905.02B roundup6.237133b7.html>

### **4. *December 28, News-Topic (NC)* — Chemical release in North Carolina sends two to hospital.** The Lenoir Fire Department responded to an accidental chemical release early Christmas Day at the Gateway Nursing Center on Harper Avenue in Lenoir, NC. Lt. Sam Smith said the release of a substance into the air, which occurred in the facility's laundry room, was most likely caused by an employee error. "It appeared that a pickup tube that measures laundry cleaning agents was put in the wrong container...The readings indicated that there was a substance in the air," said Smith. He said the center's emergency protocols that were already in place helped minimize the serious nature of the event. He said the chemical release was not life threatening but could cause some breathing discomfort if people came in close proximity to the

substance. Smith said two employees of the nursing facility were taken by Caldwell Emergency Services to Caldwell Memorial Hospital for evaluation. "The two people that went for evaluation were employees that went to investigate the smell," said Smith. Smith said once the reading levels went back to normal the patients were allowed back into the wing.

Source: [http://www.newstopic.net/articles/2005/12/28/news/22chemical\\_releasesendsto.txt](http://www.newstopic.net/articles/2005/12/28/news/22chemical_releasesendsto.txt)

5. *December 28, WRTV-6 (IN)* — **Equipment fire at Indianapolis utility plant brought under control.** A fire at a Citizens Gas and Coke utility plant on the city's near east side caused authorities to restrict traffic in the area Wednesday morning, December 28. Officials said a piece of equipment caught fire just before 6 a.m. CST, at the plant, located in the 2900 block of Prospect Street. An internal fire department and the Indianapolis Fire Department responded, and the fire was under control by 7 a.m. The fire was confined to the area of the equipment, which removes impurities from gas during the process of baking coal into coke, an official said. No injuries were reported. Citizens Gas said the fire poses no health concerns for people in the area. Authorities restricted traffic near the plant. Flames shooting into the air from the plant represented an attempt to burn off some of the gas in a line affected by the equipment fire.

Source: <http://www.theindychannel.com/news/5687474/detail.html>

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

## Defense Industrial Base Sector

Nothing to report.

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

## Banking and Finance Sector

6. *December 29, Associated Press* — **New Jersey residents to see safeguards against identity theft.** A New Jersey law that takes effect Sunday, January 1, aims to stifle identity theft crimes by allowing residents to freeze access to personal credit reports. Under the new law, New Jersey residents can control access to their own credit reports. Without access to "frozen" reports, an identity thief cannot obtain a mortgage or a credit card using someone else's name, even with the victim's Social Security number. The new law requires businesses of all sizes to destroy unneeded consumer records and report security breaches to customers. Also, Social Security numbers can no longer be used on identity badges, membership cards or used to allow the holder to gain access to products or services.

Source: [http://money.iwon.com/jsp/nw/nwdt\\_rt\\_top.jsp?cat=TOPBIZ&src=704&feed=dji&section=news&news\\_id=dji-00051220051229&date=20051229&alias=/alias/money/cm/nw](http://money.iwon.com/jsp/nw/nwdt_rt_top.jsp?cat=TOPBIZ&src=704&feed=dji&section=news&news_id=dji-00051220051229&date=20051229&alias=/alias/money/cm/nw)

7. *December 29, Australian Associated Press* — **Australian bank closes fake Websites.** National Australian Bank and Australian Federal Police have moved to shut down eight overseas Websites involved in an e-mail banking scam targeting tens of thousands of Australians. The sites in China, Turkey, Korea and Germany -- linked to a phishing scam operating Australia-wide -- were put out of action over the past four days. National Bank spokesperson Mikala Sabin said the bank, which had also been working with Internet certification authorities

worldwide, was alerted to the scam on Monday, December 26, and immediately began tracking the source of the e-mails and closing down the scam sites. Sabin said the scam appeared to be from the same group of people who moved the scam sites to different countries as Websites were closed down. Sabin said the National Bank had initiated extra security measures that customers could use for Internet banking. The system involved a requirement to enter a special code sent to the customer's mobile phone. On two occasions customers had received a Short Message Service with a code that they had not requested which then had alerted the customers that their bank details were being accessed by a third party. Sabin said the bank then worked with the customers to change their passwords.

Source: <http://finance.news.com.au/story/0,10166,17684492-31037,00.html>

8. *December 29, TechWeb News* — **Post-holiday phishing may rise.** Scammers will be busy in the post-holiday weeks, a security firm warned Thursday, December 29, and consumers should be especially watchful for fake "get out of debt" phishing pitches. "Every year during the holidays, a high percentage of consumers find themselves spending a little more than anticipated, and then begin to panic," said Jordan Ritter, chief technology officer of Internet services company Cloudmark. "A phishing offer posing as your bank and offering to consolidate your credit card debt under one easy, low-rate card might be especially tempting now," said Ritter.

Source: <http://www.techweb.com/wire/security/175701073;jsessionid=PQOC25MC02MZEQSNDBECKHSCJUMEKJVN>

9. *December 28, Netcraft* — **Hundreds of phishing attacks used Secure Sockets Layer in 2005.** Internet services company Netcraft has identified more than 450 confirmed phishing URLs using "[https](https://)" urls to present a secure connection using the Secure Sockets Layer (SSL). Anti-phishing education initiatives have often urged Internet users to look for the SSL "golden lock" as an indicator of a site's legitimacy. Although phishers have been using SSL in attacks for more than a year, the trend seems to have drawn relatively little notice from users and the technology press. The golden lock icon is a simplification of complex security concepts into a single symbol that non-technical users could understand and trust. Phishing scams designed to prompt security warnings raise the stakes, requiring users to understand what the browser warning is telling them, and how they should respond. Many banks are shifting their online banking logins to the unencrypted home pages of their Websites, further complicating the issue of training customers to trust only SSL-enabled sites. The non-SSL presentation of these bank logins is already being incorporated into spoof pages.

Source: [http://news.netcraft.com/archives/2005/12/28/more\\_than\\_450\\_phishing\\_attacks\\_used\\_ssl\\_in\\_2005.html](http://news.netcraft.com/archives/2005/12/28/more_than_450_phishing_attacks_used_ssl_in_2005.html)

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

## **Transportation and Border Security Sector**

10. *December 29, USA TODAY* — **Delta's pilots union agrees to temporary pay cut.** Delta Air Lines pilots Wednesday, December 28, narrowly agreed to take a big pay cut for the second year in a row, averting the immediate threat of a devastating strike at the U.S.'s third-biggest airline. The Air Line Pilots Association said Wednesday that members voted 58 percent to 42 percent to accept a temporary 15 percent pay cut, which follows a voluntary 30 percent cut the

pilots took last year. Wednesday's vote result brought relief to Delta passengers, but bad blood between the airline and the union remains. The airline has insisted it needs a 20 percent pay cut from pilots, while the union accused the airline of overreaching. The two sides now have until March 1 to agree on a plan to cut pilot pay longer-term. If they don't reach a deal by then, they will go to binding arbitration. Under pressure from low-fare carriers and high fuel prices, Delta has posted non-stop losses, including a \$1.1 billion loss in the third quarter alone. The company is more than \$20 billion in debt, and its employee pension plans are under-funded by more than \$10 billion.

Source: [http://www.usatoday.com/travel/news/2005-12-28-delta-pilots-deal\\_x.htm](http://www.usatoday.com/travel/news/2005-12-28-delta-pilots-deal_x.htm)

11. *December 29, Associated Press* — **Governor Rendell says he'd shut down PATCO over dredging battle.** Pennsylvania Governor Ed Rendell would consider shutting down the city's light-rail connection to New Jersey if officials there refuse to back a \$300 million project to dredge the Delaware River, his spokesperson said. A proposal to deepen 103 miles of the shipping channel from 40 feet to 45 feet is strongly backed by Pennsylvania officials, who say it would increase cargo and jobs in the port. But the dredging requires a cooperation agreement New Jersey officials have been hesitant to approve, questioning its cost-effectiveness and environmental impact. If the Delaware River Port Authority does not approve the budget by its Saturday, December 31 deadline, the agency will be in technical violation of its bond agreements. The head of the port authority's New Jersey delegation, Jeffrey L. Nash, said that could affect its bond ratings and make borrowing more expensive. The port authority runs the PATCO High-Speed Line and the Ben Franklin, Walt Whitman, Betsy Ross, and Commodore Barry bridges. PATCO riders are largely New Jersey residents commuting to jobs in Philadelphia. Because bridge tolls subsidize PATCO, Rendell would consider the eventual step of not funding the rail line, spokesperson Kate Philips said Wednesday, December 28.

Source: <http://www.pennlive.com/newsflash/pa/index.ssf?/base/news-33/1135867743313090.xml&storylist=penn>

12. *December 29, Associated Press* — **Winston-Salem man arrested at Chicago airport.** A North Carolina man is charged with unauthorized use of a weapon and attempting to board an aircraft with a weapon. Chicago Police said a screener at O'Hare International Airport found the stun gun Wednesday night, December 28, in baggage belonging to John Adegbenjo, 35, of Winston-Salem. City Aviation Department spokesperson Wendy Abrams said Adegbenjo had planned to take a United flight to Greensboro, NC. She said he had flown into Chicago on a Lufthansa flight from Germany.

Source: <http://www.wxii12.com/news/5709488/detail.html>

13. *December 29, Chickasha News (OK)* — **Airplane searched while suspect awaits charges.** A Cessna 441 plane suspected of transporting drugs around the country was parked at the Chickasha, OK, Municipal Airport on Wednesday, December 28, while its pilot awaited arraignment in the Grady County Jail. Undersheriff Irene Perske said the county was contacted by the Department of Homeland Security that they were tracking a plane suspected of trafficking drugs and needed someone to intercept it when it landed at Chickasha. With the airport inside city jurisdiction, Perske said the operation was executed as a cooperative effort between Chickasha Police and Grady County Deputies. A cursory search of the plane when it touched down on Monday night did not reveal any drugs but Chickasha Police Officers and Grady County Deputies reportedly found a 9mm Beretta handgun and a rifle, according to

Deputy Investigator Brian Layton. The pilot, Leonard Christia Schwartz, 51, of California, was arrested by Chickasha Police on the charge of possession of a firearm after a prior conviction. Schwartz was reportedly convicted in 1981 on the charge of trafficking cocaine after being caught with almost a kilo of the drug. Schwartz went before a Grady County judge on Thursday, December 29, to be arraigned on the weapons charge.

Source: <http://www.chickashanews.com/viewarticle.php?id=3915>

14. *December 28, Associated Press* — **Secret Service forces plane to land.** There were some tense moments late Wednesday morning, December 28, for the pilot of a private plane and law enforcement authorities in southern Maryland. An 84-year-old Alexandria, VA, man was forced to land his Beechcraft plane in Indian Head. The Charles County, MD, Sheriff's Office says the man was returning from Stafford Regional Airport in Virginia to Clinton, MD, when he received instructions from flight controllers to turn around, indicating that they could not access his flight plan. The pilot acknowledged the order but did not hear a response. He then learned his plane was having an electrical problem and decided to put down at the Maryland airport a few miles away. Sheriff's Office investigators responded and interviewed the man with the United States Secret Service. No charges were filed, but the incident will be referred to the Federal Aviation Administration for review.

Source: [http://www.wusatv9.com/news/news\\_article.aspx?storyid=45490](http://www.wusatv9.com/news/news_article.aspx?storyid=45490)

15. *December 28, Orlando Sentinel (FL)* — **Independence Air warns unionized employees.** Bankrupt Independence Air, which operates two daily flights from Orlando, FL, to Washington, DC, sent furlough notices on Wednesday, December 27, to unionized employees warning the carrier could shut down in January. The notices said the furloughs would be effective January 7 if the airline's parent company, FLYi, did not find a buyer or major investors by then. FLYi, which launched the airline a year ago, has been looking for investors since filing for Chapter 11 protection in November. Spokesperson Valerie Wunder said the Washington-based airline sent the same message to non-unionized employees several months ago and that the company is "continuing to pursue a number of different options" despite the deadlines mentioned in the notice. If passengers are affected by any change in operations to Independence's overall 200 daily flights in 30 markets, she said, the information will be made public. All negotiations with possible buyers or investors are being handled confidentially in Delaware bankruptcy court, Wunder said.

Source: <http://www.orlandosentinel.com/news/orl-bk-airliner122805.0.940355.story?coll=orl-news-headlines>

16. *December 26, Associated Press* — **Oregon police track drug smuggling at rural airports.** Oregon police have zeroed in on a new front in the fight against drugs: the small airports that dot the state's most rural regions. Last month, officers seized 995 pounds of marijuana valued at almost \$6 million at Burns Municipal Airport, arresting Harvey Allen Gabel, 56, and Brian Jeffrey Lindroos, 39, who had landed in Burns to refuel after a flight from British Columbia. The British Columbia residents were transferred to federal custody in Eugene last week after being held since their arrest in the Harney County Jail on \$1 million bail each. They are facing federal charges of importing cocaine and marijuana and eluding U.S. customs inspectors, and up to 40 years behind bars if convicted. The extent of smuggling by air is "probably greater than law enforcement knows," Charles J. Karl, director of Oregon High Intensity Drug Trafficking Area Programs in Salem, wrote in a letter this month to the Office of National Drug

Control Policy in Washington, DC. Authorities believe methamphetamine, heroin and cocaine are smuggled into Oregon from Mexico, while marijuana is brought across the Canadian border.

Source: <http://www.oregonlive.com/newsflash/regional/index.ssf?/base/news-13/113558544349940.xml&storylist=orlocal>

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

## **Postal and Shipping Sector**

**17. *December 29, Bloomberg* — Shipping charges will rise to offset heavy fuel costs.** Neptune Orient Lines, Evergreen Marine, and other shipping lines plan to raise surcharges on land transportation of containers in the United States by as much as 41 percent because of higher fuel prices. Starting January 1, each container will cost \$222 to move by trucks and railroad in the United States, an increase from \$158, the 12-member Transpacific Stabilization Agreement said on its Website. A box moved by trucks alone will be charged \$64, 39 percent more than the current \$46, the group said. This is the second time the levies will be increased after they were introduced on August 16. Shipping lines are grappling with escalating port fees and fuel prices, as U.S. truckers and rail companies are charging more to move cargo within Asia's biggest export market. Higher fuel prices will inflate the expense of moving cargo to the United States in 2006 by seven percent. Other members of the Transpacific Stabilization Agreement include CMA CGM, Cosco Container Lines, Hapag-Lloyd, Hyundai Merchant Marine, Mitsui O.S.K. Lines, Nippon Yusen Kaisha, Orient Overseas Container Lines and Yang Ming Marine Transport.

Transpacific Stabilization Agreement Website: <http://www.tsacarriers.org/>

Source: <http://www.iht.com/articles/2005/12/29/bloomberg/sxshipping.php>

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

## **Agriculture Sector**

**18. *December 29, Associated Press* — U.S. Department of Agriculture to reimburse growers, farmers for hurricane damage.** The U.S. Department of Agriculture (USDA) has designated at least \$200 million for Florida growers and farmers who suffered losses from the 2005 hurricanes, officials said Wednesday, December 28. The funding, authorized under Section 32 of the Agricultural Adjustment Act, gives the USDA the discretion to pay agriculture producers compensation for losses from weather and reduced market prices. This is the first year that nursery growers will be able to receive the Section 32 funds. Hurricanes made 2005 one of the worst years in recent memory for Florida agriculture. Four storms that struck the state caused an estimated \$2.2 billion in damage to the state's crops and farming infrastructure. The four hurricanes caused estimated damages of \$1.1 billion to the state's nursery and foliage industry, \$370 million to the sugar sector, \$180 million to citrus, and \$44.1 million to tropical fruit, according to the Florida Fruit & Vegetable Association.

Source: <http://www.sun-sentinel.com/news/local/florida/sfl-fcanecash29dec29.0.6636716.story?coll=sfla-news-florida>

19. *December 29, News–Press (FL)* — **New canker trees found in Cape Coral.** Six diseased trees found in Cape Coral, FL, could delay the city's canker cleanup another month or more, a state official said Wednesday, December 28. In the latest Cape find, state workers discovered the six canker–infected trees between December 13 and December 22 in about five yards, said Liz Compton of the state agriculture department. State officials have chopped down the infected trees. Now they have to cut dozens of nearby "canker–exposed" trees that also could develop the contagious bacterial disease. State officials had hoped to finish the cleanup by fall, but various factors — including new canker finds and Hurricane Wilma — kept pushing that back. Storm winds and rain help spread canker bacteria. Compton said she expects chainsaw crews to finish cutting Lee County's canker–exposed trees by the end of January. Since 2002, state officials have found 30,083 canker–infected and canker–exposed trees in Lee County. About two–thirds of those were in Cape Coral. The rest were in Pine Island, North Fort Myers and the western fringes of mainland Lee County except for one find in Buckingham in the eastern part of the county.

Source: <http://www.news–press.com/apps/pbcs.dll/article?AID=/20051229/NEWS0101/512290380/1075>

20. *December 29, Associated Press* — **Vermont agency wants to create farm registry.** The Vermont Agency of Agriculture wants to keep closer track of all livestock in the state to be prepared in case of a disease outbreak. The agency has proposed requiring that all livestock farms register with the state. The new rules must first be approved by a legislative committee. If passed, they would take effect in July, officials said. The plan is part of a national effort to eventually identify every cow, pig, and chicken and store information about them in a database, officials said. The U.S. Department of Agriculture is developing an animal tracking system that would allow livestock to be traced within 48 hours. The state's livestock have been relatively disease–free for nearly 20 years, officials said. Vermont eradicated tuberculosis in 1979, brucellosis in 1982, and is working to control rabies and West Nile virus.

Source: <http://www.nytimes.com/aponline/business/AP–Animal–Health.ht ml>

21. *December 29, USAgNet* — **United Kingdom about to implement new livestock identification rules.** The farmers union in the United Kingdom is urging members to ensure their sheep and goats are identified correctly before they go for slaughter. New regulations imposed by the Food Standards Agency and the Meat Hygiene Service in the United Kingdom will mean that all sheep and goats must be identified with a UK or 'S' tag when they enter a slaughter plant. It will become the slaughterhouse operators' responsibility to guarantee that all animals accepted onto the slaughterhouse premises are properly identified. An official veterinarian will ensure that animals, whose identity is not reasonably ascertainable, are killed separately and declared unfit for human consumption. The new regulations come into effect on January 1.

Source: <http://www.usagnet.com/story–national.cfm?Id=1297&yr=2005>

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

## **Food Sector**

22. *December 29, Associated Press* — **Hong Kong partially lifts ban on U.S. beef.** Hong Kong said Thursday, December 29, it has partially lifted a ban on U.S. beef imports that became

effective two years ago following the discovery of mad cow disease in America. Hong Kong said that only boneless beef from cattle less than 30 months old could be imported to the city. The animal's brain, spinal cord and other parts with a high-risk of mad cow disease must be removed during slaughtering. "We will closely monitor the situation and review our import requirements as and when necessary," a government statement said. The government said it decided to partially lift the ban after becoming satisfied with enhanced U.S. control measures against mad cow disease. The ban had been effective since December 24, 2003, after mad cow disease was detected in a cow in Washington state.

Source: <http://www.chron.com/disp/story.mpl/ap/business/3553700.html>

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

## **Water Sector**

Nothing to report.

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

## **Public Health Sector**

**23. *December 29, Brown County Democrat (IN)* — Response to infectious disease outbreak tested.** The Brown, IN, Health Department, as well as federal, state, and local responders gathered at the Muscatatuck Urban Training Center for a two day training event dubbed "Operation SINBAD" (Southern Indiana Bioterrorism Attack and Defense), a field training exercise and response simulation sponsored by the Indiana Department of Homeland Security (IDHS). The purpose of the training was to help public health officials interact and address issues surrounding the outbreak and containment of a human introduced biological agent. Approximately 25 local health departments, several hospitals and universities, the Indiana State Police, along with the Indiana State Department of Health participated in the two-day event, which took place earlier this month. The training exercise included testing lab protocols, mass immunization plans, and procedures for utilizing the U.S. Centers for Disease Control and Prevention's Strategic National Stockpile of pharmaceuticals. Shane Modglin, Brown County's public health coordinator, said the training exercise was a great opportunity for the employees of the health department because each played the role they now hold. That, he said, allowed them to test a mass immunization plan, which calls for 600 doses to be given in one hour.

Source: <http://www.browncountyindiana.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=6806&TM=30375.63>

**24. *December 29, Reuters* — China confirms seventh human bird flu case.** China confirmed its seventh human infection — and third human death — from bird flu on Thursday, December 29, after officials revealed a 41-year-old factory worker died from the disease over a week ago. The victim, who died on December 21, lived in Sanming City in eastern China's Fujian province. Like previous human victims of the H5N1 virus in China, she apparently contracted the disease in an area that has not officially reported previous outbreaks among birds. Initial tests for the H5N1 virus were negative. But later tests by provincial investigators and China's Center of Disease Control showed positive results.

Source: <http://today.reuters.co.uk/news/newsArticle.aspx?type=global>

**25. *December 29, Agence France-Presse* — More bird flu cases confirmed in Romania.**

Laboratory tests have confirmed the presence of the deadly strain of bird flu virus in seven more samples sent from sites in southeast Romania, officials said. The tests were conducted in Britain on samples sent from areas in four departments of the southeast of the country where the virus had already been reported, said Nicolae Stefan, head of the Institute of Animal Health. Authorities had ordered the precautionary destruction of birds in the areas affected after initial tests had shown the broader H5 virus. The latest figures bring to 22 the number of localities where H5N1 has been confirmed in Romania since the first case was reported in early October. More than 100,000 head of poultry and other birds have been slaughtered since then.

Source: [http://news.yahoo.com/s/afp/20051229/hl\\_afp/healthfluromania\\_051229191252;\\_ylt=AjZtdhell1.uuPV1unsIL3eJOrgF;\\_ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCUI](http://news.yahoo.com/s/afp/20051229/hl_afp/healthfluromania_051229191252;_ylt=AjZtdhell1.uuPV1unsIL3eJOrgF;_ylu=X3oDMTBiMW04NW9mBHNIYwMIJVRPUCUI)

**26. *December 28, United Press International* — One billion dollars for labs to fight**

**bioterrorism.** The U.S. government plans to spend at least one billion dollars on new facilities to fight bioterrorism over the next decade. The government plans to build seven large new buildings housing laboratories for research designated "biosafety level-4," or BSL-4, reserved for life-threatening diseases with no known cure, reported the Wall Street Journal Wednesday, December 28. Labs that work on infectious microorganisms range in levels of biosafety from one to four, and the BSL-4 labs are high-security facilities that research the most infectious diseases, such as the Ebola virus. Research on BSL-4 agents has been limited to the U.S. Centers for Disease Control and Prevention in Atlanta, GA, and the U.S. Army Medical Research Institute of Infectious Diseases at Fort Detrick in Frederick, MD.

Source: <http://www.sciencedaily.com/upi/index.php?feed=Science&article=UPI-1-20051228-15304300-bc-us-labs.xml>

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

## **Government Sector**

**27. *December 29, Washington Technology* — Department of Homeland Security CIO needs**

**more power, IG says.** The Department of Homeland Security's (DHS) Chief Information Officer (CIO) lacks sufficient authority to carry out plans for integrating the IT infrastructure throughout the department, according to a new report by Richard Skinner, the department's inspector general (IG). However, DHS officials, in a management response, disagreed with the criticisms and asserted that the CIO has enough power. The inspector general's report outlines major management challenges at DHS, including shortcomings in procurement, financial management, border control, and Federal Emergency Management Agency's disaster response and recovery. DHS officials disagreed, saying the CIO has the right amount of authority to accomplish its mission. DHS managers said the department's Infrastructure Transformation Office is overseeing the IT transformation including establishing an integrated enterprise network, common email and help desk; creating two data centers; and initiating a departmentwide video operations capability.

IG Report: [http://www.dhs.gov/interweb/assetlibrary/OIG\\_06-14\\_Dec05.pdf](http://www.dhs.gov/interweb/assetlibrary/OIG_06-14_Dec05.pdf)

Source: [http://www.washingtontechnology.com/news/1\\_1/daily\\_news/27662-1.html](http://www.washingtontechnology.com/news/1_1/daily_news/27662-1.html)

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

## **Emergency Services Sector**

**28. *December 30, BBC News* — Europe testing satellite–navigation technology.** This week, the first test satellite in Europe's 3.4bn–euro (US\$4bn) Galileo satellite–navigation (sat–nav) system blasted off on a Soyuz rocket from Baikonur Cosmodrome in Kazakhstan. The final global network of 30 Galileo satellites is crucial to providing the high volumes of time– and location–based data needed for new services such as advanced sat–nav, mobile location data, natural disaster surveillance and air traffic control. Each motorist would need to carry a satellite–linked "smart box" in their car. The network would allow a vehicle's exact movements to be tracked, presenting new possibilities for road–user charging and tolling. The European Commission wants these units to be used for fleet and freight management and to launch emergency calls. Drivers would use a small keyboard to enter certain parameters at the beginning of a journey, such as how many passengers were on a coach, or whether a truck was carrying hazardous chemicals. In the event of an accident, the terminal would launch an emergency call. The call would also send the information entered by the driver, allowing emergency services to adapt their response to the situation. Using the Galileo signal, the terminal message would also pinpoint the precise location of the stricken vehicle.

Source: <http://news.bbc.co.uk/1/hi/sci/tech/4552132.stm>

**29. *December 28, USA TODAY* — Compatible radio systems would cost millions.** Many of the nation's 50,000 public–safety agencies still can't talk to each other in a crisis. Incompatible radio equipment is a main culprit. Even with more money for improved systems and frequencies, other hurdles thwart seamless communication among first responders. The federal government can't force all agencies in a state or region to buy the same gear; safety agencies often fail to plan for interagency communication in disasters or to train officers in how to talk to their counterparts; and technology standards that would let disparate radio systems talk with each other have been delayed. Safecom, a program in the Department of Homeland Security that promotes public–safety communication, predicts that free–flowing information among agencies will come by 2023. While Congress is expected to pass legislation that would give emergency responders more radio channels and money for new equipment, emergency officials say the money is inadequate and the frequencies won't come soon enough. Some are pursuing state or regional radio systems that counties or towns can join. Other areas have "gateways" that bridge disparate systems in emergencies.

Source: [http://www.usatoday.com/tech/news/techpolicy/2005-12-28-radio-systems\\_x.htm](http://www.usatoday.com/tech/news/techpolicy/2005-12-28-radio-systems_x.htm)

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

## **Information Technology and Telecommunications Sector**

**30. *December 29, Secunia* — Microsoft Windows WMF handling arbitrary code execution vulnerability.** A vulnerability has been discovered in Microsoft Windows, which can be exploited to compromise a vulnerable system. The vulnerability is caused due to an error in the

handling of corrupted Windows Metafile files (".wmf"). This can be exploited to execute arbitrary code by tricking a user into opening a malicious ".wmf" file in "Windows Picture and Fax Viewer" or previewing a malicious ".wmf" file in explorer (i.e. selecting the file). This can also be exploited automatically when a user visits a malicious Website using Microsoft Internet Explorer. The vulnerability has been confirmed on a fully patched system running Microsoft Windows XP SP2. Microsoft Windows XP SP1 and Microsoft Windows Server 2003 SP0 / SP1 are reportedly also affected. Other platforms may also be affected. Secunia recommends not opening or previewing untrusted ".wmf" files and set security level to "High" in Microsoft Internet Explorer.

Source: <http://secunia.com/advisories/18255/>

31. *December 29, IDG News Service* — **Gunman attack unnerves Bangalore outsourcing industry.** An attack by a gunman late Wednesday, December 28, at the Indian Institute of Science (IISc) in Bangalore, India has sent shockwaves through the city's large outsourcing industry. One person was killed and four injured in the gunfire on the campus of IISc, one of India's most prestigious educational institutes. They were part of a large group of scientists and professors that were coming out of a conference held in the auditorium of the IISc, when the gunman attacked. Bangalore police have so far said that they cannot definitely confirm that the attack was by terrorists. But the police have put the city on high alert and asked outsourcing companies to strengthen security. Earlier this year, police in India warned that the country's software and services outsourcing industry and other high technology installations are likely new targets for a terrorist group operating in the country. On Monday, December 27, the Delhi police arrested three suspected terrorists who were planning to attack software parks in Bangalore and Hyderabad besides other targets, the police said. Documents seized from three members of the Lashkar-e-Toiba terrorist group, revealed that they planned to carry out suicide attacks on some software companies in Bangalore.

Source: [http://ww6.infoworld.com/products/print\\_friendly.jsp?link=/article/05/12/29/HNgunmanbangalore\\_1.html](http://ww6.infoworld.com/products/print_friendly.jsp?link=/article/05/12/29/HNgunmanbangalore_1.html)

32. *December 29, TechWeb News* — **Microsoft promises to patch worsening zero-day flaw.** As bleaker details emerged Thursday, December 29, about the threat posed by a zero-day vulnerability in Windows, Microsoft said it would produce a patch for the flaw but declined to put the fix on a timetable. In a security advisory posted on its Website, Microsoft confirmed the vulnerability and the associated release of exploit code that could compromise PCs, and listed the operating systems at risk. Windows 2000 SP4, Windows XP, Windows Server 2000, Windows 98, and Windows Millennium can be attacked using the newly-discovered vulnerability in WMF (Windows Metafile) image file parsing, said Microsoft. The advisory stated that Microsoft will "provide a security update through our monthly release process or providing an out-of-cycle security update, depending on customer needs." Microsoft rarely goes out-of-cycle to patch a vulnerability — it's done so only three times since it began a once-a-month patch release schedule in October, 2003; the last time was over a year ago — and didn't patch early in December when another zero-day bug surfaced, even after experts called on the developer to fix fast.

Source: <http://www.informationweek.com/news/showArticle.jhtml;jsessionid=3NDZJAOEXY4NQOSNDBECKH0CJUMEKJVN?articleID=175701152>

33.

*December 28, Internetnews.com* — **Virus tempers MSN Messenger buzz.** Finnish security firm F-Secure is reporting a new scam that is masquerading as the MSN Messenger 8 Beta (to be released in several months), which will be called Windows Live Messenger. Rather than a beta of Microsoft's latest instant messaging (IM) client, users will download a virus file, BETA8WEBINSTALL.EXE. Once installed, the virus' payload connects the users IM client to a botnet and sends download links to the virus file to everyone on the users contact list. A Microsoft spokesperson told internetnews.com that this threat does not exploit a security vulnerability, but relies on significant user action to spread to all the contacts in a user's MSN Messenger contact list. With the declining cost of domain registrations, "throw-away" domains have become a popular breeding ground for transmitting viruses by hackers. MSN Messenger's successor, Windows Live Messenger, is part of Microsoft's rebranded "Live" initiative. According to the IM Logic Threat Center, MSN Messenger has borne the brunt of IM attacks with 43.1 percent of all attacks. In the last 90 days, the target has shifted to AOL's Instant Messenger (AIM) which now bears 44.8 percent of attacks in comparison to MSN Messenger at 26.1 percent in the same period.

Source: <http://www.internetnews.com/ent-news/article.php/3573971>

- 34. December 28, ZDNet News** — **Trojan delivers unwanted gift to Windows PCs.** A new Trojan horse program was infecting PCs on Wednesday, December 28, exploiting a hole in Windows systems to sneak onto computers, then dropping adware or spyware or turning them into zombies. The Trojan, dubbed Exploit-WMF (Windows Meta File), has the potential to continue to spread, said Dave Cole, director of security response at Symantec. The exploit "is misusing a function in the WMF library in Windows," dropping onto the machine a downloader Trojan "that pulls down its big brother, a more sophisticated Trojan" from a server on the Internet, he said. Kaspersky Lab rated the vulnerability "highly critical" and predicted that "new modifications of these programs may well appear in the near future." The WMF vulnerability affects computers running Windows XP with service pack 1 and service pack 2, and Windows Server 2003 with service pack 0 and service pack 1. It can be exploited when an Internet Explorer user -- or Firefox user under certain circumstances -- visits a Website that has malicious code on it or when a user previews .wmf format files with Windows Explorer. There is no patch for it yet from Microsoft, although antivirus vendors had released software to help protect against it.

Source: [http://news.zdnet.com/2100-1009\\_22-6011406.html](http://news.zdnet.com/2100-1009_22-6011406.html)

- 35. December 28, WebProNews.com** — **AdSense Trojan could be on the loose.** An Indian web publisher claims a Trojan program that replaces Google ads with a different set of ads has been found in the wild. A report on the TechShout website said a Trojan affecting AdSense has been discovered. Google has not confirmed this yet on the AdSense blog, but a web publisher named Raoul Bangera is said to have contacted Google about the problem. Google reportedly confirmed the information provided by Bangera, including screenshots, logfiles, and system files, demonstrated the ads displayed on his site were not legitimate. "We can confirm from the screenshots that these are fake Google ads, formatted to look like legitimate ads. We agree that this phenomenon is likely the result of malicious software installed on your computer," Google reportedly said in response. Only small publishers appear to be affected, not premium publishers or Google sites.

Source: <http://www.webpronews.com/topnews/topnews/wpn-60-20051228AdSenseTrojanCouldBeOnTheLoose.html>

36. *December 28, Government Computer News* — **DHS moves fingerprint tech forward.** The Department of Homeland Security (DHS) is working with the Departments of Defense and State, the FBI, and the Commerce Department’s National Institute of Standards and Technology as well as technology vendors to develop a new generation of 10–finger “slap capture” units for fingerprint collection. DHS’ interest in the new generation of fingerprint stations has been prompted in part by secretary Michael Chertoff’s decision announced this summer to require 10–fingerprint records of foreigners crossing the borders. Chertoff’s decision will bring the DHS’ Ident database of two–fingerprint records — which it inherited from the Immigration and Naturalization Service — in synch with the FBI’s Integrated Automated Fingerprint Identification System. DHS plans to deploy existing 10–print capture systems to border locations where they would be suitable. The federal agencies have formed a user group that has sponsored a detailed “Challenge to Industry” to develop the new units over the next year. The task will include development of hardware and software, according to procurement documents. The government expects to purchase between 3,000 and 10,000 of the new units, according to the documents.

Source: [http://www.gcn.com/vol1\\_no1/daily-updates/37842-1.html](http://www.gcn.com/vol1_no1/daily-updates/37842-1.html)

### Internet Alert Dashboard

#### DHS/US–CERT Watch Synopsis

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

**US–CERT Operations Center Synopsis:** US–CERT is aware of a vulnerability reported within Microsoft Windows handling of corrupted Windows Metafiles (".wmf"). This vulnerability may be exploited through the viewing of a corrupted ".wmf" file or by viewing a malicious web site hosting a corrupted ".wmf" file. US–CERT is also aware that exploit code is publicly available and that there are active attempts to exploit this vulnerability. Once exploited, a remote attacker may be able to perform any of the following malicious activities:

Execute arbitrary code

Cause a denial of service condition

Take complete control of a vulnerable system

Although there is limited information concerning this reported vulnerability, US–CERT encourages users to not view ".wmf" files and system administrators to block ".wmf" files at the HTTP proxy and the SMTP level. US–CERT is also aware of reports that this vulnerability may affect users of Microsoft Internet Explorer as well as Mozilla Firefox. We will continue to update current activity as more information becomes available.

For more information about this vulnerability please review US-CERT Vulnerability Note VU#181038 at URL:

Microsoft Windows Metafile handler buffer overflow

<http://www.kb.cert.org/vuls/id/181038>

Multiple Heap Buffer Overflow Vulnerabilities in Symantec Antivirus Library  
US-CERT is aware of a third party report of multiple heap buffer overflows in the Symantec RAR decompression library (Dec2RAR.dll). Although there is limited information concerning this reported vulnerability, US-CERT encourages users and system administrators to consider filtering or disabling the scanning of RAR archives at email or proxy gateways.

More information can be found in Symantec RAR decompression library contains multiple heap overflows:

US-CERT Vulnerability Note VU#305272 at URL:

<http://www.kb.cert.org/vuls/id/305272>

#### Current Port Attacks

<b>Top 10 Target Ports</b>	1026 (win-rpc), 445 (microsoft-ds), 135 (epmap), 139 (netbios-ssn), 1027 (icq), 1434 (ms-sql-m), 23 (telnet), 80 (www), 123 (NetController), 137 (netbios-ns) 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 [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Website: [www.us-cert.gov](http://www.us-cert.gov).

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

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

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

**37. *December 29, Rutland Herald (VT)* — Vermont city approves security camera plan.** Bellows Falls, VT, Police Chief Keith Clark is moving ahead with plans to install 16 surveillance cameras in public places next year, including several in the village square, train station, and parking lots. Bellows Falls Trustees approved using a \$98,000 federal grant Tuesday, December 27, to install the surveillance system and approved Clark's proposed locations for the cameras. Clark said the cameras, which will keep recordings for seven days before erasing them, will be centered in areas that have seen vandalism and crime or sites where there are potential security risks, such as the waste treatment facility. "We're focusing on areas where historically there have been problems," Clark explained. "And the village square is a busy and congested area." Footage from the cameras — a mix of silent color and black and white video — is an important law enforcement tool that could assist officers responding to an emergency situation, such as a robbery or fight, Clark said. Camera locations include the police/fire station, the pumping station, Red Light Hill, the public pool, water treatment facility, waste treatment facility, the Buckley and Hardy parking lots, train station, Great Falls Medical Center, and at least three in the village square.

Source: <http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/2005/1229/NEWS/512290354/1003/NEWS02>

**38. *December 29, USA TODAY* — Superdome major part of New Orleans' comeback.** The Louisiana Superdome, that hulking, bright white spaceship on the New Orleans skyline, is more than a stadium. It is a catalyst for downtown revitalization. It epitomizes the entertainment and tourism mecca that is New Orleans. Owned by the state, it is the home of the NFL's Saints. Now, those who run the Superdome hope its quick renovation — readying the stadium for football by All Saints Day, November 1, 2006 — will make it emblematic of a city rising again. "It is a symbol of the recovery and rebirth of New Orleans," says Doug Thornton, regional vice president of SMG, which manages the Superdome. This weekend the Superdome will be empty and the streets of downtown New Orleans quieter than usual around New Year's Day. The Sugar Bowl, an annual event for more than 70 years, will take place in Atlanta's Georgia Dome. Because of the construction, the Superdome probably will not be available as a shelter during the 2006 hurricane season, which begins June 1. There are no plans to modify the Superdome to make it a better storm shelter. "That would cost \$30 (million) to \$40 million," Thornton says.

Source: [http://www.usatoday.com/travel/destinations/2005-12-28-super\\_dome-cover\\_x.htm](http://www.usatoday.com/travel/destinations/2005-12-28-super_dome-cover_x.htm)

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

## **General Sector**

**39. *December 29, Associated Press* — New storm to add to swollen California rivers.** California braced for another storm system this week — one starting Friday, December 30, and lasting through the weekend — after heavy rain swelled rivers in the north to their highest levels in seven years, causing power outages and forcing some residents to evacuate. The system was expected to spread farther south by Saturday, December 31, and potentially cause mudslides, debris flows, and flash floods in recently burned areas of Southern California, said Rob Hartman of the National Weather Service. In Modesto, a mudslide led to a pileup that killed a motorist on Monday, December 26. The main concern is heavy runoff overwhelming the Central Valley's intricate system of dams, weirs and levees. Housing developments have boomed in valley flood plains in recent years, raising the stakes for water managers who try to empty downstream reservoirs before they overflow with runoff. Federal and state water managers were releasing torrents of water at the Oroville and Folsom dams, but both reservoirs had plenty of capacity to handle additional runoff.

Source: <http://msnbc.msn.com/id/10632481/>

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

### **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.