



Department of Homeland Security Daily Open Source Infrastructure Report for 29 January 2007

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 safety experts say that determining what caused an Indonesian jetliner, a Boeing 737, to plunge into the sea with 102 people on board is important for global aviation safety in case there are structural problems with the world's most popular aircraft. (See item [17](#))
- The Department of Transportation has released a manual that will help airlines, airports, and local governments prepare to stop the introduction of emerging diseases and to recognize and control pandemic outbreaks before they have a widespread impact on public health. (See item [19](#))
- The University of Arkansas reports an interdisciplinary team of researchers has developed a portable biosensor for in-field, rapid screening of avian influenza virus that detects the avian influenza strain H5N1 in poultry in less than 30 minutes. (See item [33](#))

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. *January 26, Platts Energy Bulletin* — NRC plans major revision of its enforcement policy. The Nuclear Regulatory Commission (NRC) said it is planning a major revision of its

enforcement policy, chiefly to clarify the use of terms and enforcement issues that have changed or did not exist when the agency's policy was first published in 1980. NRC said it wants to update terms that were originally crafted for conventional enforcement and that are now also used for the significance determination process under NRC's reactor oversight process. NRC said it wants to consider enforcement issues associated with the construction phase of new reactors and new requirements in relation to safeguards and security. In its January 25 Federal Register notice, NRC says public comments are due by March 26.

Federal Register Notice: <http://frwebgate2.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=832803262065+4+0+0&WAIAction=retrieve>

Source: <http://www.platts.com/Nuclear/News/8851963.xml?sub=Nuclear&p=Nuclear/News>

2. *January 26, Associated Press* — **Union seeks federal help to resolve staffing issue.** The union representing most workers at the Pilgrim Nuclear Power Plant in Plymouth, MA, is seeking the help of federal nuclear regulators in a dispute with management over staffing levels. The Utility Workers Union of America Local 369 is petitioning the Nuclear Regulatory Commission (NRC) to stop plant owner Entergy Nuclear Operations from gaining the ability to reduce the number of radiation protection technicians on night shifts from two to one. The union says it's a safety issue. If a nuclear reactor has a leak on a weekend night, there could be just one radiation protection technician to check and test 80 sites, delaying critical response time. "We want to feel very confident, if there's an accident or a situation, the facility can respond as rapidly as possible," said David Leonardi, a senior operations instructor and 20-year employee at the plant. There are currently two radiation protection technicians on every shift. Under federal regulations, most other plants are required only to have one of each class of technician on duty at a time.

Source: <http://news.bostonherald.com/localRegional/view.bg?articleid=179348>

3. *January 26, Radio Free Europe* — **Georgia: Uranium case underscores nuke safety fears.** A Russian man, authorities allege, tried to sell a small amount of nuclear-bomb grade uranium in a plastic bag in his jacket pocket last summer. The buy was a setup by Republic of Georgia authorities, with the help of the CIA. The incident raises fresh fears worldwide that some of Russia's huge nuclear stockpiles could fall into terrorist hands. The international community is concerned about how 100 grams of nuclear-bomb grade uranium fell into the hands of a 50-year-old Russian trader, who specialized in fish and sausages. But Ivan Safranchuk of the Moscow office of the U.S.-based Center for Defense Information, says getting hold of highly enriched uranium in Russia is not that easy. "Over the past nine years, serious efforts have been made to improve the system of physical protection and security of nuclear facilities, both military and civilian. So in my opinion, obtaining nuclear substances in Russia is extremely difficult. Today, if I were a terrorist seeking nuclear substances, I would go to Pakistan, not Russia," Safranchuk says. But Vladimir Chuprov of Greenpeace says security at Russian nuclear facilities remains deplorable. "In Russia, the physical defense and security of radioactive material doesn't meet the required standards," Chuprov says.

Source: <http://www.rferl.org/featuresarticle/2007/01/573b0a06-2f67-4d30-93d4-7c9d5a034899.html>

[[Return to top](#)]

Chemical Industry and Hazardous Materials Sector

4. *January 26, Houston Chronicle* — **DuPont plant releases acidic compound.** A release of a sulfuric acid compound from a La Porte chemical plant Thursday, January 25, led to the temporary closure of Texas 225 and prompted local schools to keep their students inside for about an hour. The plant, operated by DuPont, released oleum, or disulfuric acid, sending a mistlike plume toward Pasadena, according to state and company officials.
Source: <http://www.chron.com/disp/story.mpl/metropolitan/4500696.htm>

5. *January 26, Odessa American (TX)* — **Two hundred gallons of hydrochloric acid send up cloud of gas.** A hydrochloric acid spill Thursday, January 25, at the intersection of FM 1936 and Highway 158 in Goldsmith, TX, formed an early morning gas cloud and shut down Highway 158 for hours while environmental crews cleaned up the noxious solution. Thursday morning, a Halliburton–owned 4,000–gallon tanker truck toppled after turning east onto Highway 158 from the farm–to–market road. The overturned truck rested about 30 feet from the intersection. About 200 gallons of the acid spilled out, mostly north of the shoulder area. It closed down Highway 158 between FM 1936 and Highway 385, about a four–mile section. Texas Commission on Environmental Quality regional director Jed Barker said the solution was 15 percent hydrochloric acid. When officials arrived on the scene the acid created a cloud over the affected ground.
Source: <http://www.oaoa.com/news/nw012607a.htm>

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

Defense Industrial Base Sector

6. *January 26, Government Accountability Office* — **GAO–07–211: Force Structure: Joint Seabasing Would Benefit from a Comprehensive Management Approach and Rigorous Experimentation before Services Spend Billions on New Capabilities (Report).** Joint seabasing is one of several evolving concepts for projecting and sustaining forces without relying on immediate access to nearby land bases and could be the source of billions of dollars of investment. In future security environments, the Department of Defense (DoD) expects to encounter situations of reduced or denied access to areas of operation. Even where forward operating bases are otherwise available, their use may be politically undesirable or operationally restricted. The Government Accountability Office (GAO) was asked to address the extent to which (1) DoD has employed a comprehensive management approach to joint seabasing, (2) DoD has developed a joint experimentation campaign plan for joint seabasing, and (3) DoD and the services have identified the costs of joint seabasing options. For this review, GAO analyzed joint requirements documents, experimentation efforts, and service acquisition plans. GAO recommends that DoD develop a management approach that includes senior leadership involvement, a dedicated implementation team, and a communications strategy; and develop an experimentation campaign plan and total ownership cost estimates for seabasing options. DoD agreed with the recommendations, except for the need for a dedicated implementation team.
Highlights: <http://www.gao.gov/highlights/d07211high.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-211>

7.

January 26, Federal Computer Week — **DoD considering use of high-tech balloons, UAVs as communication relays.** The Department of Defense (DoD) will launch a new generation of communications satellites to serve mobile users in 2009, even though it has no funds for satellite receivers. Meanwhile, DoD is spending \$1 billion a year on commercial broadband satellite service because of schedule delays in developing advanced military broadband satellite systems. Air Force Maj. Gen. William Lord said he is considering the use of high-tech balloons and unmanned aerial vehicles (UAVs) as communications relays to help bridge the satellite gap. Lord and other top DoD officials spoke at the 2007 SpaceComm Conference, sponsored by the Rocky Mountain chapter of AFCEA International.

Source: <http://www.fcw.com/article97492-01-26-07-Web>

8. *January 26, Federal Computer Week* — **DISA launches second NCES collaboration tool procurement.** The Defense Information Systems Agency (DISA) has released its second solicitation for Net-Centric Enterprise Services (NCES) online collaboration tools and expects to award the contract in June, DISA Director Air Force Lt. Gen. Charles Croom said Thursday, January 25, at the AFCEA SpaceComm 2007 conference, sponsored by the Rocky Mountain chapter of AFCEA International. DISA has decided to use the federated search tool developed by the intelligence community for its Intelink integrated intelligence site for NCES, Croom said.

Source: <http://www.fcw.com/article97485-01-26-07-Web>

9. *January 25, Washington Technology* — **Navy to buy more unmanned aviation systems.** The Navy plans to hold a competition to fill the requirement for a small, tactical unmanned aerial system in the coming months. Already proven to be valuable in Iraq and Afghanistan, small unmanned aerial vehicles are used by the Navy and Marines for surveillance and reconnaissance in battlefield situations. These small vehicles are expected to provide persistent intelligence, surveillance and reconnaissance support for tactical level decisions and unit level defense, and protection for Navy ships and Marine Corps ground forces. The draft request for proposal is expected to be released this fall.

Source: http://www.washingtontechnology.com/news/1_1/daily_news/30036-1.html?topic=defense

[[Return to top](#)]

Banking and Finance Sector

10. *January 26, Finextra (UK)* — **Customers want stronger authentication for Web banking, says RSA.** An overwhelming majority of consumers would willingly ditch password protection in favor of stronger authentication technology for online banking, according to a global poll published by RSA security. The survey of nearly 1,700 customers in eight countries also found that 82 percent want banks and brokerages to monitor online and telephone banking transactions for suspicious activity — similar to the way that credit card transactions are monitored. Furthermore, 91 percent are willing use a new authentication method, beyond the standard username-and-password procedure, if their banks decided to offer stronger security. Over two third of respondents (69 percent) say banks should replace the standard username-and-password log-in procedure with stronger authentication. More than half (58 percent) also want banks to ramp up telephone banking authentication. But consumers are

divided on the kind of stronger authentication they want. Nearly three quarters (73 percent) voted for "risk-based" authentication, which involves a behind-the-scenes assessment of the user's identity based on factors including log-on location, IP address and transaction behavior. Around 40 percent said they would like to use a hardware token for authentication, while 56 percent opted for image-based authentication.

RSA Study: <http://finextra.com/finextra-downloads/newsdocs/RSAauth.pdf>

Source: <http://finextra.com/fullstory.asp?id=16432>

11. *January 26, Sophos (UK)* — **'Who wants to be a millionaire?' e-mail scam attempts to defraud Internet users.** Sophos has warned Internet users of a new e-mail scam that pretends to be a lottery notification from the makers of the hit TV game show "Who wants to be a millionaire." The e-mail claims that the recipient has won a lottery run by the TV show which has been a hit around the world, and asks for the claimant to reply with their personal information in order for the winnings to be transferred. The e-mail tells recipients to contact a yahoo.co.uk e-mail address, and also lists two UK 070 personal phone numbers for people who wish to make contact via telephone or fax. Last week Sophos revealed that 070 telephone numbers are frequently used by lottery scammers who can redirect calls using the system to any phone number in the world. This week Sophos published its annual Security Threat Report, which detailed many of the different disguises used by e-mail scammers in their attempts to commit identity theft and swindle money out of Internet users.

Sophos Report: <http://www.sophos.com/report2007>

Source: http://www.sophos.com/pressoffice/news/articles/2007/01/tvmi_lion.html

12. *January 26, Honolulu Advertiser (HI)* — **Welfare families' data stolen, state reveals.** Hawaii has alerted some 11,500 families enrolled in a program for low-income women and children to guard against credit fraud and identity theft, after a Health Department employee allegedly stole information from a client database. Three families registered with the Women, Infants and Children program in Wahiawa have been confirmed as identity theft victims, said Dr. Chiyome Fukino, director of the Health Department. The state is urging others in the Wahiawa WIC programs' database, which includes clients helped as far back as 1998, to place a fraud alert on their credit reports. Officials say the case is the first of its kind involving a state agency. "I think the real message here is anyone can be a target. It doesn't matter what your income level is," Fukino said. Identity theft is one of the fastest-growing crimes in the Islands, and large databases of information are increasingly becoming targets. Though business records are more commonly hit, officials say it is not unheard of nationally for low-income clients of social service agencies to also become victims.

Source: <http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID=/20070126/NEWS15/701260357/1001>

13. *January 25, InformationWeek* — **Attorney General's credit-card theft highlights prosecution problems.** A recent attempted theft using the Massachusetts attorney general's credit card — and her comments about it — have renewed focus on jurisdictional problems authorities face when prosecuting credit-card and identity-theft cases. The state's top prosecutor, Martha Coakley, told the Boston Herald that it was unlikely the case would be prosecuted. Coakley received a call from Dell to confirm that she had purchased a \$1,250 computer and wanted it shipped to a Texas address. Coakley told the company she hadn't ordered the computer and called to have the card canceled. Her comments after the incident

have drawn attention to an issue police departments struggle with — whether, how, and where to prosecute credit-card theft when a victim reports such a crime. Paul Stephens, policy analyst for the Privacy Rights Clearinghouse, says that, for many local police departments, credit-card theft appears to be a low priority. "In some jurisdictions, there's a reluctance to investigate," he says. "Some local police departments won't even take a report." It also appears to be a low priority for credit-card issuers. Stephens says: "[Financial institutions] sort of seem to fold it into the cost of doing business."

Source: <http://www.informationweek.com/showArticle.jhtml;jsessionid=SIJKE1FOA21QQOSNDLPSKH0CJUNN2JVN?articleID=197000632>

- 14. January 25, CNET News — IBM donates new privacy tool to open-source.** IBM has developed software designed to let people keep personal information secret when doing business online and donated it to the Higgins open-source project. The software, called "Identity Mixer," was developed by IBM researchers. The idea is that people provide encrypted digital credentials issued by trusted parties like a bank or government agency when transacting online, instead of sharing credit card or other details in plain text, Anthony Nadalin, IBM's chief security architect, said. "Today you traditionally give away all of your information to the man in the middle and you don't know what they do with it," Nadalin said. "With Identity Mixer you create a pseudonym that you hand over." For example, when making a purchase online, buyers would provide an encrypted credential issued by their credit card company instead of actual credit card details. The online store can't access the credential, but passes it on to the credit card issuer, which can verify it and make sure the retailer gets paid. "This limits the liability that the storefront has, because they don't have that credit card information anymore," Nadalin said.

Source: http://news.com.com/IBM+donates+new+privacy+tool+to+open+source/2100-1029_3-6153625.html?tag=cd.lede

- 15. January 25, VNUNet — U.S. official accused of paying 419 scammer \$1.2 million.** A former treasurer of Alcona County in Michigan has been arrested after allegedly investing more than \$1.2 million of county funds in Nigerian fraud scams. Sophos said that Thomas Katona, who was treasurer of Alcona County for 13 years, has been charged with forgery and multiple counts of embezzlement. It is reported that county treasury employees became suspicious of Katona's dealings after local bank officials informed them that he had directed several unauthorized transfers to overseas accounts during late 2006, including to beneficiaries linked with Nigerian 419 scams. It was then uncovered that he had made further payments using his personal savings, and had previously been advised by bank officials that he was investing money in fraudulent schemes.

Source: <http://www.vnunet.com/vnunet/news/2173418/official-accused-paying-419>

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

Transportation and Border Security Sector

- 16. January 28, Associated Press — Maine travel agent soon to start booking space vacations.** A Maine travel agent, Pamela Hurley-Moser, was one of 45 agents across North America selected for training to become an "accredited space agent." That means that eventually she'll be able to reserve seats aboard Virgin Galactic's sub-orbital space flights. It's expected to cost

\$200,000 for a two and one-half hour flight 75 miles above the Earth's surface. The first flight isn't scheduled to take off until 2009. Hurley-Moser is going to the Kennedy Space Center in Florida this week for a two-day training session. She'll learn how to market the trips, find clients, and answer any questions potential space tourists may have. Virgin Galactic, established by British tycoon Richard Branson, is one of several startup companies that plan to rocket ordinary people into space. Its goal is to ferry 500 people in its first year — roughly the same number of people who have gone up in 45 years of space travel. Virgin Galactic's initial tourist flights will take off from California and possibly from a proposed facility in New Mexico called Spaceport America.

Source: http://www.boston.com/news/local/articles/2007/01/28/maine_travel_agent_soon_to_start_booking_space_vacations/

17. *January 27, Associated Press* — **Experts say investigation into Indonesian plane crash important to global aviation safety.** Determining what caused an Indonesian jetliner to plunge into the sea with 102 people is important for global aviation safety in case there are structural problems with the world's most popular aircraft, experts said Saturday, January 27. Signals from the Boeing 737's flight recorders, also known as black boxes, have been traced to the ocean floor at a depth of about a mile, but the government says it does not have the sea salvage technology needed to recover them. The Adam Air plane disappeared after running into 80 mile per hour winds off Sulawesi Island on New Year's Day. The pilot did not issue a mayday or report technical problems before the jetliner fell off radars at 35,000 feet. Indonesia has asked for international help recovering the black boxes, but with their battery life of 30 days about to expire, "time is of the essence," said Jim Hall, a former chairman of the U.S. National Transportation Safety Board. Ken Johnson, the former executive of the Transportation Safety Board of Canada, noted that the crash could be tied to poor maintenance, pilot error, sabotage, weather, structural faults or "a million other reasons." "It might be very, very simple, but conversely, it could be something extremely important," he said.

Source: <http://www.chinapost.com.tw/latestnews/2007127/43966.htm>

18. *January 26, Government Accountability Office* — **GAO-07-149: Rail Safety: The Federal Railroad Administration Is Taking Steps to Better Target Its Oversight, but Assessment of Results Is Needed to Determine Impact (Report).** Since 1980, the train accident rate has improved significantly, but progress has leveled off over the past 10 years. Recent serious accidents—such as one in Graniteville, SC, that led to nine deaths and 292 injuries—elevated concerns. The Federal Railroad Administration (FRA) develops safety standards and inspects and enforces railroads' compliance with these standards. This report addresses how FRA (1) focuses its efforts on the highest priority risks related to train accidents in planning its oversight, (2) identifies safety problems on railroad systems in carrying out its oversight, and (3) assesses the impact of its oversight efforts on safety. To complete this work, the Government Accountability Office (GAO) reviewed FRA regulations, planning and policy documents, and safety data. GAO also contacted FRA officials in headquarters and three regional offices and others. GAO is recommending that FRA develop measures of the direct results of its oversight and evaluate the effectiveness of its enforcement program. The Department of Transportation did not provide overall comments on these recommendations but did provide several technical comments, which were incorporated as appropriate.

Highlights: <http://www.gao.gov/highlights/d07149high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-149>

19. *January 25, Department of Transportation* — New manual helps airports respond to international passengers with communicable diseases. A manual released today will help airlines, airports and local governments prepare to prevent the introduction of emerging diseases to the United States, Secretary of Transportation Mary E. Peters announced. She noted that the manual will help officials recognize and control pandemic outbreaks before they have a widespread impact on public health. Secretary Peters said, "This manual will help airports, airlines, and local officials take steps now to get prepared, save lives, and keep our transportation network running." The manual sets out the roles of the pilot-in-command, airline operations center, the airport operator, state and local health and emergency management departments, law enforcement agencies, health care facilities, support organizations and federal government agencies when a flight arrives with ill passengers on board. The manual covers the planning needed to address an incident while the plane is in flight and upon arrival at the airport. It also discusses the treatment of passengers and crew that may have been exposed to illness and discusses recovery after an incident. Printed versions of the report may be ordered at no charge from: DOT Warehouse, 3341 75th Avenue, Landover, MD 20785-1511. The manual is available on the Internet at <http://isddc.dot.gov/OLPFiles/OST/013334.pdf> Source: <http://www.dot.gov/affairs/dot1007.htm>

20. *January 25, USA TODAY* — Airline delays set record in 2006. Airline delays increased sharply last year to record highs because of a rash of bad weather starting in the fall that shut airports and stranded thousands of passengers, according to federal data. The rise in delays demonstrates that the system is becoming more vulnerable to airport snarls as flights increase in crowded cities such as New York, Chicago and Atlanta. The data also show the system has improved in some ways. Last summer, for example, delays never reached the peaks of 2000. Summer typically has the most delays because of thunderstorms. There were delays of at least 15 minutes for 22 percent of flights on large airlines through November, according to the most recent data from the federal Bureau of Transportation Statistics. "The air-traffic control system is under stress because of the demand and unusual weather. The airline system is under stress because of the high load factors and the economic pressures," says Massachusetts Institute of Technology aeronautics professor John Hansman. Air Transport Association President Jim May said the rise in delays highlights the need for new technologies. "It inevitably is going to get worse because of the demands on a system that is at capacity," said May. Source: http://www.usatoday.com/travel/flights/2007-01-25-record-air-delays_x.htm

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

Postal and Shipping Sector

21. *January 25, USPS News Release* — Mail handlers union members approve five-year contract. Members of the National Postal Mail Handlers Union have voted to ratify a new five-year contract. The new contract will run through November 20, 2011, and affect approximately 55,000 career U.S. Postal Service (USPS) employees who are engaged in bulk transfer, loading, and unloading of mail. The agreement provides for retroactive and future general wage increases. The contract also contains continuation of cost-of-living adjustments at current levels and a reduction in the Postal Service contribution rate for health insurance by

one point during each year of the contract.

Source: http://www.usps.com/communications/news/press/2007/pr07_008.htm

22. *January 25, Great Falls Tribune (MT)* — **Powder in letter sent to Blackfeet not toxic.** The mysterious powder sent with a threatening letter that shut down the Blackfeet Tribal Office in Great Falls, MT, on Wednesday, January 24, was not toxic. A hazardous materials team from Malmstrom Air Force Base, tested the substance and cleared all tribal employees to return to work. People working in the tribal office itself didn't return to work until 1 p.m. MST because the heat system had been shut down to prevent the possibly contaminated powder from spreading. "The staff is well trained with how to handle these situations," Tribal Vice Chairman Roger Running Crane said. The FBI is investigating the source of the letter.

Source: <http://www.greatfallstribune.com/apps/pbcs.dll/article?AID=/20070125/NEWS01/70125011>

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

Agriculture Sector

23. *January 26, Associated Press* — **Fish-killing virus found in Lake Huron.** A fast-spreading aquatic virus threatening the Great Lakes fishing industry has been detected in Lake Huron for the first time, officials said Thursday, January 25. The Michigan Department of Natural Resources said it had confirmed the presence of viral hemorrhagic septicemia (VHS) in fish samples from waters as far north as Cheboygan — only about 15 miles from where Lake Huron meets Lake Michigan. VHS previously had been found in only two of the Great Lakes — Ontario and Erie — and in Lake St. Clair, which links lakes Erie and Huron. But officials have predicted the virus eventually would spread across the entire lakes system, where the \$4.5 billion fishery is a crucial segment of the economy. "This disease threatens the closure of a major portion of the Michigan baitfish industry," said Chris Weeks, president of the Michigan Aquaculture Association. "It is also expected to have significant impacts on the aquaculture industry and Michigan's recreational fisheries."

Source: http://www.cbsnews.com/stories/2007/01/26/ap/tech/mainD8MSMB_300.shtml

24. *January 26, Associated Press* — **CWD found near Waukesha County, WI.** Professional sharpshooters are being used in the Kettle Moraine State Forest for the first time because chronic wasting disease (CWD) is discovered in deer there. As many as nine cases of CWD have been found on the border of Waukesha, WI.

CWD information: <http://www.cwd-info.org/>

Source: http://www.twincities.com/mld/twincities/news/breaking_news/16552368.htm

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

Food Sector

25. *January 26, USAgNet* — **Investigation launched after United Kingdom heifers went untested for bovine spongiform encephalopathy.** The British Food Standards Agency (FSA) has launched an investigation into how an over thirty month (OTM) heifer entered the food

chain without being tested for bovine spongiform encephalopathy (BSE). Testing of all cattle that are over thirty months at slaughter is mandatory if they are intended for human consumption. The FSA said that all of the meat will have passed its use-by date, even if frozen by the consumer. A full investigation into the circumstances of this incident is underway. Since the OTM BSE testing regime came into force in November 2005, about 400,000 OTM cattle have been slaughtered in the United Kingdom for human consumption. This is the third occasion the FSA is aware of when an OTM bovine has entered the food chain untested.
Source: <http://www.usagnet.com/story-national.php?Id=208&yr=2007>

26. *January 25, Dow Jones* — U.S. rule would let in 610,000 older Canada cattle yearly. A recently unveiled U.S. plan to let Canada ship older cattle — usually too decrepit to produce milk anymore — to the U.S. for slaughter would result in an average of about 610,000 of them crossing the border yearly, according to an estimate made by the U.S. Department of Agriculture (USDA). The U.S. has banned such “cull cattle” since Canada reported its first case of bovine spongiform encephalopathy (BSE) in May 2003. The U.S. eased restrictions on cattle under 30 months old, which are the bulk of Canadian exports, in July 2005. The younger cattle are believed to be far less likely to be infected with BSE. All of the eight BSE cases found in Canada — and the three discovered in the U.S. — have involved cattle over 30 months old. A “Key Economic Impacts” summary that USDA recently distributed to state agricultural leaders is a five-year prediction. It says the imports of Canadian cattle over 30 months old “would account for about 10 percent of U.S. cull cattle slaughter.”

Source: <http://www.cattlenetwork.com/content.asp?contentid=100880>

27. *January 25, Associated Press* — Japan rejects review of U.S. beef rules. The Japanese government has rejected a U.S. request for early talks about easing restrictions on American beef imports, an official said Thursday, January 25. “We are not in a stage to accept consultations toward reviewing the trade conditions for now,” Yoshio Kobayashi, vice minister of the Agriculture, Forestry and Fisheries Ministry, said. Kobayashi said it was too early to enter talks with the U.S. as Japan’s verification of U.S. beef exporting conditions had not been completed. He did not indicate when the verification would be finished. The minister’s comments were in response to a letter from the U.S. urging Japan to ease its import conditions, the ministry said. After meeting U.S. Agriculture Secretary Mike Johanns in Washington earlier this month, Japan’s Agriculture Minister Toshikatsu Matsuoka said Japan was still conducting “deliberations” on the safety of U.S. beef. Japan must also conduct an audit of American beef plants, study the results and make the information available to the public.

Source: <http://www.forbes.com/feeds/ap/2007/01/25/ap3362121.html>

28. *January 25, Food Safety and Inspection Service* — Pasta salad recalled. Garden Leaf Foods, a Gardena, CA, firm, is voluntarily recalling approximately 1,591 pounds of pasta salad with chicken that may be contaminated with *Listeria monocytogenes*, the U.S. Department of Agriculture’s Food Safety and Inspection Service (FSIS) announced Thursday, January 25. The products were distributed to retail establishments in Arizona, California, Nevada and New Mexico. The problem was discovered through routine FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. Consumption of food contaminated with *Listeria monocytogenes* can cause listeriosis, an uncommon but potentially fatal disease.

Source: http://www.fsis.usda.gov/News_&_Events/Recall_006_2007_Release/index.asp

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

Water Sector

29. *January 26, Associated Press* — **Invasive mussels could threaten California water supply pipelines.** Lake divers have found no more quagga mussels, but state officials say they will continue to hunt for the invasive, pipe-clogging mollusks they fear could wreak havoc with water lines supplying Southern California. Quagga mussels were found earlier this month at Lake Mead in Nevada and Lake Havasu near the Metropolitan Water District (MWD) of Southern California's Whitsitt intake facility. The discoveries launched a wider search for infested reservoirs and pipelines in California that are connected to the Colorado Aqueduct, which supplies water to an estimated 18 million people. Advertisement Officials have searched the inlet tower of Diamond Valley Lake near Hemet, Lake Matthews in Riverside County and Lake Skinner near Temecula. So far, no additional mussels have been spotted. “Although it shows adult mussels are not currently in the area of the reservoirs that we're checking, it doesn't mean the quaggas are not in the lake because of the larvae,” said MWD spokesperson Bob Muir. The mollusks can plug pipes up to 12 inches in diameter, and restrict flow in larger pipes. The colonies can also speed corrosion of pipes and other underwater infrastructure. Until the mussels were found this month in Lake Mead, they had not been spotted in the western U.S. Source: <http://www.signonsandiego.com/news/state/20070126-1000-ca-in-vasivemussel.html>
30. *January 20, Bellingham Herald (WA)* — **Thieves target copper.** Bellingham, WA, Parks Department employees found Friday, January 19, that newly installed water pipes at Joe Martin Field had been dug up and hauled away. The park thefts are part of a global wave of copper theft related to soaring prices for the metal. Gina Gobo, project engineer for the parks department, said the thieves also took a drinking fountain attached to the pipe at Joe Martin Field. She estimated the loss at \$1,400 for materials alone, and added that the job of replacing them would cost a lot more than that. The Joe Martin Field theft occurred less than three weeks after the Taylor Avenue incident, reported Dec. 29, in which the thieves got 350 feet of 1½-inch copper water pipe that was exposed under the dock. Source: <http://www.bellinghamherald.com/102/story/46903.html>

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

Public Health Sector

31. *January 26, Washington University School of Medicine* — **Disabling key protein may give physicians time to treat pneumonic plague.** The deadly attack of the bacterium that causes pneumonic plague is significantly slowed when it can't make use of a key protein, scientists at Washington University School of Medicine in St. Louis report. Speed is a primary concern in pneumonic plague, which kills in three to four days and potentially could be used in a terrorist attack. The bacterium that causes plague, *Yersinia pestis*, is vulnerable to antibiotics, but by the time an unusual infection becomes evident, *Yersinia* often has gained an unbeatable upper hand. Previous research had suggested that pneumonic plague might be spreading in the body in part through use of a protein known as plasminogen activator (PLA). Researchers thought PLA

might be a tool *Yersinia* uses to break open protective blood clots that form around pockets of infection. This clotting response is believed to be a way the body attempts to limit the spread of infections. Scientists speculated that breaking open the clots might be how *Yersinia* opened a path from the lungs into the blood. When scientists infected mice with *Yersinia* that lacked PLA, though, they found infection ebbing in the lungs but spreading to the spleen. The mice still died, but it took them several days longer to do so.

Source: <http://mednews.wustl.edu/news/page/normal/8590.html>

32. *January 25, Bloomberg* — **Vaccine for children wins U.S. panel's vote.** Sanofi–Aventis SA, the largest French drugmaker, won the backing of a U.S. advisory panel Thursday, January 25, to sell a combination vaccine for five childhood diseases, including polio. A U.S. Food and Drug Administration (FDA) panel voted 13 to two in favor of the vaccine, Pentacel, after studies showed four doses of the product protected children from getting sick. U.S. officials recommend 23 separate shots for infants and Pentacel would cut that number to 16, or about two fewer at every check–up. Doctors and scientists advising the FDA said the vaccine appears to work at least as well as vaccines that target the diseases individually and may boost immunization rates by requiring fewer shots. The vaccine would be given to infants in four doses, at two months, four months, six months and 15 to 18 months of age, to protect against diphtheria, tetanus, polio, whooping cough and invasive Hib disease. About 90 percent of U.S. children now get multiple vaccines to ward off these diseases.

Source: <http://www.bloomberg.com/apps/news?pid=20601085&sid=a5WwFH2GyzMg&refer=europe>

33. *January 25, University of Arkansas* — **Rapid response to avian flu threat.** An interdisciplinary team of researchers led by Yanbin Li, professor of biological engineering in the University of Arkansas Division of Agriculture, has developed a portable biosensor for in–field, rapid screening of avian influenza virus. The inexpensive device specifically and sensitively detects the avian influenza strain H5N1 from poultry cloacal or tracheal swab samples in less than 30 minutes and could help health officials coordinate a rapid response for the eradication, quarantine and vaccination of animals. The biosensor is a portable instrument designed for field use. It can be operated as a stand–alone instrument or connected to a laptop computer for data acquisition, analysis and control. The researchers are currently pursuing funding for further testing and evaluation. Based on Li's previous research on impedance biosensors to detect *Salmonella* and *E. coli*, the new system uses magnetic bio–nanobeads, a specially designed microfluidic biochip and red blood cell complexes to detect the virus.

Source: <http://dailyheadlines.uark.edu/9896.htm>

34. *January 22, Albert Einstein College of Medicine* — **Bioterrorism alerts induce anxiety and may pose health risk, study finds.** In the wake of September 11, 2001, the government and the media have periodically alerted the American people to potential threats of bioterrorism. A team of researchers at the Albert Einstein College of Medicine of Yeshiva University has found that such messages measurably raise anxiety levels, which could pose adverse health effects. Researchers conducted their study with volunteers recruited from students enrolled at both Einstein and Ferkauf. Potential participants were asked if they would participate in a research study involving the perception of a public health message and its relation to anxiety. The 116 participants (26 men and 90 women) randomly received one of two messages: either a potent bioterrorism message portraying a graphic account of a horrific case of bioterrorism, or a

message more neutral in tone that presented bioterrorism as a risk that was minor relative to other public health challenges. Those receiving the more potent message became the “experimental” group, while those receiving the more neutral message were considered the “control” group.

Source: <http://www.aecom.yu.edu/home/news/PRdetails.asp?isPR=1&id=344>

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

Government Sector

35. *January 25, Phoenixville News (PA)* — Pennsylvania county schools 'panic button' demonstrated. Some 75 members of Montgomery County’s public safety community and school systems Wednesday, January 24, were on hand at the courthouse to witness a demonstration of the panic–button system that the county intends to install in each of the county's approximate 650 public, private, and parochial schools, day–care centers and nurseries. The panic–button system essentially will tap into the county's 911 system, allowing, without human intervention, for the immediate dispatch of emergency personnel to a school. Protecting school children is a major concern of police chiefs throughout the county, according to Lower Merion Police Superintendent Joseph J. Daly. "Right now, no such alert system exists," Daly said. "Right now as I stand here, I have no way of knowing if something is going on at a school. Even just getting an alert telling me that something is going on at a school is 100 percent more information than I possess right now." "This system will not protect our children absolutely, but this is a quantum leap for us in protecting those children," Daly said. Daly's comments came at the conclusion of a brief, real–time demonstration of the system that included alerts going out instantly to reporters' cell phones.

Source: <http://www.phoenixvillenews.com/site/news.cfm?newsid=17747330>

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

Emergency Services Sector

36. *January 27, CBS5 (CA)* — Study finds Marin residents unprepared for tsunami. Residents of Marin County's coastal communities in Northern California got mixed grades in a study measuring their knowledge of tsunamis. The study was conducted last spring by Matthew S. David, a professor of psychology at Dominican University of California in conjunction with the Marin County Office of Emergency Services. The study concluded that coastal residents knew about tsunami hazards in general, but didn't know the warning signs for the potentially lethal wave of water that often accompanies an earthquake on the ocean floor. Residents were also unsure of how much time they had to evacuate after a tsunami starting somewhere around the Pacific Rim, or after a strong earthquake off the coast of Northern California, according to the study. The survey concluded coastal residents need more education about tsunami risks.

Marin County OES: <http://www.co.marin.ca.us/depts/ES/main/index.cfm>

Source: http://cbs5.com/localwire/localfsnews/bcn/2007/01/27/n/HeadlineNews/MARIN-TSUNAMI/resources_bcn.html

37.

January 27, Times–Standard (CA) — **Mock drill mobilizes university.** With 7,000 students, Humboldt State University (HSU) in Arcata, CA, is the size of a small town—so it's important that HSU have a comprehensive emergency plan, said University Police Chief Tom Dewey. Faculty, staff, administrators and students participated in a comprehensive emergency drill Friday, January 26. Dewey announced that “the big one” had struck campus and the university needed to shut off gas lines and direct water mains toward fighting fires. Police from other California State University campuses would be arriving “as soon as they can drive or fly,” Dewey said. One woman, during the role–playing exercise, asked what to do about students who were rioting. But communication appeared to be the key issue—communication with students and their parents, with university staff and faculty and with the community at large. As well as the HSU Campus Emergency Response Team, outside agencies involved in the drill included the Eureka and Arcata police and fire departments, the Humboldt County Sheriff's Department and the U. S. Coast Guard. Local ham radio operators were also on hand.

Source: http://www.times-standard.com/local/ci_5100547

38. *January 26, Henry Daily Herald (GA)* — **Make–believe emergency tests preparedness.** On Friday, January 26, emergency response teams from across Clayton County, GA, responded to the mock emergency to test their ability to work together and respond to a major crisis in the area. Over 300 people—emergency workers and actors—participated in the exercise. SWAT teams entered the courthouse to rescue “hostages” and stop “terrorists” wearing orange reflective vests. In the parking lot, people pretended to be wounded, laying on the cold pavement waiting for a hazardous material team to treat them for possible exposure to anthrax. “We had the (Center for Disease Control) up in Atlanta bring us down some non–active anthrax so our guys could test it,” said Alex Cohilas, chief of the Clayton County Fire Department. Cohilas said his initial reaction to the drill was that the overall it went well—“at least a B+”—but there was some things that need work. “We’re probably going to need to add another tactical radio frequency,” he said. The exercise was filmed and monitored and notes from it will be compiled and turned in to Cohilas. Cohilas and the other department heads will review the report and figure out how to better respond to emergencies – both real and practice.

Source: http://www.henryherald.com/homepage/local_story_026214848.html?keyword=leadpicturestory

39. *January 26, Bellingham Herald (WA)* — **Disaster drill a ‘surreal’ event.** A mass–casualty drill was held in Bellingham, WA, on January 26. The scenario called for a radioactive bomb to blow up a car outside an office building, setting fire to part of the building and killing and injuring several people. The focus of the drill, which involved about 250 people, was to see how local agencies would and could respond in the first few hours of a large–scale emergency. It was found that Bellingham’s Emergency Operation Center could be set up in under an hour. Minor communication problems hampered parts of the drill, requiring people to use cell phones instead of radios at times. But the biggest problem was the failure to create a joint information center, which was one of the objectives, said John Gargett, a contracted organizer of emergency drills. The center, which would be separate from the Emergency Operations Center, was supposed to be where the media and others could gather information about the situation from several agencies. Another problem came with making sure all the agencies were notified. A full report on the training is expected to be released in February.

Source: <http://www.bellinghamherald.com/255/story/47424.html>

Information Technology and Telecommunications Sector

40. *January 26, InfoWorld* — **Symantec warns of new zero-day Word attack.** Hackers are exploiting a new, unpatched vulnerability in Microsoft Word that could allow them to take control of a victim's computer, Symantec has warned. The zero-day vulnerability is the fourth in Microsoft's widely used Word 2000 software that has not yet been patched, the security company said in its Security Response Weblog. This vulnerability one affects most versions of Windows running Word, Symantec's advisory said. The attack comes via an infected Word document, a method increasingly used by hackers for targeted attacks. If the document is opened, it installs a Trojan horse program, called Trojan.Mdropper.W, onto the computer. The Trojan also puts other files on a computer that enable a hacker to control it.
Symantec Advisory: <http://www.securityfocus.com/bid/22225/info>
Source: http://www.infoworld.com/article/07/01/26/HNnewwordzerodayattack_1.html
41. *January 26, VNUNet* — **Flaw found in PGP Desktop encryption tool.** Users of the popular PGP Desktop encryption tool are being urged to upgrade to the latest version of the software after the discovery of a flaw in the code. The flaw exists in the Windows Service which PGP Desktop installs, and could be used by any local or remote user to run code with escalated privileges. Vulnerability testers NGS Software rated the flaw as a "medium risk" and said that it affects versions of the software earlier than PGP Desktop 9.5.1. The company does not yet have a workaround and is urging all PGP Desktop users to upgrade as a matter of urgency.
Source: <http://www.vnunet.com/vnunet/news/2173564/flaw-found-pgp-encryption>
42. *January 25, University of New Hampshire* — **UNH unveils Cyber Threat Calculator.** Hackers, terrorists and nations all use computers, but who really is capable of damaging U.S. critical infrastructure? The University of New Hampshire (UNH) Thursday, January 26, unveiled the UNH Cyber Threat Calculator, which assesses the level of threat any attacker poses to specific sectors in the country that rely on information technology. The UNH Cyber Threat Calculator was developed by researchers at UNH Justiceworks and students, and offers a new method to identify and quantify the threats posed to the United States' cyber infrastructure. To determine the overall threat level, analysts enter data for a particular organization or country into the calculator, which assigns a value to variables that measure the actor's intent and technological capabilities. These variables assess the actor's intent to use cyber warfare means, as well as its technical capabilities to put such means into practice. The higher number assigned to a possible attacker by the calculator, the greater the threat.
Source: http://www.unh.edu/news/cj_nr/2007/jan/lw25cyber.cfm
43. *January 25, eWeek* — **Apple ships Airport security update.** Apple on Thursday, January 25, shipped an Airport security update to fix a kernel panic issue that could allow attackers to cause system crashes. The company's fix comes almost two months after the issue was first flagged in the Month of Kernel Bugs project in November 2006. Apple credited the anonymous researcher known only as L.M.H. for reporting the issue. This comes one day after the release of a QuickTime update to fix a flaw exposed by L.M.H., but in that instance Apple did not acknowledge the controversial researcher.
Airport Update: <http://docs.info.apple.com/article.html?artnum=305031>

Source: <http://www.eweek.com/article2/0.1895.2087724.00.asp>

44. January 25, eWeek — CA predicts more attacks on experienced users. The continued rise of IT threats that seek to trick even the most careful PC users ranks among the top issues highlighted by software maker CA in its latest online security research report. Published on Thursday, January 25, the 2007 Internet Threat Outlook highlights the most pressing online security trends projected to have an impact over the next 12 months. According to CA, malware writers will continue to blend multiple threat formats and utilize new, covert distribution methods in 2007, making it harder for even the most informed users to discern the difference between legitimate content and attacks. CA said malware brokers will continue to piece together threats such as Trojan horse viruses, worms and the many forms of spyware to hide their attacks and evade technological defenses. With the level of professionalism rising quickly among the most sophisticated virus distributors, CA predicts that zero-day exploits, drive-by malware downloads and extremely intricate phishing schemes will continue to become more dangerous and harder to detect. Of particular danger to PC users will be blended threats that combine different elements of the various attack models, such as spam-borne Trojans and cross-site scripting code loaded onto legitimate Websites.

Report: http://www3.ca.com/Files/SecurityAdvisorNews/ca_2007_internet_threat_outlook_final.pdf

Source: <http://www.eweek.com/article2/0.1895.2087584.00.asp>

45. January 25, IDG News Service — Half of pirated Vista is malware. About half of the downloads claiming to be free versions of Microsoft's Vista operating system are actually malicious Trojan horse software, security vendor DriveSentry warned Thursday, January 25. With Vista's consumer launch just days away, hackers have been bombarding discussion boards with offers of "cracked" versions of Windows Vista, which are typically being distributed on peer-to-peer networks, said John Lynch, vice president of sales and marketing for DriveSentry. These posts offer downloads of the operating system that skip Vista's activation process, created by Microsoft to prevent users from running illegal copies. Users who fall for the scam can end up with some pretty nasty problems, according to Lynch. DriveSentry researchers have found malicious key-logging software and spyware on about half of the downloads it has examined recently, he said.

Source: http://www.infoworld.com/article/07/01/25/HNpiratedvista_1.html

Internet Alert Dashboard

Current Port Attacks	
Top 10 Target Ports	The top 10 Target Ports are temporarily unavailable. We apologize for the inconvenience. Source: http://isc.incidents.org/top10.html ; Internet Storm Center
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov .	
Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it-isac.org/ .	

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

46. *January 28, Courier–Journal (KY)* — **Experts disagree over Lake Cumberland level.** An outside group of engineers recommended a much more drastic lowering of Lake Cumberland than the 10–foot drop the Army Corps of Engineers began last week. Those experts backed lowering the lake level an additional 30 to 70 feet to take pressure off the leaky Wolf Creek Dam as a safety precaution. But David Hendrix, manager of a project to fix the dam, said corps officials decided that an extreme drawdown wasn't necessary. They believed they could protect people who live downstream by lowering the water level to 680 feet above sea level, he said. Hendrix, who is overseeing a \$309 million, seven–year project to shore up the aging dam, said the corps also cited other reasons for not lowering the water more: Power plants that serve more than one million people would be affected. For instance, the hydroelectric plant at Wolf Creek Dam could be left with its intake line above water. A worst–case scenario could have caused an estimated \$3 billion in damage, much of it in Nashville, 280 miles down the Cumberland River from the dam. For people on the downstream side of the dam, the concerns are more about how they would deal with a flood that could arrive quickly.

Source: <http://www.courier-journal.com/apps/pbcs.dll/article?AID=/20070128/NEWS01/701280457/1008>

[[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.