Homeland Security

Daily Open Source Infrastructure Report for 13 January 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- Reuters reports that the Federal Aviation Administration has called for enhanced inspections of more than 130 older Boeing 737 planes to find possible cracks in the fuselage skin of the planes. (See item **15**)
- The Web Host Industry Review reports that a Romanian hacker has disclosed an SQL injection vulnerability on a U.S. Army Web site that could lead to a full database compromise. The Web site used to provide information about military housing facilities to soldiers, called Army Housing OneStop, was found to be storing passwords in plain text. (See item **32**)

Fast Jump Menu

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 11, WBNS 10 Columbus* – (Ohio) **AEP, scrapyards working to combat copper thefts.** Copper thefts left thousands of people without power this weekend, and American Electric Power is working to combat future thefts, and catch those responsible for the latest blackout, 10TV reported on January 11. The signs were dark

on January 9 in the Mill Run area as businesses dealt with a power outage for hours. AEP officials believe the power outage may have been caused by a copper theft at one of their substations. Customers were left in the cold and businesses lost power and money. Copper thieves sometimes try to sell the stolen copper, 10TV reported. Employees at PSC Metals said there is information they obtain to help identify potential thieves. "We have to take their ID and swipe it through a computer to make sure all the information is current, we have to get a thumb print of the individual," said a PSC employee. The scrapyard is now working closely with police to identify those people who may be attempting to sell copper and other items obtained illegally. Each incident costs AEP about $25,000 and a spokeswoman said the company is in the process of replacing materials and improving security. AEP said cars parked at the substation should have an AEP logo and anyone seen at the substations should have AEP clothing on. AEP is offering a $5,000 reward for information that could help catch the thieves.
Source: http://www.10tv.com/live/content/local/stories/2010/01/11/story-columbus-copper-thefts.html?sid=102

2. *January 11, Associated Press* – (Wyoming) **DEQ cites Sinclair for spill.** The Wyoming Department of Environmental Quality (DEQ) has cited Sinclair Refinery for a spill that released nearly 3 million gallons of potentially explosive fluid last spring. Sinclair failed to take steps to prevent the May 3 spill — one of the biggest in Wyoming history — by fixing leakage at the tank where the spill originated, the department said in the December 30 violation notice. Meanwhile, a top regulator expressed continuing frustration Monday that Salt Lake City-based Sinclair has not given state inspectors access to the inside of the tank at the refinery a few miles east of Rawlins. "We've had some difficulties with them following through the way they need to after a spill of this size," said an inspection and enforcement manager for the department's Solid and Hazardous Waste Division. The spill of light straight run, a substance that can be blended with gasoline, happened when a floating storage tank roof took on fluid and sank. The roof punctured the tank bottom in several places, causing the release of 65,000 barrels of gasoline-grade fluid onto the refinery grounds. The department is seeking a penalty. The violation notice says Sinclair failed to address leakage into the pontoons that held up the floating tanks. A contractor documented the leakage some months before the spill, but the refinery lost track of the report and did not correct the problem. A similar incident happened at the refinery in 2007.
Source: http://billingsgazette.com/news/local/article_28334132-ff42-11de-adc7-001cc4c03286.html

3. *January 10, Associated Press* – (New York) **Tanker reports rupture off NY, no ethanol in water.** A tanker with 41,000 barrels of ethanol on board has a ruptured tank off of Brooklyn's Gravesend Bay and officials are evacuating all vessels from the area. The New York Fire Department and the Coast Guard say there have been no reports of injuries and no ethanol spilled off the 443-foot ship. Firefighters have sprayed the vessel with foam as a precaution. The Coast Guard says the Sichem Defiance was offloading 55,000 barrels of ethanol when the rupture happened. The tanker master told officials that the main deck of the vessel collapsed and caused the incident. The Coast

Guard says the evacuation of the area is a precaution.
Source: http://www.wcax.com/Global/story.asp?S=11797523

For another story, see item **5**

[Return to top]

Chemical Industry Sector

4. *January 8, NorthJersey.com* – (New Jersey) **Police call off evacuation after acid spill.** Police declared the area around a plastic plant on Dey Road in Wayne safe early Friday morning hours after a nitric acid spill sent two people to the hospital, authorities said. Authorities called off an evacuation around the Saint-Gobain Performance Plastic plant, 150 Dey Road, about 1 a.m., police said. Two employees at the plant were injured and nearly 200 people in the area were evacuated Thursday night after a nitric acid spill in the plant about 9 p.m., police said. The two employees were taken to Chilton Memorial Hospital in Pompton Plains after complaining about irritation and difficulty breathing, said a police lieutenant. Twenty employees at the plant were evacuated after the spill. Employees at a nearby sewer treatment plant were also evacuated, police said. Employees were alerted to the spill when one of them smelled something, saw a "white vapor" in a room and called police. A hazmat team from the fire department was dispatched to the scene to investigate.
Source:
http://www.northjersey.com/news/passaic_morris/passaic_town_news/010810_Police_call_off_evacuation_after_acid_spill_.html

[Return to top]

Nuclear Reactors, Materials and Waste Sector

5. *January 11, U.S. Nuclear Regulatory Commission* – (National) **NRC and the North American Electric Reliability Corporation coordinate their responsibilities for cyber security requirements.** The U.S. Nuclear Regulatory Commission and the North American Electric Reliability Corporation (NERC) have signed a Memorandum of Understanding (MOU) that outlines each organization's responsibility for applying cyber security requirements to nuclear power plants. The MOU was developed to ensure consistent regulation since the NRC and NERC have overlapping authority over cyber security at these commercial facilities. The MOU acknowledges the NRC's regulatory responsibility for inspecting digital systems that can affect safety, security and emergency preparedness of a nuclear power plant as well as NERC's responsibility for regulating digital systems related to continuity of electric power generation. As part of the MOU, the NRC and NERC agree to share information discovered during respective inspections that they believe may be relevant to any digital system governed by the other organization. Since under this provision NERC may need access to sensitive information or Safeguards Information, NERC has agreed to comply with NRC requirements related to protecting this information. The NRC and NERC will

hold a series of workshops to help U.S. nuclear power plants define which of their cyber systems and assets must comply with each organization's requirements. A Federal Register notice outlining the details of the MOU was published today and is available at: http://edocket.access.gpo.gov/2010/2010-229.htm.
Source: http://www.nrc.gov/reading-rm/doc-collections/news/2010/10-005.html

6. *January 11, U.S. Nuclear Regulatory Commission* – (Nebraska) **Emergency sirens may be impacted by extreme weather conditions.** The current NOAA weather forecast for the station is predicted to be about -25 degrees Fahrenheit [on the morning of January 9, 2010]. Based on this forecast, the station reviewed the impact of these temperatures on the 101 sirens in the Fort Calhoun Station 10-mile Emergency Planning Zone (EPZ) in Nebraska. The siren manufacturer's and the FEMA approved siren design report information states that the sirens (Federal Signal model 2001) are designed for operation between the temperature readings of -22 degrees Fahrenheit and +140 degrees Fahrenheit. Events on a similar condition at another utility having the same sirens were reviewed. It was noted that the reports documented discussion with the manufacturer's technical representative confirming that the sirens are operational and no special testing is required when the temperature goes below and then returns within the operating temperature limits. The current temperature at the station is within the operational limits. Therefore, the 101 sirens are considered functional at this time. The following agencies were notified that if the temperature falls below a negative twenty-two degrees Fahrenheit, the established process of back-up route alerting is to be used notifying the public in the event of a nuclear emergency where the sirens are activated but fail to respond: Washington County, NE Emergency Management; Pottawatomie County, IA Emergency Management; and Harrison County, IA Emergency Management.
Source: http://www.nrc.gov/reading-rm/doc-collections/event-status/event/en.html#en45615

[Return to top]

Critical Manufacturing Sector

7. *January 12, Associated Press* – (Iowa) **Heaters blamed for fire at Iowa conrete plant.** Authorities say electrical problems with portable heater units inside a storage area caused a fire at a concrete plant in Clear Lake. The fire at Andrews Prestressed Concrete Inc. was reported around 8:30 p.m. on Sunday. The company makes bridge girders, columns and roof slabs. A fire department spokesman estimates the damage at $110,000 due to extensive damage to electrical systems and control equipment for plant operations. The fire broke out in a ground level storage area and extended up into a second story operations control office inside the plant. The spokesman says the fire was discovered by a motorist who noticed smoke and flames coming from the complex.
Source: http://www.kgan.com/template/inews_wire/wires.regional.ia/38d79e49-www.kgan.com.shtml

[Return to top]

Defense Industrial Base Sector

8. *January 11, Associated Press* – (Tennessee) **Old building razed at Oak Ridge.** The demolition of 1 of the oldest buildings at the government's Oak Ridge reservation removes a concern over fire safety. The Knoxville News Sentinel reported Building 3026 has been leveled and the wooden debris is being hauled to a landfill. The building is located between two other nuclear facilities and close to the main research campus at Oak Ridge. Part of the ceiling had collapsed, causing the fire sprinkler system to be shut down. The building was put up in the early 1940s to process highly radioactive materials from the Graphite Reactor - the world's first continuously operated nuclear reactor.
   Source: http://www.wrcbtv.com/Global/story.asp?S=11800168

[Return to top]

Banking and Finance Sector

9. *January 12, Wall Street Journal* – (National) **Banks brace for bailout fee.** The U.S Presidential Administration is aiming to hit banks with a fee to recoup losses associated with the government's bailout of financial firms and the auto industry, administration officials say. The White House hopes the fee will soothe the public's anger at financial firms. Most big banks that received public funds have repaid the government, but the industry is seen by many as having survived thanks to taxpayer support, and is now enjoying a profit rebound as the economy struggles. This month, many large banks will resume paying big bonuses to employees. The Administration is likely to slap banks with a fee designed to recoup losses associated with TARP, in a move that could help lower the deficit and reduce risk-taking by big banks. Much remains uncertain about how such a fee would work. The Administration is wrestling with who should pay, when it should be implemented and what would happen if banks pay more than the government-bailout program ultimately loses. Auto makers are not currently targets of the fee idea. Even though the proposal is still under discussion, it is expected to be included in the White House's budget, due next month, if only conceptually. It is expected to cost large banks billions of dollars and could also affect bank customers if firms pass along the cost.
   Source:
   http://online.wsj.com/article/SB126322918488724799.html?mod=WSJ_hpp_MIDDLETopStories

10. *January 12, HedgeCo.Net* – (Florida) **Advisers charged with $160 million Nadel related hedge fund fraud.** The SEC has charged two investment advisers with securities fraud for misleading investors about the financial condition of three hedge funds they managed, and misrepresenting that they controlled the funds' investment and trading activities when in fact they were being handled by another individual. The SEC alleges that Sarasota, Florida-based suspects, a father and son, distributed offering materials, account statements, and newsletters to investors that misrepresented the hedge funds' historical investment returns and overstated their asset values by as much

as $160 million. According to the SEC's complaint, hedge funds Valhalla Investment Partners L.P., Viking IRA Fund LLC, and Viking Fund were controlled by another individual with no meaningful supervision or oversight by the father and son. The SEC charged the other individual with fraud last year and obtained an emergency court order to freeze his assets.
Source: http://www.hedgeco.net/news/01/2010/advisers-tcharged-with-160-million-nadel-related-hedge-fund-fraud.html

11. *January 12, Insurance and Financial Advisor* – (National) **More insurance agents 'cutting corners,' engaging in fraud, group says.** The number of insurance agents involved in suspected frauds has risen since the recession took hold, a new survey found. Meanwhile, funds devoted to investigating and prosecuting all insurance frauds appears to be decreasing among states and insurers, the Coalition Against Insurance Fraud (CAIF) survey found. "We are seeing [state] fraud bureaus and insurers cutting back," the CAIF's executive director told IFAwebnews.com. "That's not a healthy combination. I think we are all going to be paying for it in the future." The majority (69 percent) of state insurance department fraud directors participating in the survey said agent fraud was up "slightly" or "much higher" than in 2008. One quarter of the 37 state fraud bureaus said agent fraud levels were the same as in 2008, and one agency reported a decline. The executive director, who authored the report, said he found the agent fraud responses surprising, but blamed the economy. As companies and individuals look more closely at their premiums, policies and other insurance information, seeking ways to cut costs, the chances of identifying improper or illegal insurance activity increases, the executive director said.
Source: http://ifawebnews.com/2010/01/12/more-insurance-agents-cutting-corners-engaging-in-fraud-group-says/

12. *January 11, Bloomberg* – (National) **Federal Reserve seeks to protect U.S. bailout secrets.** The Federal Reserve asked a U.S. appeals court to block a ruling that for the first time would force the central bank to reveal secret identities of financial firms that might have collapsed without the largest government bailout in U.S. history. The U.S. Court of Appeals in Manhattan will decide whether the Fed must release records of the unprecedented $2 trillion U.S. loan program launched after the 2008 collapse of Lehman Brothers Holdings Inc. In August, a federal judge ordered that the information be released, responding to a request by Bloomberg LP, the parent of Bloomberg News. "This case is about the identity of the borrower," said a lawyer for the government, in oral arguments on January 11. "This is the equivalent of saying 'I want all the loan applications that were submitted.'" Bloomberg argues that the public has the right to know basic information about the "unprecedented and highly controversial use" of public money. Banks and the Fed warn that bailed-out lenders may be hurt if the documents are made public, causing a run or a sell-off by investors. Disclosure may hamstring the Fed's ability to deal with another crisis, they also argued. The lower court agreed with Bloomberg.
Source: http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a4PnUdySIink

13. *January 11, Agence France-Presse* – (International) **Toronto man denies plot to bomb bourse and cash in.** A Toronto man on January 11 pleaded not guilty to plotting to bomb Canada's main stock exchange in 2006, as prosecutors said he aimed to profit from wreaking economic havoc to fund other terror attacks. The 34 year old defendant is accused of conspiring to bomb the Toronto Stock Exchange, Canada's spy agency offices and a military base in order to try to provoke Canada's withdrawal from Afghanistan. He was arrested with 17 alleged Islamic extremists in a 2006 police sting operation after the group sought to purchase three tons of bomb-making ingredient ammonium nitrate from undercover police officers. According to reports, he saw an opportunity to profit from blowing up the Toronto Stock Exchange by short-selling stocks before the bombings and reap a windfall that could be used to fund more terror attacks abroad. While his co-conspirators were impressionable young men with modest means, bent on destruction and mayhem for "religiously-inspired political purposes," prosecutors say the defendant was motivated primarily by financial gain. The plan was "to affect the economy, to make it lose half a trillion dollars," said court documents cited by the daily Globe and Mail.
    Source: http://www.google.com/hostednews/afp/article/ALeqM5jwfzJk4QP28W2baGqscr_cwf_cOQ

14. *January 11, Marketwatch* – (National) **Special bankruptcy court for big banks is on the table.** Key members of the Senate Banking Committee are in discussions to create a special bankruptcy court for "too-big-to-fail" banks, according to people familiar with discussions on the panel. The court would work in tandem with a process to dismantle a Lehman-like failing super-sized bank in a way that does not cause collateral damage to the markets. Lawmakers in the committee are working to see if they can create a broad bipartisan bank reform bill in response to the financial system's near collapse in 2008. Two Senate Banking Committee members have been charged with reaching a bipartisan deal on systemic risk issues. The Financial Crisis Commission will require top bankers and regulators to testify about the causes of the financial crisis.
    Source: http://www.marketwatch.com/story/senators-in-talks-about-big-bank-bankruptcy-court-2010-01-11?reflink=MW_news_stmp

[Return to top]

Transportation Sector

15. *January 12, Reuters* – (National) **FAA calls for inspections of older Boeing 737s: report.** The U.S. Federal Aviation Administration (FAA) has called for enhanced inspections of more than 130 older Boeing 737 planes, the Wall Street Journal said, citing a safety directive that is likely to be issued on Tuesday. The FAA has asked for enhanced structural inspections to find possible cracks in the fuselage skin of the planes, according to the paper. Undetected cracks "could result in sudden fracture and failure of the fuselage skin panels, and consequent rapid decompression," the paper cited the FAA's safety directive as saying. Boeing and the FAA could not be immediately reached for comment outside regular U.S. business hours. In July 2009, a

737 operated by Southwest Airlines developed a foot-wide hole and lost cabin pressure about 30 minutes after takeoff. Inspections in July revealed no problems with 737-300 jetliners flown by Southwest.
Source: http://www.reuters.com/article/idUSTRE60B0OC20100112

16. *January 12, NBCPhiladelphia.com* – (Pennsylvania) **Sick passenger on "Do Not Board" list flies out of Philly.** An investigation has been launched to find out why a man with an extremely contagious disease was allowed to fly out of Philadelphia International Airport. The man, who is infected with Tuberculosis, boarded US Airways flight 401 bound for San Francisco around 6 p.m. Saturday, Centers for Disease Control (CDC) officials said. He made it onto the flight even after being added to a "Do Not Board" list provided to the TSA and airlines from the CDC, officials confirmed. The agency adds people afflicted with dangerous, contagious diseases to the list to prevent the spread of infection in the controlled air environment of an airplane. That information is then relayed to the TSA who in turn notifies the airlines. Sources say officials realized the man was not fit to travel while he was on the plane and that he was quickly quarantined upon arrival in San Francisco. US Airways is notifying passengers who were on the flight, sources said. CDC officials believe the risk to passengers is low due to the length of the flight. A US Airways spokesperson says the airline is working with the TSA and CDC to figure out where the fault in the "Do Not Board" system occurred.
Source: http://www.msnbc.msn.com/id/34815230/ns/local_news-philadelphia_pa/

17. *January 12, Occupational Health and Safety* – (National) **HazCom changes proposed for transporting Lithium batteries.** The Pipeline and Hazardous Materials Safety Administration published a proposed rule Monday that would amend the Hazardous Materials Regulations to increase the safety of transported lithium batteries. Besides including requirements to ensure all lithium batteries are packaged to prevent damage leading to a catastrophic incident or minimize the effects of an incident, the proposal would require the batteries to be accompanied by hazard communication that ensures appropriate and careful handling by air carrier personnel, including the flight crew, and tells transport workers and emergency response personnel what to do in an emergency. Manufacturers will have to keep results of satisfactory completion of UN design type tests for each lithium cell and battery type and also place a mark on the battery and/or cell to indicate testing has been completed successfully. For all transport modes, lithium cells and batteries will have to be packed to protect the cell or battery from short-circuits. For aviation, unless the cells or batteries are transported in a container approved by the FAA administrator, they would have to be stowed in crew-accessible cargo locations or locations equipped with an FAA-approved fire suppression system.
Source: http://ohsonline.com/articles/2010/01/12/hazcom-changes-proposed-for-transporting-lithium-batteries.aspx?admgarea=news

18. *January 11, Associated Press* – (Wisconsin) **TSA: Passenger carries ammo on plane in Milwaukee.** A passenger inadvertently carried shotgun shells onto a Dallas-bound Midwest Airlines plane at Milwaukee's airport on Monday before he realized his mistake and alerted flight attendants, authorities said. The man, who was not identified,

did not mean any harm, saying he had forgotten that the ammunition was in his carryon bags when he boarded the flight, a Transportation Security Administration (TSA) spokesman said. TSA agents turned the ammunition over to local police and sent the man back for another security search. They then allowed him to reboard and the plane left for Dallas later Monday. "The passenger was interviewed and rescreened with negative findings," the spokesman said in a statement. "The passenger stated that he inadvertently brought the prohibited items onboard the plane and self-disclosed them when he realized they were in his possession." TSA is reviewing how the passenger got the ammunition through pre-boarding security searches. He declined to identify the man or comment further. TSA policy prohibits passengers from having firearms or ammunition in their carryon luggage.
Source: http://www.foxnews.com/story/0,2933,582803,00.html

19. *January 11, Wired* – (National) **Airport scanners can store, transmit images.** Contrary to public statements made by the Transportation Security Administration (TSA), full-body airport scanners do have the ability to store and transmit images, according to documents obtained by the Electronic Privacy Information Center. The documents, which include technical specifications and vendor contracts, indicate that the TSA requires vendors to provide equipment that can store and send images of screened passengers when in testing mode, according to CNN. The TSA has stated publicly on its website, in videos and in statements to the press that images cannot be stored on the machines and that images are deleted from the scanners once an airport operator has examined them. The administration has also insisted that the machines are incapable of sending images. But a TSA official acknowledged to CNN that the machines do have these capabilities when set to "test mode." The official said these functions are disabled before the machines are delivered to airports and that there is no way for screeners in airports to put the machines into test mode to enable the functions. The official, however, would not elaborate on what specific protections, if any, are in place to prevent airport personnel from putting the machines in test mode. The TSA also asserts that the machines are not networked, so they cannot be accessed by hackers.
Source: http://www.wired.com/threatlevel/2010/01/airport-scanners?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+wired/index+(Wired:+Index+3+(Top+Stories+2))&utm_content=Google+Reader

20. *January 11, Washington Post* – (District of Columbia) **Metro launches track safety workshop.** Metro began a three-day workshop Monday focused on safety for employees who work along the tracks, a month after a train apparently going at full speed almost hit an independent team of safety inspectors. The workshop includes safety experts from the Federal Transit Administration and transit agencies in New York, San Francisco, Baltimore and Philadelphia, as well as the Tri-State Oversight Committee, whose team was involved in the near-miss December 10. The committee, the regional agency that has oversight of Metro safety, issued a draft report December 31 that strongly criticized Metro's program for protecting employees who work along the tracks. The report said the committee "observed serious violations" of the program, concluding that the program "is not effective as it is currently written, applied and

enforced." The Metro General Manager said that the three-day session will focus on "what needs to happen to make our right-of-way a safer place for our employees," according to a Metro news release. The workshop will span a broad range of safety topics, from "advance warning systems for 'blind curves' " to "Metro's safety culture," according to the release.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/11/AR2010011103278.html?wprss=rss_metro

For another story, see item **3**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

21. *January 12, Philadelphia Inquirer* – (New Jersey) **Chocolate factory fined for fatal fall into vat.** Federal safety officials fined a Camden chocolate plant $39,000 yesterday for safety violations following the death of a factory worker who fell into a vat of chocolate last summer. Inspectors from the Occupational Safety and Health Administration (OSHA) cited Moorestown-based Lyons & Sons Inc. and Cocoa Services L.P. for failing to install railings above the tanks or post signs warning workers of potential hazards. On the morning of July 8, a temporary worker who had started at the plant two weeks earlier, was loading raw cocoa into an eight-foot mixing and melting tank when he fell into the liquid chocolate and was struck on the head by a rotating paddle. After the accident, Lyons & Sons was temporarily closed and eventually fined $1,152 by the City of Camden when inspectors discovered the plant had been operating without a mercantile license. Inspectors also found plumbing and electrical problems on the property, which, in a July interview, company officials said had been corrected.
Source: http://www.philly.com/philly/news/local/81206877.html

22. *January 11, Food Safety News* – (Massachusetts) **First beef E. coli recall of 2010.** Athol, Massachusetts-based Adams Farm Slaughterhouse, LLC., recalled approximately 2,574 pounds of beef that may be contaminated with E. coli O157:H7, according to the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS). This recall was initiated after the Massachusetts Department of Public Health (MDPH) confirmed a positive ground beef sample for E. coli O157:H7, which it collected during an epidemiological investigation. FSIS then concluded there is an association between the ground beef products and an illness in the state of Massachusetts. FSIS is continuing to work with the MDPH on the investigation. Each package of ground beef cutlets bears a label with the establishment number "EST.

5497" inside the USDA mark of inspection as well as the packaging date of "11/11/2009." The beef products were distributed to private owners on three separate Massachusetts farms.
Source: http://www.foodsafetynews.com/2010/01/massachusetts-has-first-hamburger-e-coli-recall-of-2010/

[Return to top]

Water Sector

23. *January 12, Topeka Capital-Journal* – (Kansas) **Monday fire intentionally set.** An investigation into a blaze Monday that damaged a city-owned building has determined the fire was intentionally set, said a spokesman for the Topeka Fire Department. Topeka firefighters were called about 5 p.m. to the Oakland Wastewater Treatment Plant, 1115 N.E. Poplar, in response to a blaze at one of the buildings on the site, located north of Billard Park. Firefighters first on scene reported smoke showing and quickly contained the fire to an immediate area and two vehicles. The Topeka Fire Department's Investigation Unit determined the fire was intentionally set and caused an estimated $40,000 in damage. No injuries were associated with this incident, which remains under investigation.
Source: http://cjonline.com/news/local/2010-01-12/monday_fire_intentionally_set

24. *January 12, Associated Press* – (District of Columbia; Virginia) **Area drinking water disinfectant changing.** The Army Corps of Engineers is changing the disinfectant in the drinking water for nearly 1 million residents of Washington, D.C., and Northern Virginia. The Washington Aqueduct, an arm of the U.S. Army Corps of Engineers, is making the change from chlorine gas to a liquid form of chlorine called sodium hypochlorite to avoid the threat of a release of chlorine gas by terrorists. Officials say the liquid is considered safer to transport, store and use. The aqueduct provides roughly 180 million gallons of drinking water a day to about 1 million residents in the District, Arlington and Falls Church. Officials say people will not notice any difference in the way water tastes or smells. The Washington Aqueduct general manager says the change will begin next month. Caustic soda and a sulfuric acid solution will be added to balance pH levels.
Source: http://www.wtop.com/?nid=25&sid=1861240

[Return to top]

Public Health and Healthcare Sector

25. *January 12, WBRZ 2 Baton Rouge* – (Louisiana) **Charity Hospital talks begin.** A three-judge panel began to referee a dispute Monday between state and federal governments over the amount of damage the New Orleans charity hospital received from Hurricane Katrina. Two Louisiana groups objected to the closed-door proceedings. Government officials voiced support for arbitration hearings, which are routinely held in private. FEMA has offered the state $150 million for the 2005

hurricane damage to the LSU hospital commonly called Charity. State officials say that FEMA owes the state $492 million because the hospital was more than 50 percent damaged. According to the federal Stafford Act, the federal government must replace any structure damaged more than 50 percent. The Civilian Board of Contract Appeals is expected to spend several days this week listening to the two sides debate the funding for the public hospital. The state is fighting for the most money it can get to help fund a new $1.2 billion academic medical center instead of fixing and reopening Charity. Source: http://www.2theadvocate.com/news/politics/81202362.html

26. *January 12, Madison Press* – (Ohio) **Hydrogen leak at Battelle contained.** A hydrogen gas leak late afternoon on January 11 forced the evacuation of Battelle's Hazardous Materials Research Center (HMRC) located at the Battelle Biomedical Research Center's campus at 1425 Plain City-Georgesville Road in West Jefferson. "It was a small cylinder of hydrogen that leaked," said a Battelle spokesperson. "There was no release outside of the lab and no threat to the building." However, in keeping with established Battelle safety procedures, all 40 people in the HMRC were evacuated. Units of the Jefferson Township Fire Department were called and responded to the scene at 5 p.m. According to the company spokesman, hydrogen gas is considered flammable at higher concentrations. The level of the leaking gas at HMRC was not detected at any high concentration. The building was declared safe at approximately 6 p.m., and all 40 lab employees were permitted to return to the HMRC, said the spokesman. He added that the cause of the leak continues to be investigated. Source: http://www.madisonpress.com/local.asp?ID=1869&Story=1

27. *January 11, Los Angeles Times* – (National) **Even medical professionals lack awareness of hepatitis threat, new report finds.** Hepatitis B and C remain serious threats to public health, but many healthcare providers fail to screen at-risk patients and do not know how to treat those infected with the viral diseases that can cause liver failure and cancer, according to a report released today by the National Academy of Sciences. The long-awaited assessment calls for a campaign to educate the public, doctors and lawmakers about the diseases, an approach similar to HIV/AIDS outreach that has made that issue prominent in people's minds. Researchers found that even though chronic viral hepatitis infections are three to five times more frequent than HIV in the United States, many doctors and nurses do not understand the extent and seriousness of the problem. Most of the estimated 3 million to 5 million people with chronic hepatitis B and C do not know they have the diseases. Infected people can show no signs of illness for years, and by the time they start to show symptoms, they may have already developed scarring of the liver or liver cancer and can be close to death. The 176-page report requested by federal health officials was released by the Institute of Medicine, the health arm of the National Academy of Sciences. Source: http://latimesblogs.latimes.com/lanow/2010/01/even-medical-professionals-lack-awareness-of-hepatitis-threat-new-report-finds.html

28. *January 11, KECI 13 Missoula* – (Montana; International) **Nuclear medicine shortage causing delays.** All across Montana, hospitals are experiencing a shortage of nuclear medicine. Nuclear medicine is used to screen for cancer and Parkinson's disease. The

shortage means a delay of four or five days for patients who need tests. The problem is only five nuclear reactors in the world produce the medical isotopes. The country's biggest supplier is in Canada. Unfortunately, that plant has been shut down for a long time causing a critical shortage. A a cardiologist at the Montana Heart Center noted that the plant supplies about 70 percent of the nuclear medicine isotopes in the United States. "It's hard in our nuclear medicine world because it's what we do and we can't do it when we don't have our isotopes," she said, adding that by early spring at St. Patrick Hospital in Missoula they plan to use stress cardiac MRI's, an alternative diagnostic tool, not affected by the isotope shortage.
Source: http://www.keci.com/Nuclear-Medicine-Shortage-Causing-Delays/6089577

29. *January 11, Nextgov* – (National) **FDA nationwide electronic network will track safety of drugs and medical devices.** The Food and Drug Administration (FDA) is constructing a nationwide electronic system to continuously track the safety of drugs and medical devices using anonymous patient data, but federal officials and health care specialists say its usefulness might be limited without more personal information. The Sentinel initiative, launched in May 2008, will complement existing systems that monitor side effects and other adverse changes in health linked to FDA-regulated products. The system will tie together information from various registries, including electronic health record systems and insurance claims databases, allowing FDA workers to query an issue quickly. To protect patient privacy, the owners of the various registries will maintain the underlying data. FDA would send questions to the data holders, who in turn would deliver summary results to the agency.
Source: http://www.nextgov.com/nextgov/ng_20100111_6160.php?oref=topstory

30. *January 11, Global Security Newswire* – (California) **CDC announces $2.7M for emergency health planning research.** Two new research centers were set up recently with $2.7 million from the U.S. Centers for Disease Control and Prevention (CDC) with the aim of analyzing the framework, track record and capacities of public health systems' emergency response programs. Seven other emergency planning research centers were established in 2008 with $10.9 million in funding. Centers at the University of California, Berkeley, and the University of California, Los Angeles, are the two latest to be funded, according to a CDC press release. The 2006 Pandemic and All-Hazards Preparedness Act, which seeks to better local, state and federal public health preparations and emergency response activities, mandated the creation of the research centers. The nine centers are to receive research funding for four more years for their efforts to strengthen public health systems' abilities to meet evolving health dangers.
Source: http://www.globalsecuritynewswire.org/gsn/nw_20100111_2038.php

For another story, see item **16**

[Return to top]

Government Facilities Sector

31. *January 11, WPIX 11 New York* – (New Jersey) **4 students arrested, charged for making 'terroristic' threats.** Four high school students were arrested and charged Monday, after making terroristic threats against their school on Facebook, police said. According to investigators, the teens — all students at Belleville High School — talked about blowing up or setting fire to the school on the social media website. The alleged threats were found by a fellow student who immediately alerted school officials. The school was evacuated around 11:30 a.m. and students were sent home by the superintendent after police were notified, authorities said. A search of the school conducted by the Essex County Sherriff's Office Bomb Squad turned up nothing unusual. Of the students arrested were two 16-year-old females, one 17-year-old female and a 17-year-old male. The suspects were not identified because of their ages, police said. All four students are being charged with causing a false public alarm, making terroristic threats and conspiracy.
Source: http://www.wpix.com/news/local/wpix-teens-charged-for-threats,0,4487930.story

32. *January 11, Web Host Industry Review* – (National) **Hacker finds SQL injection vulnerability in Army Web site.** A Romanian hacker has disclosed an SQL injection vulnerability on a U.S. Army Web site that could lead to a full database compromise. According to a report from Softpedia, a Web site used to provide information about military housing facilities to soldiers, called Army Housing OneStop, was found to be storing passwords in plain text — a major security oversight. A compromised AHOS Web site could provide an intruder access to some 76 databases on the server, some containing confidential information on worldwide Army installations. The AHOS has since been taken offline. A security enthusiast going by the name of TinKode blogged about a proof-of-concept attack on onestop.army.mil, which seems to have been developed by a third-party government contractor, DynaTouch Corporation. The published screenshots reveal that the Web server runs on Microsoft Windows 2003 with Service Pack 2 and the database engine used to power the ASP Web site is Microsoft SQL Server 2000.
Source: http://www.thewhir.com/web-hosting-news/011110_Hacker_Finds_SQL_Injection_Vulnerability_in_Army_Website

[Return to top]

Emergency Services Sector

33. *January 12, WISN 12 Milwaukee* – (Wisconsin) **Aldermen call for Ladder Co. 10's return.** Milwaukee aldermen are considering a plan to use part of the city's emergency fund to restore a fire company closed due to budget cuts. The move is prompted by a rash of recent fires, two of which were fatal. Also, two fires in the last three days happened in the neighborhood the former company served. On Monday morning, a group of people jumped out of a burning house at North Bremen and East Wright streets. Firefighters said four people were lucky enough to escape the fire without serious injury. Rescue crews said they did arrive quickly, but they are becoming

increasingly concerned that budget cuts may cut into safety.
Source: http://www.wisn.com/news/22211238/detail.html

34. *January 12, Denver Post* – (National) **False signals produce problems for search and rescue teams.** A wilderness rescue device designed as a "just in case" safety lifeline has developed into a recurrent nuisance for search and rescue teams near Berthoud Pass. A string of eight false alarms in the past month has renewed debate over the controversial personal locator beacons (PLBs) and leaves local rescue experts frustrated over a lack of backcountry education in the technological era. Members of the Alpine Rescue Team have been working overtime to solve a mystery that began December 14 when an emergency signal emanating from an ACR Electronics PLB-300 MicroFix was picked up by the U.S. Air Force. Since then, the same signal has bounced off a satellite from an area between Winter Park and Jones Pass on seven occasions, sending a cascade of rescuers ranging from the Air Force to state search and rescue (SAR) coordinators, local sheriff's departments and multiple mountain rescue teams scrambling to locate the signal and determine if someone was in need. Six times teams have headed up the pass, only to find that the unregistered PLB had been turned off. After determining the serial number of the unit, SAR teams are no longer responding to the emergency signal last received January 5 but are hoping to prevent similar incidents from occurring in the future. Satellite-detectable PLBs are a relatively new phenomenon in the world of inland backcountry recreation, although they are increasing in popularity among hunters, campers, hikers, climbers, skiers and boaters, according to the ACR Electronics website. PLBs perform the same function as Emergency Position Indicating Radio Beacons often used by ocean-going boaters, but are smaller, lighter and more convenient to carry. Both units transmit signals on internationally recognized distress frequencies monitored by the National Oceanic and Atmospheric Administration (NOAA), sending out GPS coordinates with a push of the panic button.
Source: http://www.denverpost.com/sports/ci_14169778

35. *January 11, Nextgov* – (National) **Public safety officials seek additional spectrum for first responders.** Top public safety officials plan to ask Congress to enact legislation directing the Federal Communications Commission to allocate a slice of cellular communications spectrum to first responders and halt auctions to commercial carriers. The push comes seven years after the 9/11 commission recommended in its report that local public safety agencies be assigned new spectrum quickly. In what it described as an "unparalled event," the Association of Public-Safety Communications Officials (APCO) International said it will hold a briefing at the National Press Club on Tuesday with leading police and fire officials to urge Congress to immediately reallocate the 700 megahertz D block cellular spectrum for public safety use. The broadband network also could support automated license plate recognition and biometric technologies, including mobile fingerprint and iris identification, according to APCO. FCC failed to attract a bidder for block D during a February 2008 cellular auction, and unless Congress acts now, the commission must put the block up for auction again.
Source: http://www.nextgov.com/nextgov/ng_20100111_8068.php?oref=topnews

[Return to top]

Information Technology Sector

36. *January 12, IDG News Service* – (International) **Google blames 'human error' for leak of users' business data.** Google is apologizing after it mistakenly e-mailed potentially sensitive business data last week to other users of its business listings service. The company's Local Business Center allows businesses to create a listing for Google's search engine and Maps application, as well as add videos, coupons or photos. Google then provides data on how customers found the listing, showing search terms people used before clicking the listing and other data such as the geographic location of someone who looked up driving directions to the business. Google will send reports to those who are signed up. Early last week, Google sent the reports to third parties by mistake. The mistake affected several thousands businesses registered with Local Business Center, of which there are more than a million. People who received the data then began to publicize the incident, realizing the privacy implications. A Chicago-based Internet consultant wrote on his blog that he received information regarding the listing for Boscos, a restaurant in Tennessee that brews its own beer. The data included the number of times Boscos' listing appeared in Google's local search results, the number of times it had been clicked on and the number of follow-through clicks on the actual business' Web site.
Source: http://www.infoworld.com/d/security-central/google-blames-human-error-leak-users-business-data-408

37. *January 12, The Register* – (International) **Apple sits on critical Mac bug for 7 months (and counting).** Researchers have disclosed a critical vulnerability in the latest version of Mac OS X that they say Apple has sat on for almost seven months without fixing. The buffer overflow flaw could be exploited by attackers to remotely execute malicious code, and virtually all Apple devices - including Mac computers and servers, iPhones, and even Apple TV - are susceptible, one of the researchers told The Register. SecurityReason.com, the Poland-based security firm he works for, alerted Apple to the vulnerability in the middle of June and again last month, but the computer maker has yet to patch the bug. By contrast, developers for OpenBSD, NetBSD, FreeBSD, and a variety of Mozilla applications have fixed identical vulnerabilities, in some cases within hours of notification. The bug affects all applications and operating systems that implement gdtoa floating point numbers. The OS X bug resides in the libc/strtod(3) and libc/gdtoa function. The researcher said the vulnerability could be remotely exploited using booby-trapped PHP code on a website, among other methods.
Source: http://www.theregister.co.uk/2010/01/12/critical_osx_security_bug/

38. *January 12, The Register* – (International) **Frustrated bug hunters to expose a flaw a day for a month.** A Russian security firm has pledged to release details of previously undisclosed flaws in enterprise applications it has discovered every day for the remainder of January. Intevydis intends to publish advisories on zero-day vulnerabilities in products such as Zeus Web Server, MySQL, Lotus Domino and Informix and Novell eDirectory between January 11 and February 1, a security blogger

reports. As an opener, Intevydis published a crash bug in Sun Directory Server 7.0, along with exploit code. The final line-up of zero-days is still being finalised, but the MySQL buffer overflows and IBM DB2 root vulnerability flaws on the provisional menu sound much tastier than Intevydis's somewhat bland opener. Advisories are due to be published on the Intevydis blog here. Intevydis said it launched its campaign after becoming more and more disillusioned with foot-dragging by vendors when confronted by security flaws in their products. Only one software vendor, Zeus, reportedly worked with Intevydis in developing a patch to be released at the same time as an upcoming advisory from the Russian security firm. Intevydis's stance is likely to reboot the long running debate about the responsible disclosure of security vulnerabilities. An entry on the Intevydis blog accuses software vendors of exploiting researchers as unpaid lackeys.
Source: http://www.theregister.co.uk/2010/01/12/enterprise_sec_disclosure_campaign/

39. *January 11, IDG News Service* – (Maryland) **Maryland aims to be cybersecurity 'epicenter'.** Maryland officials want the state to be the U.S. "epicenter" for fighting cyber attacks, and on January 11 they launched an effort to bring more cybersecurity research and jobs to the state. Maryland has several resources that make it the perfect place to be a national — and world — leader in cybersecurity, said the Governor, speaking at a kick-off event at the U.S. National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland. In addition to the NIST, Maryland is home to the U.S. National Security Agency, 12 major military installations, world-class schools such as Johns Hopkins University and dozens of top cybersecurity vendors, the governer and other officials said. Cybersecurity leadership and innovation is needed at a time when the U.S. is getting attacked from all sides, said a Maryland Democratic senator. "Cybersecurity is all-hands-on-deck and all-agencies-on-deck," she said. The governor's administration on January 11 released a 32-page report, called CyberMaryland, focused on ways to improve cybersecurity efforts in the state. The report calls for the state to work with the U.S. government to establish a national center of excellence in cybersecurity in the state, including a cybersecurity business incubator and an education and training center.
Source:
http://www.computerworld.com/s/article/9143823/Maryland_aims_to_be_cybersecurity_epicenter_

40. *January 11, DarkReading* – (International) **More researchers going on the offensive to kill botnets.** Yet another botnet has been shut down as of January 11 as researchers joined forces with ISPs to cut communications to the prolific Lethic spamming botnet — a development that illustrates how botnet hunters increasingly are going on the offensive to stop cybercriminals, mainly by disrupting their valuable bot infrastructures. For the most part researchers monitor and study botnets with honeypots and other more passive methods. Then security vendors come up with malware signatures to help their customers scan for these threats. But some researchers are turning up the heat on the bad guys' botnet infrastructures by taking the lead in killing some botnets: Aside from the recent takedown by Neustar of Lethic, which is responsible for about 10 percent of all spam, FireEye in November 2009 helped shut

down the MegaD botnet. And researchers at the University of California at Santa Barbara in May revealed they had taken the offensive strategy one step further by infiltrating the Torpig botnet, a bold and controversial move that stirred debate about just how far researchers should go to disrupt a botnet.
Source:
http://www.darkreading.com/insiderthreat/security/vulnerabilities/showArticle.jhtml?articleID=222300408

41. *January 11, The Register* – (International) **False Facebook charge group used to spread malware.** A false rumor suggesting that Facebook is to start charging is being used to bait malware traps. Thousands of disgruntled punters, angry at the $4.99 a month charge for using the social networking site that will supposedly kick in from June (or July, according to other false reports) have been induced to visit "protest group" sites in response to spam emails. However, in reality, there is no such plan and the protest pages often contain malware, as urban myth debunking site Snopes warns: The protest page was a trap for the unwary; clicking on certain elements of it initiated a script that hijacked users' computers. Some of those who did venture a click had their computers taken over by a series of highly objectionable images while malware simultaneously attempted to install itself onto their computers.
Source:
http://www.theregister.co.uk/2010/01/11/facebook_charging_rumour_malfeasance/

For another story, see item **43**

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

42. *January 12, Kentucky Post* – (Ohio) **Verizon scrambles to fix fiber optic line.** Landline phone service remains disrupted in parts of Adams and Brown counties on January 11. Verizon brought field workers from as far away as Dayton and Wilmington to try to locate a severed fiber optic line near Sardinia in Brown County. "It's a huge problem, but we'll work through the night to get service to our valued customers," said a local manager for Verizon. Work was slowed, however, when a power line was discovered on top of one of Verizon's access boxes. Earlier in the day it was thought that a Sardinia crew working to fix a water line may have disrupted the phone service. In the meantime, Verizon says that as of 8:30 p.m. (EST), a majority of service in the affected region had been re-routed and thus, restored. Field crews may have to wait until daylight Tuesday morning to identify and repair the damaged fiber

optic line.
Source: http://www.kypost.com/content/wcposhared/story/Verizon-Scrambles-To-Fix-Fiber-Optic-Line/ENgZj94o7kibph1umFtByQ.cspx

43. *January 11, IDG News Service* – (International) **Group behind Twitter hack takes down Baidu.com.** The group that took down Twitter.com in December 2009 has apparently claimed another victim: China's largest search engine Baidu.com. Baidu.com was offline on January 11, but at one point it displayed an image saying "This site has been hacked by Iranian Cyber Army," according to a report in the official newspaper of the Chinese Communist Party and other Web sites. With more than half of China's Internet search market, Baidu is by far China's most-used search engine. The company could not immediately be reached for comment. Not much is known about the Iranian Cyber Army, which first gained notoriety with its December 18 Twitter attack. Hacking groups such as this are constantly defacing Web sites, but it is extremely rare for them to take down a site as widely used as Twitter or Baidu.com. According to security experts, Baidu's domain name records appear to have been tampered with. On Monday, the company was using domain name servers belonging to HostGator, a Florida ISP, instead of the Baidu.com nameservers the company normally uses. "It looks like their domain account credentials may have been snagged," said a researcher with the antivirus vendor Trend Micro. That is the same technique that was used to hijack Twitter, when Iranian Cyber Army hackers were apparently able to log in to the account used to manage Twitter's DNS records and redirect visitors to another Web server that posted a message similar to the one spotted on Baidu.com. That attack knocked Twitter offline for more than an hour.
Source: http://www.computerworld.com/s/article/9143919/Group_behind_Twitter_hack_takes_down_Baidu.com

44. *January 11, The Register* – (Florida) **Judge awards Dish Network $51m from satellite pirate.** A federal judge has slapped a $51m judgment on a Florida man for distributing software that allowed people to receive television programming from Dish Network without paying for it. The ruling, issued on January 11 by a US District judge of Tampa, found that the defendant violated both the Digital Millennium Copyright Act and the Communications Act. Using the online monikers "Thedssguy" and "Veracity," the defendant provided 255,741 piracy software files, making him liable for damages of $51.148m, or $200 per download. Under the DMCA, the defendant could have been forced to pay $2,500 for each download, an amount that would have brought damages to more than $639m. The defendant was also ordered to pay Dish Network's attorney fees and to permanently stop making or distributing software that circumvents the satellite provider's security. The software at issue allowed users to bypass access security technology provided by Dish co-venture NagraStar, so they could receive premium programming and regular channels on so-called free-to-air receivers. The receivers are designed to play only unencrypted satellite transmissions, such as ethnic, religious, and advertising content. After flashing the devices with the software, users could watch paid programming on the receivers.
Source: http://www.theregister.co.uk/2010/01/11/satellite_piracy_judgement/

45. *January 11, Government Technology* – (Michigan) **Michigan releases shared data center RFI.** Michigan has formally launched an initiative to build a massive new data center that will provide cloud computing services to state agencies, cities, counties and schools across the state. The Michigan Department of Information Technology (MDIT) — in conjunction with the state's Department of Treasury and Department of Management and Budget — issued a request for information (RFI) January 7 seeking industry feedback on forming a public-private partnership to build and operate the facility. "This marks another big step in our effort to establish high-tech investment in Michigan," said state CIO in a statement released by the MDIT. "A data center built through public-private partnership will allow all levels of government in Michigan to benefit, by getting the most of our taxpayer dollars." The RFI seeks input from companies or teams of companies that are interested in financing, building and operating the new facility, as well as providing shared IT services to state agencies and others. The state is particularly interested in tapping alternative energy sources for the data center, according to the RFI.
Source: http://www.govtech.com/gt/articles/736695

For another story, see item **35**

[Return to top]

Commercial Facilities Sector

46. *January 11, Los Angeles Times* – (California) **ELF member pleads guilty to placing bomb in Pasadena condo project.** A man who admitted being a member of the radical environmental group Earth Liberation Front— or ELF, as it's known — pleaded guilty in federal court today to placing a gasoline-filled bomb in a Pasadena condominium project that was under construction in 2006, authorities said. The 44- year-old man pleaded guilty in U.S. District Court in Los Angeles to one count of conspiracy to commit arson. The man placed the bomb in the Vista del Arroyo Bungalows project, which was being built directly under the Colorado Bridge in Pasadena, federal prosecutors said. He lighted the device and then fled the scene; but the timer failed, so it did not ignite. The crime remained unsolved until 2009 when investigators matched DNA extracted from the incendiary device to a sample of his DNA in a law enforcement database. He is scheduled to be sentenced April 5 and faces a maximum of five years in federal prison, the U.S. attorney's office said.
Source: http://latimesblogs.latimes.com/lanow/2010/01/elf-member-pleads-guilty-to-placing-bomb-in-pasadena-condo-project.html

47. *January 11, Orlando Sentinel* – (Florida) **Scene cleared in "suspicious" incident near OIA.** Orlando police have cleared the scene of a suspicious incident that prompted the evacuation of a hotel near Orlando International Airport, a police sergeant said. Officers were called to Hazeltine National Drive before 1:30 p.m. after a caller reported a suspicious, unattended FedEx delivery truck. As a precaution, police brought an explosive-sniffing dog to the scene, which alerted its handler to possible explosives, the sergeant said. An Orange County dog did the same, but investigators ultimately

determined they were wrong. Three businesses were evacuated, including a nearby Embassy Suites on T.G. Lee Boulevard.
Source: http://www.orlandosentinel.com/news/local/breakingnews/os-hotel-evacuated-suspicious-incident-20100111,0,2551054.story

48. *January 11, Red Bluff Daily News* – (Michigan) **Pipe bomb shuts Red Bluff River Park.** Members of the Shasta County bomb squad destroyed a pipe bomb early Saturday afternoon on Willow Street. Police received reports of a pipe bomb lying in the street between Hal's Eat 'Em Up and Tom's Glass and Muffler Center around 8 a.m. and quickly moved to seal off the block. At one point, traffic on main street was halted as the Shasta County Bomb Squad's robot was used to move the pipe to Red Bluff River Park at the end of Willow Street. Hal's was closed temporarily as a precaution. The bomb itself was a black plastic pipe about six inches in length, sealed on both ends, and with an unlit fuse sticking out. It was destroyed shortly after noon when officers, using the robot, moved it to the edge of Red Bluff River Park and shot it with a clay, 12-gauge bullet, Shasta County sheriff's officer said. The bomb did not ignite when shot, but had been concealing a black powder, the officer said. Police did not have any suspects or leads as of Saturday afternoon.
Source: http://www.redbluffdailynews.com/news/ci_14165485

[Return to top]

National Monuments and Icons Sector

49. *January 12, Summit Daily News* – (Indiana) **Forest Service plans for fire mitigation near Breckenridge.** The U.S. Forest Service is gathering public input for a proposed fire-mitigation project in the Breckenridge area. Dillon Ranger District officials met with residents Saturday to answer questions and respond to concerns about the proposed logging. Through the Breckenridge Forest Health and Fuels Project, the Forest Service would conduct clear-cut and salvage logging on 5,700 acres of White River National Forest land affected by the pine-beetle epidemic between Farmer's Korner and Hoosier Pass. The project would include lands in the Golden Horseshoe area, Indiana Gulch and the area extending north from Peak 7. The project's main goal is to reduce fire danger along the "urban interface," where forest land abuts human development. The Forest Service estimates beetle-induced mortality of lodgepole pines in the area to be approaching 80 percent. Officials anticipate that 90 percent of the trees will die within the next three to five years.
Source:
http://www.summitdaily.com/article/20100112/NEWS/100119952/1078&ParentProfile=1055

[Return to top]

Dams Sector

50. *January 12, Monterey County Herald* – (California) **Deal struck to demolish San Clemente Dam.** The proposal to demolish San Clemente Dam and restore wildlife habitat on the Carmel River is gaining momentum. Numerous public officials joined executives of California American Water on Monday at Mission Ranch in Carmel to sign a declaration pledging their support for the project. The $84 million dam removal and river reroute could be the first project of its kind in the United States, officials said. The plan to demolish the dam and reroute the Carmel River through San Clemente Creek, leaving about 2.5 million cubic yards of sediment buildup in the reservoir, was revived in November. Cal Am, which owns the dam, said that about nine months earlier, it was changing course after being unable to reach an agreement with the California Coastal Conservancy and the National Oceanic and Atmospheric Administration concerning the project's long-term liabilities. The fear is the sediment could be released after the structure is removed.
Source: http://www.montereyherald.com/local/ci_14171079

[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 NICCReports@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