



Homeland Security

Daily Open Source Infrastructure Report for 9 December 2009

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

For information, click here:
<http://www.dhs.gov>

Top Stories

- WGN 9 Chicago reports that one person is dead and one is hurt after an explosion Monday at the NDK America plant in Belvidere, Illinois, which manufactures crystals used in liquid-crystal displays. (See item [9](#))
- According to U.S. News and World Report, TSA officials say that a “full review” is underway to determine how a 2008 copy of its standard operating procedures for all airport security checkpoints was released in its entirety on the Internet. The document was “improperly redacted,” TSA officials say. (See item [15](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)

SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)
- [National Monuments and Icons](#)

Energy Sector

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

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

1. *December 8, Dothan Eagle* – (Alabama) **Property stolen from power substation in Geneva.** Geneva County Sheriff’s deputies are looking for information in the theft of more than \$12,000 worth of property from a fenced area at an Alabama Power substation. The chief deputy said the property was stolen between December 3 and the early morning hours on December 7 after someone broke the lock on a fenced-in area at

a power substation on Alabama Highway 87 about a mile and a half from the Florida state line. He said a John Deere Gator worth about \$10,000, a 14-foot trailer worth about \$1,500, about \$500 worth of copper wire, a generator, a gas powered drill, and a climbing belt were all taken.

Source:

http://www2.dothanagle.com/dea/news/crime_courts/article/property_stolen_from_power_substation_in_geneva/114158/

2. *December 8, Kentucky Post* – (Kentucky) **Power restored after 15,000 lose power.** Over 15,000 Duke Energy customers in Northern Kentucky have power after losing it for a period of time Monday night. A spokesperson for Duke Energy says the problem originated at a substation in Covington. Electricity was rerouted to different substations and that caused the periodic outages. The problems started around 7:30 p.m. on Monday night and all power was restored by 11:55 p.m. The company is still investigating what caused the problem. There were power outages in Hamilton County as well Monday night, however, the spokesperson says those were not related to the Northern Kentucky issue. The Hamilton County issues were related to a car accident. Source: http://www.kypost.com/content/wcposhared/story/Power-Restored-After-15-000-Lose-Power/sIHM1qlUAkSZO4rP2e0t_g.csp
3. *December 8, Associated Press* – (New Hampshire) **NH emergency officials hold session on ice storm.** New Hampshire officials are reviewing the state's response to the December 2008 ice storm, which left thousands without power for days. Emergency officials and utility regulators will hold a joint session on Tuesday. Homeland Security and Emergency Management and the Public Utilities Commission have done extensive reviews of the event and made changes in operating plans. The utilities also have made changes following the storm. The session starts at 11 a.m. at the state Incident Planning and Operations Center in Concord. Source: <http://wbztv.com/wireapnewsnh/Emergency.officials.regulators.2.1356283.html>
4. *December 7, Associated Press* – (California) **Police arrest 29 during protest outside of Chevron.** Police say 29 people were arrested during a protest outside the headquarters of Chevron Corporation in San Ramon. Police say the protesters were taken into custody after they blocked streets and refused to disperse outside the oil giant's headquarters around 7 a.m. on December 7. Most of those arrested were cited and released. The protest was organized by the group Mobilization for Climate Justice West. The protest coincided with the first day of the United Nations climate change conference in Copenhagen, Denmark. Source: <http://www.mymotherlode.com/news/state/ap/694790/Police-arrest-29-during-protest-outside-of-Chevron.html>
5. *December 7, Pennsylvania Department of Environmental Protection* – (Pennsylvania) **DEP fines Chesapeake Appalachia LLC, Schlumberger Technology Corp. for hydrochloric acid spill in Bradford County.** The Department of Environmental Protection (DEP) has fined Chesapeake Appalachia LLC and Schlumberger

Technology Corp. \$15,557 each for a 295-gallon hydrochloric acid spill at Chesapeake's Chancellor well site in Asylum Township, Bradford County. Chesapeake staff notified DEP on February 9 that a 21,000-gallon tank containing 36 percent hydrochloric acid was leaking. The acid was used for hydraulic fracturing. When a DEP inspector arrived at the site, it was determined that the tank had two leaks and was losing about 7.5 gallons per hour of hydrochloric acid. Chesapeake's emergency contractor arrived that evening and removed free-standing acid from the ground with absorbent pads; excavated trenches to contain the acid; neutralized acid-contaminated soil with soda ash and hydrated lime; and transferred about 11,000 gallons of acid from the leaking tank to two temporary tanks. About 126 tons of contaminated soil had to be excavated, and more than 13,800 gallons of a hydrochloric acid and water mixture were removed from the well site. Chesapeake Appalachia LLC is a natural gas exploration company located in Charleston, W. Va., and Schlumberger Technology Corp. is a natural gas service company based in Sugar Land, Texas.

Source:

<http://www.ahs2.dep.state.pa.us/newsreleases/default.asp?ID=5758&varQueryType=Detail>

For another story, see item [19](#)

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

Chemical Industry Sector

6. *December 7, Opelousas Daily World* – (Louisiana) **Tanker truck overturns on I-49 on-ramp.** The northbound Interstate 49 on-ramp at U.S. Route 190 will remain closed overnight following a one-vehicle accident that occurred around 4:30 p.m. Monday and left an 18-wheeler carrying sodium hydroxide lying on its side. Sodium hydroxide is a chemical present in cleaning products, which in high concentrations, can cause burns on the skin. The Louisiana State Police Hazmat team found that the truck had not been compromised, said a state trooper. "However, a small amount of the product did leak from the valves. Currently, the U.S. Environmental Services out of Baton Rouge are responding to the scene to offload the product from the trailer," the trooper said. The recovery of the chemical is expected to continue through the night, the trooper added. The driver was transported to a local hospital with minor injuries. The tanker truck continues to lie on its side, blocking the ramp. The intersection remains closed at this time and the hazmat team has been dispatched to the scene.

Source:

<http://www.dailyworld.com/article/20091207/NEWS01/91207001/1002/Tanker-truck-overturns-on-I-49-on-ramp>

For another story, see item [5](#)

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

Nuclear Reactors, Materials and Waste Sector

7. *December 8, Reuters* – (Georgia) **Southern Ga. Vogtle 1 reactor shut.** Southern Co’s 1,152-megawatt Unit 1 at the Vogtle nuclear power station in Burke County, Georgia shut from full power on December 7, a spokeswoman for the company said Tuesday. An equipment issue resulted in the loss of condenser vacuum on the non-nuclear turbine side of the plant resulting in an automatic shutdown, she said. She could not say when the unit would return to service, noting a team was putting together a return to service plan. Electricity traders guessed it would be back within a few days. In a report to the U.S. Nuclear Regulatory Commission, the company said the equipment problem was likely a switchgear problem. All systems responded as expected to shut the unit. Source: <http://www.reuters.com/article/idUSN0819085120091208?type=marketsNews>

8. *December 7, Boston Herald* – (New Hampshire) **Seabrook nuclear plant shut down for repair.** The owner of the Seabrook nuclear power plant in coastal New Hampshire has shut down its reactor to replace a low-pressure turbine rotor that had a vibration. Operators detected and monitored the rotor vibrations since the plant returned from a refueling outage November 10, a plant spokesman told Bloomberg News in a telephone interview. He declined to say how long the outage would last, citing company policy. The plant was running at about 65 percent of capacity prior to the shutdown, the spokesman said. Workers will replace the low-pressure turbine that is experiencing vibrations with another one on site, a spokesman for the U.S. Nuclear Regulatory Commission said in an e-mail to Bloomberg News. “Because of the high rate of speed at which the blades spin, any imbalance, or vibrations, must be fixed to prevent damage to the turbines,” he said. Source: http://news.bostonherald.com/business/general/view/20091207seabrook_nuclear_plant_shut_down_for_repair/srvc=home&position=recent

For another story, see item [22](#)

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

Critical Manufacturing Sector

9. *December 7, WGN 9 Chicago* – (Illinois) **1 dead, 1 hurt after blast at Belvidere plant.** A Belvidere factory designed to break apart during an explosion did just that Monday afternoon, but debris from the still unexplained blast killed a truck driver in the parking lot of a nearby Tollway Oasis. Investigators are still trying to discover what caused the explosion at the NDK America plant, 701 Crystal Parkway, which manufactures crystals used in liquid-crystal displays. They are also exploring whether other parts of the building could pose a danger. The Belvidere Fire Chief said the blast happened about 2:30 p.m., apparently in a highly pressurized vessel where crystals are made. He said the six-story factory, which has been there for about five years, was built with special exterior panels that are meant to break away during an explosion. One employee who was inside the building was unhurt by the blast, he said. But he said a piece of one of the exterior panels, several feet long, flew through the air before striking a man standing outside his vehicle on the north side of the Interstate 90

Tollway Belvidere Oasis. The distance appeared to be less than a quarter mile. The debris field left from the explosion spanned several hundred feet, he said. Some who lived near the factory said the blast felt like an earthquake.

Source: <http://www.chicagobreakingnews.com/2009/12/belvidere-ndk-crystal-parkway-explosion.html>

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

Defense Industrial Base Sector

See item [9](#)

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

Banking and Finance Sector

10. *December 7, Washington Post* – (National) **La. firm sues Capital One after losing thousands in online bank fraud.** An electronics testing firm in Louisiana is suing its bank, Capital One, alleging that the financial institution was negligent when it failed to stop hackers from transferring nearly \$100,000 out of its account earlier this year. In August, Security Fix wrote about the plight of Baton Rouge-based JM Test Systems, an electronics testing firm that in February lost more than \$97,000 from two separate unauthorized bank transfers a week apart. According to JM Test, Capital One has denied any responsibility for the losses. On December 4, JM Test filed suit in a Louisiana district court, alleging breach of contract and negligence by the bank. The firm says it is still out a total of \$89,000, and that it has spent roughly \$70,000 investigating and responding to the breaches. The lawsuit is the latest to challenge whether banks are doing enough to help customers prevent losses when a virus infection, phishing attack or hacker break-in jeopardizes a company's online banking credentials, said a digital media lawyer with the Los Angeles law firm Jeffer Mangels Butler & Marmaro LLP. He said that under the Uniform Commercial Code, banks generally are required to maintain "commercially reasonable" methods of providing security against unauthorized payment orders." But he said just what constitutes "commercially reasonable" security practices has only recently been challenged, citing a recent court case in Illinois expected to go to trial soon in which a couple is suing their bank over \$26,500 lost when cyber thieves stole the user name and password needed to access their home equity line of credit.

Source: <http://voices.washingtonpost.com/securityfix/2009/12/jmtest.html>

11. *December 7, Bank Info Security* – (National) **Phishing scam spreads to three more states.** Banking customers in three additional states have received bogus text messages purporting to be from their institutions. As part a growing wave of similar phishing attempts throughout the nation, customers in Cincinnati, Ohio, St. Louis, Missouri and Lewiston, Idaho last week reported receiving text messages stating their bank accounts had been frozen. These attacks mirror those against bank customers in October in Pennsylvania, Nebraska and New York, and are part of a continuing wave of phishing

attacks that have shot up 600 percent over last year, according to the Anti-Phishing Working Group. In Ohio, one Cincinnati US Bank customer told law enforcement about receiving the text message, calling the phone number listed and then giving out an account number, expiration date and PIN. The next day, the customer became suspicious and called the number again and heard the following message: “This is a message from the Federal Trade Commission. The telephone number you have just called has been disconnected because it may be involved in a scam.” The customer called US Bank, had the card replaced and did not lose any money. Law enforcement reported a number of banks had been targeted in the scam. Similar reports come in from Bridgeton, Missouri-based Vantage Credit Union customers who reported to the credit union they received the text message phishing scam.

Source: http://www.bankinfosecurity.com/articles.php?art_id=1986

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

Transportation Sector

12. *December 8, WTLV 12 Jacksonville* – (Florida) **FAA sued again over Jacksonville air traffic control operations.** For the third time in recent years, the Federal Aviation Administration (FAA) has come under fire for the operations of its air traffic control tower at Jacksonville International Airport (JIA). On November 17, the daughters of a couple killed in a plane crash near the Gainesville airport filed a lawsuit against the FAA; the third such lawsuit to name the Jacksonville operations tower this decade. On November 7, 2008, the couple and their pilot were killed when the small plane they flew in attempted to land in thick fog at the Gainesville airport. A man was on his way to Shands Hospital for a kidney transplant at the time. On December 12, 2001, four people were a small plane as it attempted to land at JIA in foggy conditions. Two Jacksonville attorneys and their clients from Orange Park died in the crash. Four years later, the FAA settled with the victims’ families for nearly \$10 million dollars. On December 18, 2005, a father and daughter died when their small plane crashed off the coast of Vilano Beach in stormy weather. Two other teens aboard survived. This summer, the FAA settled with another family for \$3 million. In each of the three crashes, the families of those who died say air traffic controllers did not properly do their jobs when guiding in the small planes. The lawsuit alleges the air traffic controller did not notify the pilot of inclement weather conditions, which are the same allegations in the civil lawsuits filed after the 2001 crash at JIA and the 2005 crash off Vilano Beach. In the investigations of the 2001 and 2005 crashes, the National Transportation Safety Board did not find air traffic control at fault.

Source: <http://www.firstcoastnews.com/news/local/news-article.aspx?storyid=149194&catid=3>

13. *December 8, Associated Press* – (California) **Snow, ice close stretch of I-5 as storm moves east.** State Highway 101 commuters are sharing the road with a lot of big-rigs because of the snow-and-ice shutdown of a portion of Interstate 5, the main freeway connecting Northern and Southern California. The 30-mile stretch over the Grapevine in the Tehachapi Mountains has been closed in both directions since Monday night.

Snow plows are now working to get I-5 open. The California Highway Patrol is escorting traffic over State Route 58 between Bakersfield and Mojave. It was closed because of ice, leaving Highway 101 the only route between northern and southern portions of the state. The storm has moved east, leaving Southern California with freezing temperatures Tuesday. Lower temperatures include 25 degrees in San Pedro and Acton, 30 in Palmdale, 32 in Claremont and 36 in Fullerton and Burbank.

Source:

http://www.montereyherald.com/state/ci_13951091?nclick_check=1&forced=true

14. *December 7, Helena Independent Record* – (Montana) **Airliner makes emergency landing at Helena airport.** One hundred and fifty Oregon-bound people ended up spending the night in Helena after their Continental Airlines flight developed engine trouble on a westbound flight from New Jersey, airport officials said. The assistant manager of the Helena Regional Airport said a Continental Airlines 737-800 from Newark bound for Portland landed in Helena shortly after 10 p.m., after shutting down one of the jet's two engines. Emergency vehicles were scrambled, the assistant manager of the Helena Regional Airport said, but the landing was routine. Passengers spent the night in the terminal while the airline first worked with local mechanics to determine whether the plane could be fixed, then had a replacement jet flown to Helena from Portland. The assistant manager said the flight left Helena without incident at around 6:15 a.m. Monday.

Source: http://www.helenair.com/news/local/article_5c6b0936-e34e-11de-896b-001cc4c002e0.html

15. *December 7, U.S. News and World Report* – (National) **TSA to conduct full review after leak of sensitive information.** TSA officials say that a “full review” is underway to determine how a 2008 copy of its standard operating procedures for all airport security checkpoints was released in its entirety on the Internet. The document was “improperly redacted,” according to TSA officials, meaning that with a few keystrokes what was once secret spilled out into the public domain. The document itself details screening procedures at metal detectors, explosive residue testers, and other elements of airport security. It outlines procedures for escorting certain travelers around security checkpoints, including air marshals, diplomats, and CIA officers. An annex to the document gives several examples of official credentials for agencies including the CIA, Congress, and federal air marshals and notes on determining their authenticity. Another redacted section of the document reveals that travelers are selected for screening if their passports are issued by any one of 12 specific countries. The TSA document, dated June 30, 2008, is stamped “Sensitive Security Information,” a description of sensitive but not classified information. To redact the TSA document for public release, officials apparently used a computer program to blacken particularly sensitive parts of the handbook, including which types of travelers are exempt from various kinds of random and required screening, the procedure for CIA officers escorting foreign dignitaries and others through checkpoints, the minimum gauge of wire used to calibrate X-ray machines, and the types of chemicals used for cleaning explosive residue scanners. The document was then published online as a PDF, a common file format used widely by the government. To redact it, officials obscured text using a program which

successfully obscures the text as viewed on a computer monitor. But the information was not deleted. Highlighting the text of the PDF page and then using the copy and paste functions on a computer easily revealed the hidden information.

Source: <http://www.usnews.com/articles/news/2009/12/07/tsa-to-conduct-full-review-after-leak-of-sensitive-information.html>

For more stories, see items [6](#) and [34](#)

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

Postal and Shipping Sector

Nothing to report

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

Agriculture and Food Sector

16. *December 8, Progressor Times* – (Ohio) **County firm cited for health, safety violations.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) recently cited a Wyandot County firm for safety and health violations. Endres Processing Ohio, LLC, a manufacturer of an animal feed supplement, is located in Lovell, Ohio. Its parent company is Endres Processing LLC, Rosemont, Minnesota. An OSHA regional news release states that OSHA began a health inspection of Endres in June after receiving word that fires had occurred in the Wyandot County plant and that large amounts of dust from the manufacturing process had accumulated throughout the worksite. Proposed fines for the violations total \$472,900. According to the report, health violations included a lack of explosion protection, the failure to equip process equipment with combustible dust collection systems, hazardous accumulations of dust, and the use of electrical equipment that was unsafe to use in areas with combustible dust accumulation. Other health violations included hazards from workers breathing dust, allowing combustible materials in areas where workers were welding, and unsafe electrical equipment and practices. In all the proposed health violation fines totaled \$266,900. Following a safety inspection OSHA issued safety violations for confined space hazards and failing to train employees in using the firefighting system. Other violations included fall hazards, problems with emergency exit lighting, failure to train on and exposure to hazardous machine-energy sources and additional unsafe electrical equipment and practices. The report stated that several of the violations were willful or “committed with intentional, knowing or voluntary disregard for the laws requirements, or with plain indifference to employee safety and health.” Proposed safety violation fines totaled \$206,000.

Source: <http://www.theprogressortimes.com/articles.asp?articleID=13168>

17. *December 7, Examiner* – (Texas) **Federal and State health agencies investigating Norovirus illnesses from Texas oysters.** The U.S. Food and Drug Administration (FDA) is advising consumers to avoid eating oysters harvested from the San Antonio

Bay on the Gulf of Texas on or after November 16 due to reports of norovirus-associated illnesses in some people who had consumed oysters harvested from this area. There have been about a dozen cases of norovirus-like illnesses reported in the Carolinas. These patients had eaten oysters from the San Antonio Bay. The Texas Department of State Health Services has ordered a recall of all oysters harvested from the San Antonio Bay between November 16 and November 25. The implicated oyster beds in the San Antonio Bay were closed by the Texas Department of Health Services on November 26, 2009, and remain closed. Noroviruses belong to a family of viruses that cause the “stomach flu” or gastroenteritis. Consumers who purchased oysters on or after November 16 that has a label showing they came from San Antonio Bay are advised to dispose of the oysters and not eat them. At restaurants, consumers should ask about the source of oysters offered as menu items.

Source: <http://www.examiner.com/x-7707-Infectious-Disease-Examiner~y2009m12d7-Federal-and-State-health-agencies-investigating-Norovirus-illnesses-from-Texas-oysters>

18. *December 7, WHIO 7 Dayton* – (Ohio) **911 calls released in fatal barn**

fire. Authorities in Lebanon, Ohio have released multiple 911 calls after a barn fire killed two men and 43 horses. The call described a huge fire that started sometime before 5 a.m. Saturday inside Barn 16 at the Lebanon Raceway, which is part of the Warren County Fairgrounds. The Warren County Coroner confirmed on Monday that the two victims, who worked as groomers, died of smoke inhalation. Firefighters from 10 different fire departments responded to Barn 16. The firefighters worked to keep the flames from spreading to other nearby barns. By sunrise, the damages totaled hundreds of thousands of dollars in lost equipment and horses. Warren County fairboard members are still refusing to comment on reports that the two men had been living inside the barn while working there.

Source: <http://www.whiotv.com/news/21887071/detail.html>

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

Water Sector

19. *December 6, Charleston Post and Courier* – (South Carolina) **Tests on specks in**

water prove inconclusive. In separate analyses, state environmental investigators and South Carolina Electric and Gas Co. (SCE&G) said black specks they found in well water next to the power company’s plant are not coal or coal ash. But in a letter to residents in the area, the state Department of Health and Environmental Control (DHEC) said the agency did not have the equipment to “positively identify all of the particles,” and that they need more samples to get to the bottom of the matter. Meanwhile, SCE&G said its consultant found black specks in wells belonging to two employees near the plant but that the sediment was “not consistent with coal.” Tests also showed that the well water was safe to drink. Residents said these tests do not tell them what the black materials are nor from where they are coming.

Source: <http://www.postandcourier.com/news/2009/dec/06/tests-on-specks-in-water-prove-inconclusive/>

20. *December 5, University of Wyoming News* – (Wyoming) **Modified tadpoles help detect water pollution.** Research conducted by a University of Wyoming (UW) professor and others demonstrates that genetically modified tadpoles work well for rapidly detecting water pollution. In an article published in *Environmental Science and Technology*, the scientists demonstrated that African clawed frog tadpoles “light up” in response to a pollutant, and can indicate the presence of several chemicals at the same time. The professor said the research meets a pressing need to improve technologies for rapidly detecting physiological effects of environmental pollutants. The basic principle involves creating genetic constructions that enable a green fluorescent protein to be expressed in response to the physiological stress exerted on the tadpoles by pollutants for which the genetic modification was designed. “Tadpoles are particularly useful as environmental monitors because they develop a complete immune system as well as complex heart and circulatory systems, similar to humans, but maturing over days, and not years,” he said. “In this work we combined genetically modified tadpoles with a detection system developed at UW to detect the presence of heavy metal pollution in river water in real time.” He said numerous detection methods exist for environmental heavy metal monitoring, but they are very labor intensive and time consuming. Such easy-to-use technologies combining rapidity with living organism measurements had not been developed previously.
Source: http://billingsgazette.com/news/state-and-regional/wyoming/article_aab76b9a-e220-11de-a3a4-001cc4c002e0.html

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

Public Health and Healthcare Sector

21. *December 7, MissouriNet* – (Missouri) **State digitizing medical records.** Missouri has launched an effort to implement electronic health records, a move the Department of Social Services will make the medical industry more efficient for consumers and physicians. Missouri is asking the federal government for more than \$13 million to implement a statewide system for electronic medical records. The Department of Social Services says less than 17 percent of the nation’s physicians and 9 percent of hospitals use electronic health records, which would greatly improve the medical industry. A spokesman expects the federal funding to come in January. He says advisory groups will meet bi-weekly to get the electronic system plan in place, and that things are happening quickly with this project. Health care professionals from around Missouri are participating in the Missouri Office of Health Information Technology (MO-HITECH). MO-HITECH will be part of the Department of Social Services.
Source: <http://www.missourinet.com/2009/12/07/state-digitizing-medical-records/>
22. *December 7, Associated Press* – (California) **FDA investigating reports of dangerous radiation from medical scans.** Federal health regulators are investigating reports of dangerous radiation levels at two more California hospitals, following earlier unsafe medical scans at a Los Angeles facility. The Food and Drug Administration (FDA) is probing the use of CT scans at Glendale Adventist Medical Center and Providence St. Joseph Medical Center in Burbank, California. The brain scans are used to diagnose

strokes. FDA officials told reporters Monday that they are investigating at least 10 reports of excessive radiation at Glendale Adventist and an unspecified number of problems at St. Joseph. A spokeswoman for Glendale Adventist said the problems, first disclosed last month, were related to a specialty scan that involves three different techniques. The FDA began looking into problems with CT scanning in October after patients at Cedars-Sinai Medical Center in Los Angeles reported losing hair or skin redness. The hospital last month said 260 patients were exposed to excess radiation, up from prior reports of 206. A Cedars-Sinai spokeswoman said the hospital continues to work with the FDA to identify the cause of the problems. FDA officials say it is unclear whether the dangerous exposures are being caused by human error or a problem with CT equipment. Cedars-Sinai and Glendale Adventist both use scanners from General Electric. But FDA officials said they have received reports of problems at other hospitals using different brands of scanners, including models from Toshiba.
Source: http://blog.al.com/spotnews/2009/12/fda_investigating_reports_of_d.html

23. *December 7, FDA News* – (New York) **FDA cites dental syringe maker for numerous GMP violations.** Sci-Dent received a warning letter citing it for 13 good manufacturing practice (GMP) violations and for making a variety of aspirating dental injection syringes without FDA approval or clearance. During a July inspection of the company's Hamburg, New York facility, FDA investigators found no procedures to control the design of the syringes produced since 2004. Sci-Dent changed their design but had no data or documentation to support the verification, review and approval of the change, according to the November 10 letter posted recently to the FDA website.
Source: <http://fdanews.com/newsletter/article?issueId=13245&articleId=122612>

24. *December 7, CNN* – (National) **H1N1 vaccine likely to become more widely available.** Restrictions limiting the H1N1 flu vaccine to high-risk groups could be lifted in many U.S. states now that production of the vaccine has increased, state health officials said Monday. Illinois could open up vaccinations to the general public as soon as Friday, while Oregon plans to re-evaluate the progress of its vaccination program next week, representatives of those states' public health agencies said. Arizona also wants to open its vaccine stocks, but some of its large counties need more time to make sure high-risk populations get vaccinated, said the interim Department of Health Services Director. The federal Centers for Disease Control and Prevention says 73 million doses of H1N1 vaccine are now available, up from about 42 million in mid-November. The agency has said children, pregnant women, parents of infants who cannot be vaccinated, health-care workers and people with chronic illnesses should get the first inoculations, but the director of the CDC Director told reporters last week that some states have been opening up vaccinations as the number of available doses has increased.
Source: <http://www.cnn.com/2009/HEALTH/12/07/swine.flu.vaccine/>

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

Government Facilities Sector

25. *December 8, Mid Columbia Tri-City Herald* – (Oregon) **Oregon fines depot contractor \$111,000.** The state of Oregon has fined URS, the contractor operating the incinerator at the Umatilla Chemical Depot, \$111,000. Most of the fine is for violations of the facility's hazardous waste and air contaminant discharge permits as it began to burn mustard weapons agent and the agent containers. The Umatilla Chemical Agent Disposal Facility has not incinerated any chemical weapons agent or containers for 40 days while it addresses the issue. "They are delaying operations to make sure it doesn't happen again," said an official from the Oregon Department of Environmental Quality's Chemical Demilitarization Program in Hermiston. URS's Washington Demilitarization Co. reported the problems to the state, including eight occasions when the plant exceeded its emissions limit for carbon monoxide as it began incinerating mustard agent. The plant exceeded limits for four to 33 minutes in the eight incidents between July 30 and October 26, said the protocol manager for the facility.
Source: http://www.tri-cityherald.com/kennewick_pasco_richland/story/821262.html
26. *December 7, Associated Press* – (Iowa) **Police: Man threatens to blow up courthouse.** Police said Sunday that a man who twice ran for the Cedar Rapids City Council has been arrested for allegedly threatening to blow up the Linn County Courthouse. Officers said the 43-year-old suspect told mental health staff at St. Luke's Hospital in Cedar Rapids that he was going to buy explosives in Missouri and then make national news by blowing up the courthouse. Police arrested the suspect Thursday night at his home. He is charged with two aggravated misdemeanor counts of making threats and first-degree harassment. The suspect ran for the Cedar Rapids City Council in 2005 and again this past November, when he received more than 2,000 votes. Police escorted the suspect out of a city council meeting earlier this year for allegedly using profanity.
Source: <http://www.kcci.com/news/21882866/detail.html>
27. *December 7, Washington Post* – (National) **Secret Service counts 91 breaches.** Long before a pair of gate-crashers penetrated a White House state dinner, the Secret Service had detailed for its internal use a lengthy list of security breaches dating to a Presidential Administration in the late 1970s — including significant failures in the agency's protection of the President. A summary of a secret 2003 report obtained by the Washington Post, along with descriptions of more recent incidents by federal homeland security officials, places the party crashing couple squarely in a rogues' gallery of autograph hounds, publicity seekers, unstable personalities and others identified by the Secret Service as defeating its checkpoints at least 91 times since 1980. The list of security breaches exposes significant gaps that could be exploited by would-be assassins, the document states, and erode "one of the best tools for deterring future attempts" — the aura of invulnerability around the White House. A Secret Service official confirmed the authenticity of the unclassified document, which was a 39-slide presentation, and said it had been used to train agents and officers in an effort to improve agency operations. "This document reflects a proactive attempt to evaluate our security and obviously raises the awareness of uniformed division officers and agents about their jobs," a spokesman said. "We have to be concerned about the threats to our protectees at all times, whether at the White House or away from the White

House.”

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/06/AR2009120602556.html?nav=hcmodule>

28. *December 7, Notre Dame Observer* – (Indiana) **24,000 employees affected by data breach.** Important personal information, such as social security numbers, names and zip codes, of many Notre Dame employees was exposed to the Internet after the University accidentally placed the information in a publicly accessible location. The data breach affected about 24,000 employees, including some students who work for the University, said the associate vice president of information technology and the University’s chief information officer. The personal information that was exposed will no longer be accessible because the University immediately removed it from the Internet and secured it, he said.

Source: <http://www.ndsmcobserver.com/news/24-000-employees-affected-by-data-breach-1.979963>

29. *December 6, Oregon Statesman Journal* – (Oregon) **State launches inquiry into records breach.** A state inquiry is under way to determine whether two state agencies broke Oregon law by dumping records with people’s names and Social Security numbers into an open recycling bin. Regulators with the Oregon Department of Consumer and Business Services are checking for violations of the Oregon Consumer Identity Theft Protection Act, officials said. The inquiry follows last Sunday’s story in the Statesman Journal, which described mishandling of confidential records by Oregon Housing and Consumer Services and state Parks and Recreation. “We are looking at both agencies,” said a spokeswoman for the Department of Consumer and Business Services. The Oregon Legislature in 2007 passed the Oregon Consumer Identity Theft Protection Act to safeguard records with personal information. The law requires businesses and government agencies to maintain “reasonable” security for the personal information of employees, clients and customers. Failure to do so can result in fines. However, enforcement action is rare; only one fine has been levied.

Source:

<http://www.statesmanjournal.com/article/20091206/NEWS/912060344/1001/news>

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

Emergency Services Sector

30. *December 8, WJZ 13 Baltimore* – (Maryland) **3 firehouses set to close under new proposal.** It is a plan few people like, but the City of Baltimore says it is necessary. Three firehouses will close at the start of the new year. Like other major cities across the country, the fire chief is recommending these closures in order to save money during this budget crisis. Engine 14 in Carrollton Ridge will be used for storage. Truck 15 will be occupied by Engine 31 until its own building renovation wraps up in July. Truck 16 will only be reduced to an engine and a medic unit. Neighbors are worried about what this means for service. The chief says the areas surrounding the three spots will still have great coverage. “In outer edges of the city, we don’t have that

redundancy of fire trucks nearby. The primary reason we selected companies toward the center of the city is because other fire trucks can cover their area quicker,” the fire chief said. “Public safety is the number one priority of this administration and we want to ensure it to the best of our ability facing these economic times and the way we did that best, first and foremost, is no layoffs,” said a representative with the mayor’s office. The 60 to 65 firefighters who work in these three stations will be relocated.
Source: <http://wjz.com/local/fire.houses.close.2.1355350.html>

31. *December 8, Springfield News-Leader* – (Missouri) **Phone emergency system tested today.** The city of Branson will test the new CodeRED high-speed telephone emergency notification system between 7 and 8 p.m. today, according to a news release from the city. The system was installed to better inform Branson residents and businesses of emergencies. The message will inform citizens and businesses that the notification is just a test by the police and fire departments. A follow-up test message is planned for Thursday. CodeRED system could be used to include tornado or flood warnings; utility outages, evacuations, missing persons, hostage situations; chemical or sewage spills and other emergency incidents where rapid accurate notification is essential for life safety. Residents and businesses in the city limits with a land line and a listed number are automatically in the system. Those who have changed their number within the last year or use a cell as their primary home phone must go to www.bransonmo.gov, and click on the CodeRED link where they can register. Also, if citizens want to be notified through text messages or e-mails, they must sign up on the city Web site.
Source: <http://www.news-leader.com/article/20091208/NEWS01/912080371/1007/NEWS01/Phone-emergency-system-tested-today>
32. *December 7, Associated Press* – (New Hampshire) **NH prosecutors unveil cold case Web site.** New Hampshire prosecutors are asking the public to help solve 117 unsolved murders by using a new Web site to send in tips. The Senior Assistant Attorney General will head New Hampshire’s four-member cold case unit. He said Monday investigators are reviewing cases now to determine which have the best chance of being solved. The NH Governor signed a law in July creating the unit. It is being funded by \$1.2 million in federal grants. The unit will investigate unsolved murders, suspicious deaths and missing persons cases dating back more than 40 years. The cold case unit web site is <http://www.doj.nh.gov/coldcaseunit/index.htm>
Source: <http://www.seacoastonline.com/articles/20091207-NEWS-912079985>
33. *December 7, KSL 5 Salt Lake City* – (Utah) **Hydrogen-sulfide suicide in Utah prompts notice to first responders.** A suicide in North Ogden, Utah has the state putting first responders on notice about possible hazards. North Ogden Police and North View firefighters responded to the report of a suicide on November 20. The victim had used hydrogen sulfide to kill himself — a method that has become somewhat of a trend in Japan — but it is also a potential hazard for people called to the scene. In the North Ogden case, fire officials tell KSL News the victim had posted a note warning them and others of the dangers. One police officer and several firefighters

who were at the scene were tested for possible exposure, but they were unharmed. According to the Occupational Safety and Health Administration's website, hydrogen sulfide is a colorless gas that can be extremely hazardous in higher concentrations. It gives off what many describe as a "rotten egg" or "swamp gas" odor. It can also be created by mixing some ordinary household chemicals. Several suicides involving homemade hydrogen sulfide have been reported in the United States. But in Japan, hundreds of people have committed suicide using the gas. In some cases, people in neighboring areas have also become sickened.

Source: <http://www.ksl.com/?nid=148&sid=8947952>

34. *December 7, Oregonian* – (Oregon) **Leaking fuel, oil from sunken boats at John Day Dam contained.** Two government boats are still sitting at the bottom of the Columbia River, and investigators are not certain how they got there. The U.S. Army Corps of Engineers maintenance boats and part of the dock they were tied to sank Sunday evening in high winds at the John Day Lock and Dam east of The Dalles. Though the two boats, 43- and 45-foot long, have a combined 950 gallons of diesel on board, there is little fuel or oil leaking from them, spill responders said. The boats sank Sunday evening as a winter storm with wind gusts of up to 40 miles per hour blew in from the east, kicking up waves on the Columbia River as temperatures dropped into the low 20's. "Apparently the high winds just battered the boats around and knocked down structures and split the dock in half," said a spokeswoman for the Washington Department of Ecology in Yakima. The bow of the 43-foot Sea Mule is just below the surface of the river while the 45-foot Celilo could be at a depth of 65 feet. Neither poses a navigation hazard, Corps officials said Monday. The Corps had a floating boom on site that it put out Monday morning to contain oil and fuel from the boats. The sheen from the spill is about 250 yards long and 15 yards wide, he said. There have been no signs of impacts to wildlife, state officials said, and the incident has not affected operations of the adjacent navigation lock, he said. The cleanup will continue on Tuesday, and divers will assess the state of the sunken dock and boats. Then on Wednesday, the Corps plans to bring in a recovery contractor with cranes to raise the two boats.

Source:

http://www.oregonlive.com/environment/index.ssf/2009/12/leaking_fuel_oil_from_sunken_b.html

For more stories, see items [3](#) and [42](#)

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

Information Technology Sector

35. *December 8, IDG News Services* – (International) **Social network and banking scams are on the rise, says Cisco.** What do phishing, instant messaging malware, DDoS attacks and 419 scams have in common? According to Cisco Systems, they are all has-been cybercrimes that were supplanted by slicker, more menacing forms of cybercrime over the past year. In its 2009 Annual Security Report, due to be released on December

8, Cisco says that the smart cyber-criminals are moving on. “Social media and the data-theft Trojans are the things that are really in their ascent,” said a Cisco researcher. “You can see them replacing a lot of the old-school things.” The researcher is talking about attacks such as the Koobface worm, which spreads via Facebook and Twitter.

Koobface asks victims to look at a fake YouTube video, which ultimately leads to a malicious download. Cisco estimates that Koobface has now infected more than 3 million computers, and security vendors such as Symantec expect social network attacks to be a major problem in 2010. Another sneaky attack: the Zeus password-stealing Trojan. According to Cisco, Zeus variants infected almost 4 million computers in 2009. Eastern European gangs use Zeus to hack into bank accounts. They then use their networks of money mules to wire stolen funds out of the U.S. They have been linked to about \$100 million in bank losses, some of which have been recovered, the U.S. Federal Bureau of Investigation said last month. With that kind of success, older types of attacks such as instant messaging worms and phishing are now on the decline, the Cisco researcher said.

Source:

http://www.computerworld.com/s/article/9141942/Social_network_and_banking_scams_are_on_the_rise_says_Cisco

36. *December 8, The Register* – (International) **Adware touts \$1 bribe to prospective zombies.** An adware distributor is offering to pay punters \$1 to install their software. The bribe comes attached to malware, specifically an application bundle that includes adware and agents that change browser home pages, detected by Sunbelt Software as C4DLMedia and classified as a medium risk threat. The offer of payment is buried in the application’s terms and conditions. Even if the adware slingers come through on this offer to pay via PayPal, the amount of the bribe is probably a problem. “In places where a dollar is worth enough to make this worth the effort, there probably isn’t any internet connectivity,” writes a Sunbelt security researcher.
Source: <http://www.theregister.co.uk/2009/12/08/bribeware/>

37. *December 7, The Register* – (International) **Webmasters targeted in cPanel look-alike phish.** Fraudsters are targeting webmasters in a massive phishing campaign that attempts to trick marks into giving up credentials needed to administer their sites. The emails are sent to customers of some of the world’s most widely used webhosts, including GoDaddy, Hostgator, Yahoo!, and 50Webs. Although the subject lines vary, they all purport to come from the hosting service. In all, admins from at least 90 different webhosts are being targeted. “Due to the system maintenance, we kindly ask you to take a few minutes to confirm your FTP details,” the emails state. Those who take the bait are led to a website formatted to look like a page from cPanel, the widely used website administration program. Once a website’s address and FTP credentials are entered, users are directed to their host’s login page. Over the past year, scammers have increasingly targeted administrators of legitimate websites. According to a review in the third quarter of this year by security firm Dasient, 5.8 million pages from 640,000 websites were infected with code designed to launch malware attacks on visitors. ScanSafe, a separate security firm, has been tracking a single infection known as Gumblar that has taken over at least 2,000 websites by stealing their administrator

credentials.

Source: http://www.theregister.co.uk/2009/12/07/webmaster_phishing_campaign/

38. *December 7, V3.co.uk* – (International) **Scientists promise an end to web attacks.** Research published by academics at the University of Bristol’s Department of Computer Science suggests that a new technology could render cyber attacks “computationally impossible”. The experts will present their research at the ASIACRYPT 2009 security and cryptology conference being held in Japan this week. The experts will discuss how a new technique could be applied that makes web site attacks impossible. The researchers plan to demonstrate how encryption could be used to prevent attacks such as denial of service, while also providing two-factor authentication that does not overburden users. Both hardware and software issues will be discussed. A second paper will demonstrate how to transfer information between databases in a truly encrypted way. The researchers suggested that this could be used by doctors to access centralized healthcare databases in a way that protects patient confidentiality, for example. A final paper covers what the researchers call “basic constructions in cryptography”, which could be applied to applications like the web browser.

Source: <http://www.v3.co.uk/v3/news/2254544/boffins-hacking>

39. *December 7, DarkReading* – (International) **Microsoft warns of malware-laced counterfeit software.** Citing a rising tide of complaints from people who unknowingly bought counterfeit software infected with malware, Microsoft on Thursday announced the launch of educational initiatives and enforcement actions in over 70 countries to raise awareness of counterfeit software and to protect consumers. Such complaints have doubled in the past two years, according to the company, reaching 150,000, a fairly large number considering such reports are made voluntarily by consumers. “Consumers who are duped by fraudulent software encounter viruses, lose personal information, risk having their identities stolen, and waste valuable time and money,” said a associate general counsel for Worldwide Anti-Piracy and Anti-Counterfeiting at Microsoft, in a statement. “Today’s announcement demonstrates our commitment to working with others, including our partners, government agencies and nongovernmental organizations, to protect people from the ill effects of counterfeit software.” Microsoft is calling its anti-piracy campaign Consumer Action Day. The event includes an intellectual property education program in schools across China, a club for software resellers in Germany to provide legitimate software, a course in counterfeit software risks offered by Mexico’s consumer protection agency, an online safety program for children in Greece, and a business piracy impact study in Argentina. Microsoft claims that counterfeit software is becoming more dangerous. It cites a 2006 IDC study that found 25 percent of counterfeit software attempted to install unwanted or malicious code when downloaded. More recently, German anti-piracy company Media Surveillance found that among several hundred pirated copies of Windows and hacks, 32 percent contained malicious code.

Source:

<http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=222000906>

40. *December 7, The Register* – (International) **Service cracks wireless passwords from the cloud.** A security researcher has unveiled a low-cost service for penetration testers that checks the security of wireless networks by running passwords against a 135-million-word dictionary. The WPA Cracker is a cloud-based service that accesses a 400-CPU cluster. For \$34, it can run a password against all 135 million entries in about 20 minutes. Those willing to wait 40 minutes can pay \$17 to access the system at half mode. In addition to operating in the cloud, the service is also notable because its dictionary has been set up specifically for cracking Wi-Fi Protected Access passwords. While Windows, Unix and other systems allow short passwords, WPA pass codes must contain a minimum of eight characters. Its entries use a variety of words, common phrases and “elite speak” that have been compiled with WPA networks in mind. WPA Cracker is used by capturing a wireless network’s handshake locally and then uploading it, along with the network name. The service then compares the PBKDF2, or Password-Based Key Derivation Function, against the dictionary. The approach makes sense, considering each handshake is salted using the network’s ESSID, a technique that makes rainbow tables only so useful.
- Source: http://www.theregister.co.uk/2009/12/07/cloud_based_password_cracking/

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at sos@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

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

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

Communications Sector

41. *December 8, V3.co.uk* – (International) **Satellites touted as solution to UK’s rural broadband issue.** Satellite broadband could be the answer to Britain’s digital divide, according to internet industry experts. The chief executive of Skyware Global told V3.co.uk that the government “will have to look at satellite technology as a solution to providing broadband across the country”. The installation of fiber optic cable would be too time-consuming and expensive to provide broadband in rural areas, according to the executive, and bottlenecks are appearing in the telecoms infrastructure as data rates on the network grow. “Currently there are around 865,000 satellite broadband customers worldwide, but the industry is expecting that to reach 10 to 15 million as the technology is made cheaper and demand grows,” he explained. A senior analyst with Northern Sky Research agreed, saying that in developed economies satellite broadband is helping meet the demand from users who see broadband access as a must-have service. He also agreed that satellite broadband is an excellent technology for issues of rural divide and has done very well in countries with government subsidy programs, like Australia. However, he pointed out that satellite broadband subscriber patterns mirror population densities. “Satellite broadband is very effective at filling the still substantial number of broadband white spaces that are found in and around urban and

suburban areas.” Currently there are around 1.2m satellite broadband customers worldwide, with around 900,000 subscribers in North America, and around 150,000 in Europe.

Source: <http://www.v3.co.uk/v3/news/2254591/satellite-broadband-provide>

42. *December 8, Federal Communications Commission* – (National) **FEMA, FCC announce standards for wireless carriers to receive and deliver emergency alerts via mobile devices.** As part of the Integrated Public Alert and Warning System (IPAWS), the nation’s next generation of emergency alert and warning networks, the Department of Homeland Security’s Federal Emergency Management Agency (FEMA) and the Federal Communications Commission (FCC) recently announced the adoption of the design specifications for the development of a gateway interface that will enable wireless carriers to provide its customers with timely and accurate emergency alerts and warnings via their cell phones and other mobile devices. The Commercial Mobile Alert System (CMAS) is one of many projects within IPAWS intended to provide emergency managers and the President of the United States a means to send alerts and warnings to the public. Specifically, CMAS provides Federal, state, territorial, tribal and local government officials the ability to send 90 character geographically targeted text messages to the public regarding emergency alert and warning of imminent threats to life and property, Amber alerts, and Presidential emergency messages. The CMAS is a combined effort of the federal government and cellular providers to define a common standard for cellular alerts. Today’s announcement marks the beginning of the 28-month period, mandated by the FCC in August 2008, for commercial mobile service providers who have elected to participate in the design specifications known as CMAS to develop, test and deploy the system and deliver mobile alerts to the public by 2012. “Working as a team with our partners in the public and private sectors, the adoption of the CMAS standard brings us even closer to making the nation’s next-generation of emergency alerts and warnings – Integrated Public Alert and Warning System (IPAWS) – a reality,” said FEMA’s Administrator. “Our goal is simple, to give one message over more devices to more people for maximum safety.”

Source: <http://www.rfglobalnet.com/article.mvc/FEMA-FCC-Announce-Standards-For-Wireless-0001?VNETCOOKIE=NO>

43. *December 8, Baltimore Computers Examiner* – (National) **Comcast plans on nationwide limit on monthly data usage.** Comcast is proceeding with plans to implement a plan to limit data transfers to 250Gb per month. The move will change how consumers have used the Internet and how Internet Service Providers (ISPs) provide Internet access. Comcast has been developing different plans to curb what it considers an overuse of its networks by file-sharers and downloaders of large files. ISPs or Internet service providers have been trying to implement different types of data caps for some time now.

Source: <http://www.examiner.com/x-23513-Baltimore-Computers-Examiner~y2009m12d7-Comcast-plans-on-Nationwide-limit-on-monthly-data-usage>

44. *December 7, Coated* – (National) **AT&T iPhone application to track network problems.** AT&T has developed a new application for the Apple iPhone that allows

AT&T customers to easily report mobile phone problems in a given network area. Users will be able to report such things as poor coverage, dropped calls, data errors as well as a general network outages. The software application is free to download and install through iTunes.

Source: <http://www.coated.com/att-iphone-application-to-track-network-problems-93410006/>

For more stories, see items [37](#) and [40](#)

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

Commercial Facilities Sector

45. *December 8, Athens Banner-Herald* – (Georgia) **Man threatens at Clarke skate park.** Officers took a man for a psychological evaluation Sunday afternoon after he claimed to have a bomb at Southeast Clarke Park and threw a jar that contained sodium hydroxide into the Lexington Road skate park, Athens-Clarke police said. Officers evacuated the park about 2 p.m. while they took the man into custody, and members of the fire department's hazmat unit cleaned up the chemical, also known as lye or caustic soda, police said. A relative told police the 25-year-old man had been in and out of rehabilitation centers, and he had been taking hallucinogenic drugs, according to police. A witness said the man came from woods near the park, claimed to be a terrorist, and said he had a bomb that he would set off by pushing a button, police said. Officers did not arrest the man, but they continued to investigate for a possible charge of terroristic threats and acts, police said.

Source: http://www.onlineathens.com/stories/120809/cop_533102881.shtml

46. *December 7, WFSB 3 Hartford* – (Connecticut) **Flames destroy East Hartford warehouse.** Crews from multiple towns were called to battle a massive blaze at an East Hartford warehouse Monday morning. The fire was reported at the Office Furniture Rental Alliance building on George Street before 9 a.m. The building was owned by the New Boston Fund. Firefighters from Hartford, West Hartford, New Britain, Glastonbury, South Windsor and Manchester were called to the blaze, which sent thick black smoke that could be seen for miles into the air. A person who works in the building told Eyewitness News that all of the workers were able to escape the blaze. The East Hartford Mayor's Office said that the company had about 15 employees in the building, and all escaped safely. The fire was so intense it collapsed walls and ceilings inside of the burning structure and melted signs on buildings across the street. Officials said it took the fire crews two hours to knock the fire down and crews remained to make sure the fire did not reignite. The company's office building is adjacent to the warehouse.

Source: <http://www.wfsb.com/news/21885522/detail.html>

For another story, see item [18](#)

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

National Monuments and Icons Sector

47. *December 8, Associated Press* – (Idaho; Montana; Wyoming) **Aerial survey shows pine beetle’s toll in Yellowstone.** A beetle epidemic that is killing trees across the Rocky Mountain region has taken an especially heavy toll on whitebark pine trees in the Yellowstone ecosystem, according to preliminary findings of a recent aerial survey. The six weeks of flights this summer covered 2.5 million acres of whitebark forests in 21 mountain ranges in the 22-million-acre Yellowstone ecosystem. The survey involved the National Park Service, the U.S. Forest Service and the environmental group Natural Resources Defense Council. Up to now, aerial surveys conducted by the Forest Service have focused primarily on documenting beetle damage among the lower-elevation species. “We knew the impact was huge. But we really didn’t have a good feel of the true extent,” said a retired forest service beetle expert who helped coordinate the survey. Beetles have all but wiped out some whitebark forests, including along the east side of Yellowstone National Park, researchers said. The demise of the high-elevation forests has implications that include the survival of grizzly bears and the ability of mountain ranges to hold snow and supply water for farming, ranching and municipal use.

Source: http://www.helenair.com/news/state-and-regional/article_5d8f620e-e3ca-11de-9329-001cc4c002e0.html

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

Dams Sector

48. *December 6, Sacramento Bee* – (California) **New operating manual needed for Folsom Dam upgrade.** Nearly a billion dollars for a massive new spillway and flood-control gates at Folsom Dam promises a new level of protection for the Sacramento region. The full impact of one of the nation’s most ambitious dam upgrades, however, will not be measured for some time because a rewrite of rules governing the reservoir’s flood-control operations is late getting started. Construction of the spillway is on track, an important achievement given setbacks four years ago caused by unexpectedly high bids for an earlier project design. Now, excavation is nearly complete, and the U.S. Army Corps of Engineers expects concrete to be poured in about a year. But perhaps because of the tight focus on construction, work has yet to start on a new set of rules that will dictate how the dam is managed. The spillway will be finished in 2015 and one board member of the American River Watershed Institute said the rules rewrite should have begun by now, so that all key players in the dam’s operation have time to address potential conflicts over everything from flood protection to salmon habitat. Like software that runs a computer, the rules are a framework for dam operations. Without the rules he says the dam would be like a new computer running on outdated software. Called the Folsom Dam Joint Federal Project, the \$1.5 billion job — which among other things also includes raising the dam’s height 3.5 feet — is a rare partnership between the U.S. Bureau of Reclamation, which owns the dam, and the Army Corps, which is responsible for flood protection. The agencies jointly produced the spillway design. The new spillway will include a 3,000-foot-long concrete channel,

adjacent to the existing main dam, and six giant new flood-control gates. Estimated cost: \$919 million.

Source: <http://www.sacbee.com/ourregion/story/2373443.html>

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

DHS Daily Open Source Infrastructure Report Contact Information

About the 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 Web site: <http://www.dhs.gov/iaipdailyreport>

Contact Information

Content and Suggestions:

Send mail to NICCCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

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.