



# Department of Homeland Security Daily Open Source Infrastructure Report for 16 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 Nebraska Department of Agriculture has unveiled a new avian influenza surveillance program -- Avian Influenza: Testing Pays! -- for Nebraska poultry producers, providing free avian influenza tests of birds to any poultry producer who requests it. (See item [19](#))
- The Associated Press reports police and sheriff's deputies rushed to check on churches early Sunday, January 14, after fires broke out at two Baptist churches and a break-in was discovered at a third in Greenville, North Carolina. (See item [38](#))

### 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 14, Associated Press* — **Ice storm lashes much of U.S.; crews struggle to restore power as storm moves east.** The ice storms that have been blamed for at least 20 deaths continued to lash much of the nation Sunday, January 14, as crews tried to restore power to hundreds of thousands. Missouri Governor Matt Blunt (R) said about 300,000 households there remained without power on Sunday. About 350 National Guardsmen were going door to door checking on residents in the hardest-hit areas and were helping to clear slick roads of tree limbs and power lines. About 111,000 customers lacked power in Oklahoma, utilities reported. In Nebraska, which has been pummeled by winter storms in the past month, the weekend storm

dropped even more snow, making roads treacherous. In the St. Louis region, about 150,000 people remained without power Sunday afternoon, after a pattern of freezing and thaws. As the storm began to fade from the nation's midsection, parts of the East began to suffer.

Ameren news release: <http://www.myfoxstl.com/myfox/pages/News/Detail?contentId=2060481&version=1&locale=EN-US&layoutCode=TSTY&pageId=3.2.1>

Oklahoma Gas & Electric news release:

<http://www.oge.com/systemwatch/newspage.asp?newsid=42>

Source: <http://www.abcnews.go.com/US/print?id=2794630>

2. *January 14, Mercury (PA)* — **NRC: Dry casks not part of new 9/11 safeguards.** In the wake of the 9/11 attacks, the Nuclear Regulatory Commission (NRC) required existing nuclear plants to develop new, more stringent security procedures including ways to protect against an attack with an airplane. What neither the NRC or the industry addressed, however, is whether standards for dry cask fuel storage facilities should also be upgraded to protect against a 9/11-type attack. Tony Pietrangelo of the Nuclear Energy Institute said there was no reason to address changes in the dry cask storage regulations because they are already adequate. NRC spokesperson Neil Sheehan said that the NRC has conducted vulnerability assessments for dry cask storage systems, and that the results "indicate that it is unlikely that a significant release of radioactivity would occur from a ground assault or a large aircraft impact on a dry spent fuel storage cask." David Lochbaum of the Union of Concerned Scientists said he does not consider dry storage casks to be the greatest risk at a nuclear plant under attack from a plane, although he does have some concerns. More vulnerable, Lochbaum said, are the spent fuel pools located inside the reactor buildings.

Source: [http://www.pottstownmercury.com/site/news.cfm?newsid=17709994&BRD=1674&PAG=461&dept\\_id=18041&rfi=6](http://www.pottstownmercury.com/site/news.cfm?newsid=17709994&BRD=1674&PAG=461&dept_id=18041&rfi=6)

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

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

3. *January 12, NBC 10 (PA)* — **Residents urged to remain indoors following chemical plant fire.** A 5-alarm fire destroyed a Berks chemical plant Thursday night, January 11. Fire officials said the fire destroyed the Misco Cleaning Supplies factory in Bern Township, PA, but noted that no one was injured. As the fire burned, officials warned people in the area to stay inside their homes, but it is not clear what chemicals burned and if they were harmful.

Source: <http://www.nbc10.com/news/10731915/detail.html>

4. *January 11, WFSB (CT)* — **Noxious fumes prompt evacuations.** Police activity closed Ocean State Job Lot along the shoreline in Old Saybrook, CT, late Thursday morning, January 11. The building was evacuated because of some type of noxious fumes.

Source: <http://www.wfsb.com/news/10723514/detail.html>

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

## **Defense Industrial Base Sector**

5. *January 11, Defense Industry Daily* — **Israel's defense exports reached \$4.4 billion in 2006.** In a Tuesday, January 9, release, Israel's Ministry of Defense has confirmed that the country's 2006 Defense Export contracts broke all records, reaching over \$4.4 billion in 2006 and making Israel one of the top five defense exporters in the world behind the U.S., Russia, Britain and France. Israel's tight deploy–design–deploy cycle in an environment where many of the designers can expect to personally use the equipment in battle has made their equipment very popular, and signature global successes like the LITENING pod have helped raise the profile of Israeli firms.  
Source: <http://www.defenseindustrydaily.com/2007/01/israels-defense-exports-reached-44b-in-2006/index.php>
6. *January 11, Federal Computer Week* — **Navy next–generation e–warfare targets cellular spectrum.** The Office of Naval Research (ONR) has asked industry to help develop next–generation electronic warfare technologies that will extend the Navy's e–warfare dominance over a broader range of spectrum, including frequency bands used by cell phone companies, FM radio and TV stations. ONR said it also wants to develop the capability to detect, locate, track and counter radio frequency emitters beyond the traditional scope of Navy and Marine Corps e–warfare systems. Both services operate EA6B Prowler aircraft that fly e–warfare missions to support all military services. The goal of e–warfare is to control the electromagnetic spectrum by exploiting, disrupting or denying enemy use while ensuring that friendly forces can use it, ONR said.  
Source: <http://www.fcw.com/article97333-01-11-07-Web>

[[Return to top](#)]

## **Banking and Finance Sector**

7. *January 14, Onalaska Life (WI)* — **Online loan scam reports prompt warning from Better Business Bureau.** The Wisconsin Better Business Bureau (BBB) is issuing a nationwide alert regarding a company that alleges to be located in Milwaukee and has scammed consumers out of more than \$15,000. The Wisconsin BBB has received six complaints in less than a week against an online loan company called Intrest Plus Financial (the spelling of the word “interest” is correct). These complaints allege that Intrest Plus Financial approved a loan for the applicants, but required a “collateral payment” be wired to a Canadian address via MoneyGram. In some cases, applicants were coerced into sending a second payment after being told that their loans had been “reassessed.” None of the complainants have received their loans. Amounts lost range from \$1,570 to \$3,760. Victims have come from Colorado, Illinois, North Carolina, California and Nevada. All of the complainants applied for their loans online.  
Source: [http://www.onalaskalife.com/articles/2007/01/14/news/06loans\\_cam.txt](http://www.onalaskalife.com/articles/2007/01/14/news/06loans_cam.txt)
8. *January 12, TechWeb* — **New phisher tactic: Pay me or I'll kill you.** A new e–mail scam contains a death threat, Sophos said Friday, January 12, and marks a new low in scammer tactics. The spammed message claims to come from a professional hit man who supposedly has orders to murder the recipient, but will drop the contract if he is paid \$80,000. The "killer" says he has been shadowing the recipient for 10 days, and will produce taped evidence of the planned killing for a down payment of \$20,000. According to Sophos, it's just as likely that the scammer will try to dupe the recipient out of personal information, such as bank account

numbers and passwords, as to follow through on the demand for money. Graham Cluley of Sophos said, "The intention of this e-mail is clearly to frighten the recipient into coughing up a substantial amount of money or, at the very least, their bank account details."

FBI Advisory: <http://www.fbi.gov/cyberinvest/escams.htm>

Source: <http://www.techweb.com/showArticle.jhtml;jsessionid=MQ5MFFGI4PS3AQSNDLRCKHSCJUNN2JVN?articleId=196900571>

9. *January 12, eWeek* — **University of Idaho reports computer thefts.** The theft of three desktop computers from the Advancement Services office at the University of Idaho in November may have put personal data of university alumni, donors, employees and students at risk. An internal investigation by the university revealed that six months prior to the theft, the stolen hard drives contained datasets with names, addresses and Social Security numbers for about 70,000 individuals. The theft occurred during the Thanksgiving holiday and was discovered and reported by an employee in the university's Advancement Services department. The incident remains under investigation by the Latah County Sheriff's Office, which asked the university to delay notification of the theft to preserve the integrity of the criminal investigation. To date, school officials said they have no indication that the information has been accessed, misused or used for fraudulent purposes. As a precaution, the University of Idaho is making a broad public notification about the computer theft to approximately 331,800 individuals.

Source: <http://www.eweek.com/article2/0,1895,2082796,00.asp>

10. *January 12, SecurityFocus* — **Spammers get bullish on stocks.** A year ago, stock spam made up only about five percent of all spam e-mail messages, according to MessageLabs. Now, stock spam is on a trajectory to become the biggest category in unsolicited e-mail marketing, with 35 percent or more of spam touting a stock. Symantec has also noted the trend, finding that the monthly fraction of spam dedicated to stocks varies between 20 percent and 40 percent. The increasing popularity of stock-touting spam is also notable because the total amount of spam — driven by botnet activity — is on the rise. While a Christmas drop in the number of compromised PCs appears to have led to a general drop in spam volume, the number of PCs coopted by botnets for use in spamming operations continues to increase. Stock spammers are becoming more savvy about the practice. "The spam in the early day — by which I mean the late 1990s — use to contain blatant falsehoods," said John Reed Stark of the Securities and Exchange Commission. "It was very easy to prove the false statements. Now, the spammers aren't as bold in their projections and use disclosures to attempt to appear legitimate."

Source: <http://www.securityfocus.com/print/news/11435>

11. *January 10, Cleveland Plain Dealer* — **The latest online scam.** The "puppy scam," is one of the newest tricks among Internet scam artists, said Sue McConnell of the Better Business Bureau of Cleveland. Victims are lured to Websites offering rare dog breeds at affordable prices. Photos and text are often stolen from Websites of legitimate breeders, McConnell said. The puppy purchaser is told to wire payment in advance, and the seller continues soliciting money until the buyer gives up. By then, however, the money is irretrievable. The cases are often reported to the FBI or Internet crime investigators, McConnell said. But most of these scam artists typically operate overseas, and the anonymity of the Internet makes these cases nearly impossible to solve, she said. Blogs and message boards are filled with posts from victims, alerting others to variations of the puppy scam. TerrificPets.com, which matches

prospective buyers with breeders, keeps a running list of suspected scammers who have tried to use the site.

Source: <http://www.cleveland.com/printer/printer.ssf?/base/news/116843010895130.xml&coll=2>

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

## **Transportation and Border Security Sector**

- 12. *January 15, Brampton Guardian (Canada)* — Handgun found in luggage at Pearson Airport.** A loaded handgun was located by Canadian Air Transport Security Authority (CATSA) officers in the carry-on luggage of a traveler going through Pearson International Airport. On Saturday, January 13, the suspect presented his carry-on bags for screening. During the screening process, the CATSA officer observed the outline of a handgun within the luggage. Peel Regional Police located a .25 caliber handgun within the carry-on bag, along with a magazine that contained ammunition. Police have charged 51 year-old Marcos Placeres Padron of Louisville, KY, with Carry a Prohibited Weapon Carelessly, Possession of a Firearm without a License, Possession of a Prohibited Firearm, along with Ammunition and Submit for Screening while in Possession of a Weapon. The investigation is continuing by the Airport Division Criminal Investigation Bureau.  
Source: [http://www.northpeel.com/br/regionalnews/story/3843094p-4447\\_143c.html](http://www.northpeel.com/br/regionalnews/story/3843094p-4447_143c.html)
- 13. *January 12, Associated Press* — Plane at Ohio airport isolated after bomb threat reported.** A commuter plane preparing for takeoff from Toledo, OH, with 33 people aboard was isolated on a runway on Friday, January 12, after a passenger reported a bomb threat, officials said. Authorities had not verified whether there was a bomb aboard the American Eagle plane, said FBI spokesperson Scott Wilson. Fire trucks and emergency vehicles began to approach the area after the plane — with all its passengers still aboard — had sat on the runway for about an hour. Buses also were being brought in. The 911 call came in from a passenger's cell phone, acting Deputy Fire Chief Greg Locher said. He did not say whether the caller found out about the threat or was the one making the threat. The plane had pushed away from the terminal and was getting ready to take off for Chicago when officials found about the call, said Andrea Huguely, spokesperson with American Eagle, an American Airlines regional carrier. Thirty passengers and three crewmembers were on board; no injuries were reported, she said.  
Source: <http://www.startribune.com/484/story/932656.html>
- 14. *January 12, KFMB (CA)* — Dead body found on Africa-Atlanta flight.** A body was found in an airplane wheel well after a Delta Air Lines flight from Africa landed in Atlanta Friday morning, airline spokesperson Betsy Talton said. The flight had left Dakar, Senegal, more than nine hours earlier. It landed at Hartsfield-Jackson Atlanta International Airport. No additional details were available pending an investigation by federal and local law enforcement.  
Source: <http://www.kfmb.com/stories/story.76655.html>
- 15. *January 12, LasVegasNOW* — Northwest evacuates plane due to "suspicious" baggage.** A plane scheduled to be leaving McCarran Airport for Minneapolis was delayed from leaving Friday morning, January 12, after concern for a passenger's baggage caused an evacuation.

Northwest Airlines released the following statement: "Northwest Airlines flight 778, a Boeing 757 aircraft from Las Vegas to Minneapolis/St. Paul with 179 passengers, experienced a delay today after concern was raised regarding a passenger's carry-on baggage while the aircraft was parked at the gate. Northwest is cooperating with the appropriate government agencies. As a precautionary measure, passengers have been asked to deplane while the situation is reviewed. Northwest apologizes to its customers for the inconvenience."

Source: [http://www.klas-tv.com/Global/story.asp?S=5931557&nav=menu10\\_2\\_2](http://www.klas-tv.com/Global/story.asp?S=5931557&nav=menu10_2_2)

**16. *January 12, Reuters* — Northwest Airlines files reorganization plan.** Northwest Airlines Corp. filed a plan to exit bankruptcy as an independent company on Friday, January 12, aiming to give fresh stock to some creditors and raise capital from investors, including private equity firms. The plan, which will be fleshed out in a more detailed filing next month, moves the U.S. No. 5 airline a step closer to exiting bankruptcy, and adds urgency to any rival airlines considering a bid for the company, as consolidation fever grips the sector. Northwest has been in talks with bankrupt Delta Air Lines about a possible link-up after exiting Chapter 11, according to one source familiar with the talks. Delta itself is the target of a \$10.5 billion bid by US Airways Group Inc. Northwest filed its plan in a federal New York bankruptcy court ahead of its January 16 deadline to do so without interference from outside parties.

Source: [http://biz.yahoo.com/rb/070112/northwest\\_plan.html?.v=2](http://biz.yahoo.com/rb/070112/northwest_plan.html?.v=2)

**17. *January 12, Department of Transportation* — New air traffic control tower will lead to expansion of Sky Harbor.** Phoenix Sky Harbor International Airport is equipped for continued expansion and will be able to handle expected growth in air traffic thanks to the opening of the new \$89 million air traffic control tower, Department of Transportation Secretary Mary E. Peters announced on Friday, January 12, after an inspection and tour of the new facility. The new tower will begin operation on January 13, and will go fully operational on January 27, replacing the existing 30-year-old facility, said Secretary Peters. The Secretary said the new tower also will give an unobstructed view of the entire airfield to air traffic controllers, unlike the current tower which is partially blocked by a parking garage. Peters also noted the new tower will have the best new technology in order to make flying in and out of Sky Harbor safer and more efficient. Traffic at the airport, which is the nation's 8th busiest, is expected to double to nearly one million take-offs and landings annually by 2025. The new digital and ground radar technology will enable Sky Harbor Airport to handle the projected growth, she said.

Source: <http://www.dot.gov/affairs/dot0707.htm>

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

## **Postal and Shipping Sector**

Nothing to report.

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

## **Agriculture Sector**

**18. *January 14, Argus Leader (SD)* — Tests turned up soybean rust spores in South Dakota.** Spores capable of causing a serious soybean disease apparently made their way to South

Dakota in 2006, after making their first appearance in 2005. Asian soybean rust first made it to the continental U.S. in 2004. Spores closely resembling the disease fungus were detected in Brookings in August and possibly Beresford in June, said Brad Ruden, an extension associate at South Dakota State University. The spores never actually caused disease in the state or any of its neighbors.

Source: <http://www.argusleader.com/apps/pbcs.dll/article?AID=/20070114/NEWS02/701140338/1001/NEWS>

19. *January 11, Nebraska Department of Agriculture* — **Nebraska announces new avian influenza surveillance program.** Greg Ibach, Director of the Nebraska Department of Agriculture (NDA), unveiled a new avian influenza surveillance program for Nebraska poultry producers Thursday, January 11. The goal of the program, entitled, "Avian Influenza: Testing Pays!" is to provide free avian influenza tests of birds to any poultry producer who requests it. The test, a simple swab, is taken by NDA staff and then submitted to the University of Nebraska Veterinary Diagnostic Center for testing. Ibach said, "It's a simple, quick way to assist in surveillance that will help protect our state's poultry industry, which accounts for \$1.35 billion a year." Birds being tested include: chickens, turkeys, pheasants, quail, guineas, ducks and geese.

Source: [http://www.agr.state.ne.us/newsrel/january2007/surveillance\\_program.htm](http://www.agr.state.ne.us/newsrel/january2007/surveillance_program.htm)

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

## **Food Sector**

20. *January 12, U.S. Food and Drug Administration* — **FDA and states closer to identifying source of E. coli contamination associated with illnesses at Taco John's Restaurant.** The U.S. Food and Drug Administration (FDA) Friday, January 12, announced that it has moved closer to identifying the source of illness for the Taco John Restaurant E. coli outbreak. FDA and the state of California, working in conjunction with state health officials in Minnesota, Iowa, and Wisconsin, have DNA-matched the strain of E. coli O157:H7 bacteria associated with the outbreak with two environmental samples gathered from dairy farms near a lettuce growing area in California's Central Valley. The investigation is ongoing, including obtaining additional samples, to determine if and how material from the dairy farms may have contaminated the lettuce growing area. The outbreak sickened approximately 81 individuals in November and December of 2006. Illnesses were reported in Minnesota (33), Iowa (47), and Wisconsin (1). Twenty-six people were hospitalized, and two suffered hemolytic uremic syndrome, a serious complication of E. coli O157:H7 infection that can cause permanent kidney damage and death. No deaths have been associated with the outbreak. No new cases of illness are being reported and the outbreak is now considered over.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01546.html>

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

## **Water Sector**

21.

*January 14, KOTV (OK)* — **Ice storms leads to water rationing.** Oklahoma's icy weather is affecting the water supply in Delaware County and Hughes County. In Delaware county residents are being asked to conserve water. Both have lost power, with no electricity the pumps cannot refill the water tower. Mandatory water rationing has been ordered in Hughes County.

Source: <http://www.kotv.com/news/local/story/?id=118124>

22. *January 11, Philadelphia Inquirer* — **Chemical in school water draws alarm.** Drinking water at a South New Jersey elementary school has been found to be tainted with a chemical that the Environmental Protection Agency has labeled a likely carcinogen, a union and environmental groups announced Wednesday, January 10. In November, water samples were taken at several sites near the Chambers Works plant run by DuPont Co. near the Delaware Memorial Bridge, said a spokesperson for the United Steelworkers, which represents many DuPont workers. One of the water samples was taken from a boys' restroom at Paul W. Carleton Elementary School in Penns Grove, five blocks from the Salem County plant. According to the Steelworkers union, the tests revealed high levels of PFOA (perfluorooctanoic acid) in some area drinking water. PFOA is a chemical used to manufacture Teflon nonstick cookware, Gore-Tex fabrics, and Stainmaster carpeting. It is also used to create nonstick coatings on pizza boxes and microwave popcorn bags. It does not remain in the finished product. Scientists hired by the union found a level of combined PFOA and PFCs (perfluorinated chemicals) totaling 0.112 parts per billion in the school's water and 0.18 parts per billion of PFOA in a Penns Grove water-supply well.
- Source: [http://www.philly.com/mld/inquirer/news/local/states/new\\_jer sey/16432859.htm](http://www.philly.com/mld/inquirer/news/local/states/new_jer sey/16432859.htm)

[[Return to top](#)]

## **Public Health Sector**

23. *January 14, Deutsche Presse-Agentur* — **Bird flu making reappearance in Asia, claims 61st Indonesian.** Two Indonesian women died from the avian flu late Friday, January 12, and early Saturday, January 13, bringing the total number of deaths from the disease in the country to 61, health official said on Saturday. Yulfa, 27, a Tangerang resident died late Friday and Jakarta resident Ani Apriani, 22, died early Saturday, after they had undergone two and three days of treatment in Jakarta's Persahabatan Hospital. "Their deaths have been confirmed from bird flu," Runizar Ruesin, an official at the Indonesian Health Ministry's bird flu information center said. The deaths followed that of a 37-year-old Indonesian woman who died from bird flu early on Friday.
- Source: <http://www.bangkokpost.com/topstories.php?id=115969>

24. *January 14, Financial Times* — **Europe warned over resurgence of bird flu.** The H5N1 strain of avian influenza is making a seasonal resurgence in Asia and could easily spread to Europe again this year, the World Health Organization (WHO) warned on Sunday, January 14. "We are convinced that we're in a repeat of last year and the year before when the virus began to get very active again [in the northern hemisphere winter] and spread from Asia into the Middle East and beyond," said Peter Cordingley, the WHO spokesperson for the western Pacific region. "Most countries are becoming better prepared and the countries that were caught out last year, especially wealthier ones in Europe and close to Europe, we hope are going to be better prepared," he said. "But we're still losing more than we're winning." The strain detected

in Asia is a mutation of last year's but "it is not showing any sign of moving to a strain that would be more dangerous to humans or have a greater likelihood of human-to-human transmission," Cordingley said.

Source: <http://www.ft.com/cms/s/e9f79c66-a3f9-11db-bec4-0000779e2340.html>

**25. *January 12, Associated Press* — New outbreak of bird flu hits Nigeria.** A new outbreak of H5N1 bird flu has hit Nigeria, and one new state has reported its first cases in birds after months without any known infections in Africa's most-populous nation, officials said Friday, January 12. Sokoto state in Nigeria's far north had its first cases along with a nearby state that reported re-infection. The last known infection was in September.

Source: <http://www.chron.com disp/story.mpl/ap/world/4466357.html>

**26. *January 11, Associated Press* — Arizona valley fever cases soared in 2006.** Cases of the fungal infection known as valley fever soared by 56 percent in 2006, with a record 5,493 cases diagnosed in Arizona, state health officials said. The rapid increase in cases prompted health officials to label the disease at epidemic proportions, and they noted that thousands of other cases likely went unreported. The number of deaths in 2006 weren't immediately available, but 28 state residents died of valley fever in 2005. Valley fever, or coccidioidomycosis, is a relatively obscure disease caused by inhaling the spores of a fungus found in the U.S. Southwest, northwestern Mexico and California's Central Valley. An estimated 130,000 people are exposed each year, but fewer than half develop symptoms that lead to diagnosis and only about 10 percent require treatment.

Valley fever information: <http://www.cdc.gov/ncidod/dbmd/diseaseinfo/coccidioidomycosis.htm>

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/11/AR2007011101464.html>

**27. *January 11, U.S. Food and Drug Administration* — FDA proposes barring certain cattle material from medical products.** The U.S. Food and Drug Administration (FDA) is proposing to limit the materials used in some medical products in order to keep them free of the agent thought to cause mad cow disease, also known as bovine spongiform encephalopathy (BSE). This is the latest in a series of BSE safeguards that would bar material that has been found to harbor the highest concentrations of this fatal agent in infected cattle. These materials would be prohibited from use as ingredients in medical products or elements of product manufacturing. The proposed rule would cover drugs (prescription, over-the-counter, and homeopathic), biologics (such as vaccines) and medical devices intended for use in humans as well as drugs intended for use in ruminant animals like cattle and sheep. Cattle can get mad cow disease, while sheep can get a similar disease known as scrapie. The cattle materials prohibited in the proposed rule are those that pose the highest risk of containing infectious material and include: the brain, skull, eyes and spinal cords from cattle 30 months and older; the tonsils and a portion of the small intestines from all cattle regardless of their age or health; any material from "downer" cattle; any material from cattle not inspected and passed for human consumption.

Source: <http://www.fda.gov/bbs/topics/NEWS/2007/NEW01545.html>

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

## **Government Sector**

28. *January 12, Reuters* — **White powder found in Pennsylvania courthouse.** A suspicious white powder was found in a county courthouse in Allentown, PA, on Friday, January 12, a local sheriff said. The Lehigh County Courthouse was not evacuated and there were no injuries reported, Lehigh County Sheriff Ronald Rossi said. Rossi said a letter had arrived in the courthouse mailroom on Friday morning and an assistant had found white powder inside the envelope. "That is what started this whole thing," Rossi said. "They don't know if this is the real thing. They have to test the powder."

Source: [http://today.reuters.com/news/articleinvesting.aspx?type=bondsNews&storyID=2007-01-12T152218Z\\_01\\_N12210344\\_RTRIDST\\_0\\_SECURITY-PENNSYLVANIA.XML](http://today.reuters.com/news/articleinvesting.aspx?type=bondsNews&storyID=2007-01-12T152218Z_01_N12210344_RTRIDST_0_SECURITY-PENNSYLVANIA.XML)

[[Return to top](#)]

## **Emergency Services Sector**

29. *January 14, Honolulu Star Bulletin* — **Disaster plans show a shortage of sirens.** Schools, parks, harbors, shopping centers, and beaches are among more than 100 places in Hawaii where additional emergency sirens are needed to properly warn residents and visitors about natural disasters such as tsunamis, according to state disaster plans. In all, 148 extra sirens are required to cover "gap areas," a list prepared by the state Civil Defense agency shows. Several factors have led to the shortage of sirens, which were first instituted after a 1946 tsunami caused widespread destruction in Hawaii, killing 159 people in Hilo and Laupahoehoe on the Big Island. For one, officials said the state has not been able to keep up with housing developments. Also, in recent years, only about \$1 million has been appropriated annually for new sirens, but that ends up cut in half as \$500,000 is spent every year to maintain the network, state Civil Defense officials said in October. Finally, the sirens, which have high-tech speakers and cost as much as \$75,000 each, are sometimes vandalized, said Ray Lovell, a spokesperson with the agency.

Source: <http://starbulletin.com/2007/01/14/news/story02.html>

30. *January 13, Battle Creek Enquirer (MI)* — **One-of-a-kind truck is fully equipped to be a first responder.** An antiterrorist unit at Fort Custer in Georgia now has the first and only response truck of its kind in the world. The truck is designed as the first vehicle on the scene of any incident involving chemical, biological, radiological, or nuclear terrorism. Captain Bryan Kirby, operations officer of the 51st WMD Civil Support Team, said the sensors in the truck can detect and provide information on health and safety threats at the scene. Computers on board include digital mapping, wireless Internet accessibility and the ability to provide information about hazardous substances. The truck is equipped with a night-vision system that enables the driver to see in the dark and is installed with radios to communicate with first responders from other agencies. Kirby said the truck hasn't yet been shown to emergency services directors or first responders in the area, other than the Michigan State Police, but was taken to the funeral of President Gerald Ford in Grand Rapids to detect for any foreign hazardous agents and provide decontamination and emergency medical assistance if necessary.

Source: <http://www.battlecreekenquirer.com/apps/pbcs.dll/article?AID=/20070113/NEWS01/701130315/1002>

31. *January 12, Government Technology* — **Homeland funds provide mobile computers to Kentucky first responders.** Kentucky Governor Ernie Fletcher presented a homeland security check Friday, January 12, to provide mobile data computers to area first responders. The Georgetown homeland security project will provide for more than 50 computers to be installed in local response vehicles. Mobile data computers are a rapidly emerging technology tool for first responders. They enable responders to quickly send and receive critical and timely reports and provide an added means of communication.  
Source: [http://www.govtech.net/magazine/channel\\_story.php/103301](http://www.govtech.net/magazine/channel_story.php/103301)

[[Return to top](#)]

## **Information Technology and Telecommunications Sector**

32. *January 12, Agence France–Presse* — **A time–tested solution for Asia's damaged Internet cables.** Workers are relying on 19th century technology to fix a very 21st century problem — disruption of the Internet traffic that tech–savvy Asia relies on. Crewmen on boats south of Taiwan are dragging the seabed with grappling hooks at the end of long ropes to recover fiber optic cables damaged in a 7.1–magnitude earthquake that struck the region on December 26. "No electronics involved," said John Walters, general manager of Global Marine, one of the firms engaged in the repairs. "It's an old and traditional technique." Millions of people across the region, in Taiwan, China, Hong Kong, Japan, Singapore, South Korea and as far away as Australia, suffered Internet and telephone blackouts when the cables, linking Asian countries with the U.S. and beyond, were damaged. Telecom operators have diverted the traffic to allow service to return to normal but the repair work continues. "At this point none of those cables have been repaired," Walters told AFP in an interview.  
Source: [http://news.yahoo.com/s/afp/20070112/tc\\_afp/asiaquakeinterne\\_t](http://news.yahoo.com/s/afp/20070112/tc_afp/asiaquakeinterne_t)
33. *January 12, VNUNet* — **Cyber–crooks switch to code obfuscation.** Security firm Finjan has reported that dynamic code obfuscation was increasingly used as a method to bypass traditional signature–based security systems and propagate malware during the fourth quarter of 2006. The technique works by providing each visitor to a malicious site with a different instance of obfuscated malicious code, based on random functions and parameter name changes. A conventional signature–based security solution would theoretically need millions of signatures to detect and block this particular piece of malicious code. "Hackers have begun to take advantage of new Web technologies to create complex and blended attacks," said Yuval Ben–Itzhak, chief technology officer at Finjan. "With the creation of dynamic obfuscation utilities, which enable virtually anyone to obfuscate code in an automated manner, they have dramatically escalated the threat to Web security."  
Report (registration required): <http://www.finjan.com/content.aspx?id=827>  
Source: <http://www.vnunet.com/vnunet/news/2172438/cyber–crooks–switc h–code>
34. *January 12, VNUNet* — **New Java exploits brewing.** Attackers have released exploit code targeting two previously patched flaws in Sun Microsystems' Java Runtime Environment (JRE) and Java Software Development Kit (SDK). The flaws could allow an attacker to remotely execute code on a Windows, Linux or Solaris system. Sun issued patches for both vulnerabilities in December. The JRE component allows JavaScript code to be executed on most operating systems, including Windows, Mac OS, Linux and Unix. The vulnerabilities

affect JRE 1.3.x, 1.4.x and 1.5.x, as well as versions 1.3.x and 1.4.x of the SDK and versions 1.5.x of the Java Development Kit.

Source: <http://www.vnunet.com/vnunet/news/2172403/java-exploits-brewing>

35. *January 12, Tech Web* — **Telecom carriers face declining revenue growth in core businesses.** As telecom carriers strive to become full-service providers delivering mobile broadband and Internet-related services, it's likely they will experience a rapid decline in revenue growth, a market research firm says. Year-over-year growth of total revenue from telecom services will shrink to just 1.7 percent in 2010, with actual revenues increasing to \$1.5 trillion in 2010 from \$1.3 trillion in 2006, Gartner said Thursday, January 11. As a result, carriers will spend more on new markets, such as media and information technology, to compensate for revenue losses in traditional telecom services.

Source: <http://www.techweb.com/showArticle.jhtml;jsessionid=MQ5MFFGI4PS3AQSNDLRCKHSCJUNN2JVN?articleId=196900481>

36. *January 11, eWeek* — **Exploit released for critical PC hijack flaw.** A fully working exploit for a high-risk vulnerability fixed by Microsoft two days ago has been put into limited release, prompting new "patch now" warnings from computer security experts. The exploit, which allows PC takeover attacks on Windows XP SP2, has been published to Immunity's partners program, which offers up-to-the minute information on new vulnerabilities and exploits to intrusion detection companies and larger penetrating testing firms. The company's exploit takes aim at a "critical" bug in the way Vector Markup Language is implemented in Windows. It has been successfully tested on Windows XP SP2 and Windows 2000, with default installations of Internet Explorer 6.0. "This is a fully working exploit, [it] will give you full access to do anything on the target machine," says Immunity researcher Kostya Kortchinsky. The exploit was created and confirmed in less than three hours after Microsoft's Patch Tuesday release on January 9, a fact that clearly illustrates just how much the gap has narrowed between patch release and full deployment on enterprise networks.

Source: <http://www.eweek.com/article2/0,1895,2082416,00.asp>

### Internet Alert Dashboard

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

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

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

37. *January 14, Contra Costa Times (CA)* — **More bottle explosives in Pleasanton.** Someone exploded two plastic liter bottles Saturday afternoon, January 13, possibly with a chemical

reaction, bringing to four the number of such incidents in recent weeks, according to Pleasanton, CA, police. The two explosions on Saturday occurred about two minutes apart, according to police. A witness reported seeing a young man throw a bottle from a moving vehicle on Olive Drive. Remnants of that bottle and another that exploded on Desertwood Lane were seized. One of the bottles contained some kind of chemical, which hasn't yet been identified, according to police.

Source: [http://www.mercurynews.com/mld/mercurynews/news/breaking\\_news/16461305.htm](http://www.mercurynews.com/mld/mercurynews/news/breaking_news/16461305.htm)

**38. *January 12, Associated Press* — Fires strike two churches in North Carolina.** Police and sheriff's deputies rushed to check on churches early Sunday, January 14, after fires broke out at two Baptist churches and a break-in was discovered at a third. Authorities stopped short of saying the fires were arson. But the state Bureau of Investigation, along with Greenville officials and the federal Bureau of Alcohol, Tobacco, Firearms and Explosives, planned to begin an investigation later Sunday morning. "Anytime you have two fires like that in succession, it's certainly a suspicious fire," Fire Department Battalion Chief Sandy Harris said. There were no immediate reports of injuries, and authorities said they found no signs of fires at any other church in Greenville, which is about 75 miles east of Raleigh. "At this point we're still collecting evidence. However, we have all these churches set on fire minutes apart from each other, so you can take that for what it is worth," police Cpl. Kip Gaskins said.

Source: [http://hosted.ap.org/dynamic/stories/C/CHURCH\\_FIRES?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/C/CHURCH_FIRES?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT)

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

## **General Sector**

Nothing to report.

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

### **DHS Daily Open Source Infrastructure Report Contact Information**

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

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

#### **DHS Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions:

Send mail to [dhsdailyadmin@mail.dhs.gov](mailto:dhsdailyadmin@mail.dhs.gov) or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to [dhsdailyadmin@mail.dhs.gov](mailto:dhsdailyadmin@mail.dhs.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.