Daily Open Source Infrastructure Report 23 January 2012

Top Stories

- A monster Pacific Northwest storm brought much of Washington state to a standstill January 19, shutting down roads, railways, and airports, and knocking out power to hundreds of thousands. – *Associated Press* (See item **22**)
- A group of researchers found serious security holes in six top industrial control systems used in critical infrastructure and released exploit modules in the hopes they would be patched before they are attacked. – *Wired* (See item **44**)

Fast Jump Menu

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: LOW, Cyber: LOW
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) - [http://www.esisac.com]

1. *January 20, KSAT 12 San Antonio* – (Texas) **3 injured in oil well explosion.** An explosion at a fracking site south of Pearsall, Texas, injured three workers January 19. Just before 6 p.m., officials said the explosion knocked the top off one of an oil well, launching it 25 yards in the air. Heavy flames and black smoke could be seen from

miles away. Firefighters from Pearsall and Dilley used a combination of water and foam to attack the blaze. A spokesman said firefighters also monitored levels of hydrogen sulfide and were able to control the fire by 8 p.m. The extent of the three worker's injuries were unknown, but police said all three men were conscious and breathing when they were taken to the hospital. The cause of the explosion was unknown.
Source: http://www.ksat.com/news/3-injured-in-oil-well-explosion/-/478452/8397286/-/n1578uz/-/

2. *January 20, Associated Press* – (Washington; Oregon) **About 250,000 Washington customers without power.** A powerful Pacific Northwest storm knocked out power to about 250,000 electric customers around Seattle, Tacoma, and Olympia after it coated much of Washington in ice and swelled Oregon rivers, killing a child and two adults, the Associated Press reported January 20. Most of those affected were customers of Puget Sound Energy, which said it had restored service to 87,000 customers who lost power in the snowstorm that began January 18. But the utility said it could take into the weekend or later to get the power back on for the roughly quarter million additional homes and businesses still in the dark. The storm knocked down so many trees that Washington State Patrol troopers brought chainsaws in their cruisers to hack through the obstacles. More than 50 downed trees on railroad tracks and the threat of more falling forced Amtrak officials to close service between Portland and Seattle through January 20.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/01/20/national/a055959S16.DTL

3. *January 20, Reuters* – (Montana) **Exxon to pay Montana $2.4 million in spill accord.** Exxon Mobil Corp. would pay more than $2 million in penalties and cleanup costs to Montana for a pipeline rupture in July that spilled an estimated 1,500 barrels of oil into the Yellowstone River, according to a proposed legal settlement unveiled January 19. Under the negotiated agreement between Exxon and the Montana Department of Environmental Quality, the Texas-based oil company would pay a fine of $1.6 million, the largest penalty ever levied in Montana for violations of its water quality regulations. Exxon also would reimburse Montana $760,000 for state cleanup expenses and cover any future costs should the state incur them, according to the deal. The company originally put the size of the spill at 1,000 barrels of crude, but has since revised the volume of oil released into the river at 1,500 barrels, Montana environmental officials said. In addition, Exxon must still settle with the state for any damages assessed by the Montana attorney general under the state's natural resource laws, a spokesman said. The cause of the accident, which occurred amid historically high water levels on the pristine river, remains under investigation by the federal Pipeline and Hazardous Materials Safety Administration.
Source: http://www.reuters.com/article/2012/01/20/us-exxon-pipeline-montana-idUSTRE80J0AD20120120

4. *January 20, St. Paul Pioneer Press* – (Minnesota) **Marathon Petroleum fined $700,000 for St. Paul Park benzene release.** Marathon Petroleum Corp. was given a $700,000 civil penalty for failing to treat hazardous wastes properly at a suburban St.

Paul Park oil refinery it once owned in Minnesota. Marathon committed the violations at the plant over 4 months in 2010 before selling it to St. Paul Park Refining Co., the current owner and operator, according to the Minnesota Pollution Control Agency (MPCA). Under an agreement, Findlay, Ohio-based Marathon paid the penalty to settle violations that led to the release of benzene, a potent carcinogen, into the environment. The MPCA said Marathon failed to manage the hazardous waste properly off and on for 65 days from June 15 to October 16, 2010. During that period, the MPCA said, Marathon illegally disposed of 115 million gallons of benzene process wastewater in an unlined lagoon instead of treating it properly in its wastewater-treatment plant. Liquids in the lagoon, situated near the Mississippi River, can filter into shallow groundwater connected to the river.
Source: http://www.twincities.com/localnews/ci_19775952

5. *January 19, Pittsburgn Post-Gazette* – (Pennsylvania) **OHSA fines coal bed methane driller for dangerous job site.** A Smithton-based, gas drilling contractor has been cited for 16 safety violations and fined $53,200 by the Occupational Safety and Health Administration (OSHA) following an investigation spurred by a July job-site death, the Pittsburgh Post-Gazette reported January 19. Target Drilling Inc.'s coal bed methane drilling site in Greene County's Franklin Township, Pennsylvania, was found to have 14 serious violations. The serious violations included failures to protect cables entering electrical boxes, to cover electrical boxes, to properly ground electrical systems, and to ensure that a diesel fuel pump was adequate for damp and wet locations. Target has 15 business days to pay, ask for an informal conference with OSHA's area director, or contest the citations and penalties.
Source: http://www.post-gazette.com/pg/12019/1204627-100.stm

For more stories, see items **22** and **44**

[Return to top]

Chemical Industry Sector

6. *January 20, Safety.BLR.com* – (Ohio; National) **Safety board says fatal fire points to need for national code.** A fatal chemical fire at Heritage-WTI, Inc., a hazardous waste facility in East Liverpool, Ohio, has led to recommendations from the U.S. Chemical Safety Board (CSB), Safety.BLR.com reported January 20. On December 17, two workers were seriously burned, and one died. A flash fire occurred when workers were splitting a large solid waste drum of hazardous material into smaller storage drums. The CSB has made recommendations to the Environmental Technology Council (ETC), an industry trade group. One is to petition the National Fire Protection Association to issue a standard specific to hazardous waste treatment storage and disposal sites. The standard would provide guidance to prevent similar fires, explosions, and releases. The second recommendation to ETC is to develop a guidance document for members on safe processing, handling, and storage of hazardous waste. The CSB identified nearly two dozen other fire and chemical release incidents at haz-waste sites from 2002 to 2007.

Source: http://safety.blr.com/workplace-safety-news/hazardous-substances-and-materials/chemical-hazards/Safety-Board-Says-Fatal-Fire-Points-to-Need-for-Na/

7. *January 19, Springfield Republican* – (Massachusetts) **60-gallon chemical spill triggers haz-mat response at Solutia plant in Indian Orchard.** A spill involving 60 gallons of flammable chemicals at the Solutia compound in the Indian Orchard section of Springfield, Massachusetts, triggered a hazardous materials response from the Springfield Fire Department (SFD), officials said. An SFD spokesman said the spill, reported at 2:44 p.m. January 19, was contained inside a concrete holding basin. Workers were not evacuated. The spill involved a mixture of ethanol, butanol, and formaldehyde. The mixture was diluted with water until it was no longer flammable and then pumped into another tank. The spill was at the Solutia property but it involved employees with Ineos Melamines, a separate firm also located at the site. Officials said the state department of environmental protection was contacted. Employees were relining a 20,000-gallon tank when they discovered a gasket was leaking. The tank had about 5,000 gallons of the chemical in it, a company official said. Workers drained the tank to bring the fluid level below the leak.
Source: http://www.masslive.com/news/index.ssf/2012/01/60-gallon_chemical_spill_trigg.html

8. *January 19, Arizona Republic* – (Nevada) **Truck with hazardous chemicals rolls on I-10 west of Phoenix.** A semitruck carrying boxes of chlorine rolled over, forcing the closure of Interstate 10 in both directions about 10 miles west of Tonopah, Arizona, January 19. Westbound Interstate 10 has since reopened, according to the state department of public safety. The freeway was expected to remain closed eastbound at Milepost 81 until 5 p.m., according to the Arizona Department of Transportation. The semitruck was leaking fuel. The double trailer and tractor were tipped on their side blocking both eastbound lanes on the I-10.
Source: http://tucsoncitizen.com/arizona-news/2012/01/19/truck-with-hazardous-chemicals-rolls-on-i-10-west-of-phoenix/

9. *January 19, WSFA 12 Montgomery* – (Alabama) **Nitrous Oxide tanker accident shuts down lane of I-65.** Local authorities asked motorists to use caution when traveling on I-65 in Lowndes County, Alabama, near mile marker 144.5 after a tractor trailer carrying Nitrous Oxide collided with a dump truck. The Lowndes County EMA director said one northbound lane of I-65 at the 144 mile marker was shut down for a short time while crews attempted to remove the tanker carrying Nitrous Oxide, which is flammable. He said crews would also have to clean up about 50 gallons of diesel fuel spilled on the roadway.
Source: http://lowndescounty.wsfa.com/news/news/137079-nitrous-oxide-tanker-accident-shuts-down-lane-i-65

For more stories, see items **4** and **44**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

10. *January 20, Chattanooga Times Free Press* – (Tennessee) **TVA orders unpaid safety work stoppage at Watts Bar Nuclear Plant.** The Tennessee Valley Authority (TVA) ordered an unpaid safety work stoppage at Watts Bar Nuclear Plant in Spring City, Tennessee, for about 1,000 contract workers after finding cables had been erroneously removed from Unit 1 — the operating reactor — in December, the Chattanooga Times Free Press reported January 20. The week of January 9, a valve in Unit 2, the reactor now under construction at the plant, also was removed from another system without workers following proper guidelines. The TVA's senior vice president for nuclear generation, development, and construction ordered the stoppage — known as a "stand-down" — to start at noon January 18 "until the errors discovered are clearly communicated to all personnel," along with the TVA's demand for quality work, according to a TVA spokeswoman. She said the safety of the public was at no time put at risk.
    Source: http://timesfreepress.com/news/2012/jan/20/tva-orders-unpaid-safety-work-stoppage-watts-bar-n/

11. *January 20, VTDigger.org* – (Vermont) **Judge rules against state, says Entergy can continue to operate Vermont Yankee.** A U.S. district court judge ruled Entergy can continue to operate the Vermont Yankee Nuclear Power Plant in Vernon, Vermont, past a March 21 state-mandated shut down date, the VTDigger.org reported January 20. In the decision, the judge struck down several state laws, one of which (Act 160) prohibits the Louisiana-based corporation from running the aging nuclear plant beyond its current 40-year license without legislative approval. The other (Act 74) requires Entergy to obtain permission from the general assembly to store high level nuclear waste at the site. In February 2010, the state senate voted to deny Entergy an opportunity to seek a 20-year renewal of its license to operate Vermont Yankee from the public service board. The judge wrote the Atomic Energy Act preempts Vermont law. Consequently, the state cannot bring an enforcement action against Entergy, he wrote.
    Source: http://vtdigger.org/2012/01/20/judge-rules-against-state-says-entergy-can-continue-to-operate-vermont-yankee/

12. *January 20, Mainichi Daily News* – (International) **TEPCO left backup power for nuclear data equipment detached for 4 months.** Tokyo Electric Power Co. (TEPCO) left the backup power source of a reactor-monitoring device at Japan's Fukushima Nuclear Power Plant disconnected for 4 months until the March 2011 earthquake and tsunami triggered a disaster at the plant, the Mainichi Daily News reported January 20. Failure to connect the backup source is said to have prevented data on the status of the plant being sent to the government for about 2 hours after the outbreak of the crisis. It is believed this may have affected the initial response to the disaster and the predictions on the spread of radioactive materials. TEPCO officials said workers tried to connect the backup power supply to the media converter during renewal work in November 2010, but the cable was too short so it was left disconnected.
    Source: http://mdn.mainichi.jp/mdnnews/news/20120120p2a00m0na008000c.html

For another story, see item **44**

[Return to top]

Critical Manufacturing Sector

13. *January 20, U.S. Department of Transportation* – (National) **NHTSA Safety Recall - Kia Optima and Kia Rondo.** Kia Motors America, Inc., announced the recall January 20 of 145,755 model year 2006-2008 Kia Optima and model year 2007 and 2008 Kia Rondo vehicles. The clock spring contact assembly for the driver's side air bag supplemental restraint system (SRS) may become damaged through usage over time. If the clock spring contact assembly becomes damaged, the driver's side air bag electrical circuit will experience a high resistance condition potentially causing the driver's air bag to not deploy. If the clock spring develops high resistance, in the event of a crash, the driver's air bag will not deploy and will not be able to properly protect the driver, increasing the risk of injuries. Kia will notify owners, and dealers will replace the vehicle's air bag clock spring contact assembly as necessary. The safety recall is expected to begin during March.
Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V014000&summary=true&prod_id=288668&PrintVersion=YES

14. *January 19, Northwest Indiana Times* – (Indiana) **Dust catcher system malfunction causes problems for U.S. Steel.** United States Steel Corp. had to repair a key piece of environmental equipment tied to one of its Gary, Indiana blast furnaces the week of January 9 after a malfunction that reduced steel production levels for a few days, the Northwest Indiana Times reported January 19. A dust collection system for the No. 4 blast furnace failed January 7 and required maintenance before normal pig iron production resumed January 11, according to the deputy director for the Indiana Department of Environmental Management's Northwest Regional Office. He said there were no emissions exceedances to trigger a permit violation, but production was shut down for safety reasons because of high carbon monoxide concentrations.
Source: http://www.nwitimes.com/business/local/dust-catcher-system-malfunction-causes-problems-for-u-s-steel/article_b803f1b9-fe0d-5a15-b165-b87f546340a3.html

For another story, see item **44**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

15. *January 20, Associated Press* – (Texas) **Dallas: conviction over $14M investment scheme.** A federal jury in Dallas has convicted a man of deceiving more than 200 people in a $14 million investment scheme, federal prosecutors announced January 19. He was convicted of seven counts of wire fraud and one count of securities fraud. Prosecutors said the man tricked investors into putting money into a company he created called Sardaukar Holdings. Investigators said he then squandered most of the money on cars, entertainment, and jewelry. Each count of wire fraud carries a maximum sentence of 20 years in prison and a $250,000 fine. The securities fraud count carries a maximum sentence of 5 years in prison and a $250,000 fine.
Source: http://www.chron.com/news/article/Dallas-conviction-over-14M-investment-scheme-2643601.php

16. *January 20, Fort Collins Coloradoan* – (Colorado) **Windsor man guilty of securities fraud.** A jury January 19 convicted a former Windsor, Colorado investment adviser on securities fraud and theft charges in connection with what prosecutors said was a $5.7 million scam with dozens of Fort Collins-area victims. He was convicted on six of the seven felony counts he faced. He remains free on bond pending his sentencing in a case that prosecutors said victimized more than 70 people. He was convicted on four counts of securities fraud, one count of securities fraud as a course of business, and one count of theft. He was acquitted on one count of securities fraud. The U.S. Securities and Exchange Commission, also is seeking a $10 million fine on behalf of 64 investors, many of whom lost their life savings. An assistant attorney general said in trial the adviser told investors their money would remain safe, but instead it was used either to fund risky schemes or pay back earlier investors. Each charge against the adviser is a Class 3 felony punishable by 4 to 12 years in prison and fines up to $750,000. The adviser's two former co-defendants each pleaded guilty to securities fraud in March and received 1-year deferred sentences. As part of the sentences, they agreed to pay about $1.2 million in restitution.
Source: http://www.coloradoan.com/article/20120120/NEWS01/201200330/Windsor-Man-guilty-securities-fraud?odyssey=mod|newswell|text|News|s

17. *January 20, Associated Press* – (International) **Feds shut down popular file-sharing website Megaupload.** One of the world's most popular file-sharing sites was shut down January 19, and its founder and several company officials were accused of facilitating millions of illegal downloads of films, music, and other content. A federal indictment accused Megaupload.com of costing copyright holders at least $500 million in lost revenue. Megaupload is based in Hong Kong, but some of the alleged pirated content was hosted on leased servers in Ashburn, Virginia, which gave federal authorities jurisdiction, the indictment said. The Justice Department said in a statement that Megaupload's founder and three other employees were arrested January 19 in New Zealand at the request of U.S. officials. Three other defendants are at large. The indictment said Megaupload was estimated at one point to be the 13th most frequently visited Web site on the Internet. Current estimates by companies that monitor Web traffic place it in the top 100. The five-count indictment, which alleges copyright infringement, as well as conspiracy to commit money laundering and racketeering,

described a site designed to reward users who uploaded pirated content for sharing, and turned a blind eye to requests from copyright holders to remove copyright-protected files. For instance, users received cash bonuses if they uploaded content popular enough to generate massive numbers of downloads, the indictment said. Such content was almost always copyright protected. The site boasted 150 million registered users and about 50 million hits daily. Megaupload is considered a "cyberlocker," in which users can upload and transfer files too large to send by e-mail. The Web site allowed users to download content for free, but made money by charging subscriptions to people who wanted access to faster download speeds or extra content. The Web site also sold advertising. Several sister sites were also shut down, including one dedicated to sharing pornography files.
Source: http://www.msnbc.msn.com/id/46070076/ns/technology_and_science-tech_and_gadgets/#.TxmmEYH-5YR

18. *January 19, Orange County Register* – (California) **Another 'Market Duo Bandit' arrested, police say.** A man suspected of being one of the "Market Duo Bandits" was arrested in California January 18, nearly 2 weeks after another suspected member of the robbery team was shot by a deputy at the end of a high-speed pursuit. The suspect was arrested in a traffic stop near his La Mirada home after La Habra detectives and FBI Robbery Task Force members identified him as a suspected member of a group believed to be tied to at least five Orange County bank robberies, a police spokeswoman said. The "Market Duo Bandits," believed to have struck in La Habra, Seal Beach, Lake Forest, and Placentia, earned their nickname for targeting bank branches in supermarkets. The last holdup took place January 5, when the two returned to a Wells Fargo in a Stater Bros. market on Imperial Highway that police say they had previously robbed. A Brea police officer saw the robbers leaving the scene and a freeway chase ensued. The two fled from the vehicle in Paramount. A deputy confronted and shot one of the men. FBI officials say a third suspect was arrested several days after the shooting.
Source: http://www.ocregister.com/news/market-336328-duo-police.html

19. *January 19, Minneapolis Star Tribune* – (Minnesota) **More plead guilty to Cloud 9 fraud scheme.** Two real estate professionals have pleaded guilty in connection with kickbacks at the troubled Cloud 9 Sky Flats development in Minnetonka, Minnesota, a scheme prosecutors say defrauded lenders out of $7 million to $20 million. The pair pleaded guilty in federal court January 18 to conspiracy to commit mail and wire fraud. They face a maximum of 20 years in prison. One defendant was the owner and loan officer of the mortgage brokerage company Team Access. The other defendant owned the business Trend Title and closed residential real estate transactions. The pair admitted that from 2007 to 2008, they obtained mortgage loan proceeds under false pretenses on behalf of home buyers associated with an unnamed investment group. The owner of Team Access admitted he lied on those applications, including inflating incomes of buyers and failing to disclose that buyers would receive cash kickbacks from mortgage loan proceeds. He secured loans for the purchase of about 108 properties in all. The owner of Trend Title admitted she closed about 88 fraudulent transactions for the investment group, concealing from mortgage lenders that the purchasers got kickbacks from mortgage loan proceeds and that the buyers were often

not the source of the "cash to close." The kickbacks were disguised as prepaid management fees and facilitator fees. She also closed eight to 10 transactions involving undisclosed Cloud 9 buyers. Four others have already pleaded guilty in the scheme. The number of condo units involved in the overall kickback arrangement has topped 100 at Cloud 9 and elsewhere. Kickbacks from the loan proceeds exceeded $8 million, according to federal prosecutors.
Source: http://www.startribune.com/business/137678373.html

20. *January 19, Berkshire Eagle* – (Massachusetts; National; International) **Fraudulent buys made with stolen debit, credit card info.** Fraudulent purchases have been made with dozens of people's debit and credit card information because sales records were stolen from a local retail business in the Pittsfield, Massachusetts area, the Berkshire Eagle reported January 19. Because the breach sprang from a retailer, it is impacting a host of local and regional banks whose customers shopped at the store over the last 2 months. Information from hundreds of debit and credit cards may have been obtained by those who stole the retailer's records, though the number of customers whose data was used to make purchases is much less. At Greylock Federal Credit Union, purchases were made with information from 19 cards. The data obtained from the retailer was used to make impostor credit or debit cards, according to bank officials. Great Barrington police are investigating. The vice president of retail banking and marketing for the Pittsfield Cooperative Bank said his office became aware of the problem late the week of January 9 with fraudulent purchases being made in Canada, specifically at pharmacies and gas stations. It later spread to the United States, in places such as New Jersey and Florida. Berkshire Bank and Greylock have not sent out blanket notifications to customers, but they are working with individuals directly affected. Information from as many as 70 cards from Pittsfield Cooperative may have been compromised.
Source: http://www.berkshireeagle.com/ci_19777441?source=most_viewed

21. *January 19, PC Magazine* – (International) **Israeli hackers target UAE, Arab Bank sites.** In the wake of recent hacks that targeted Israeli Web sites, a group known as IDF Team January 19 went after the Web sites for two major Arab banks. As of 1:30 p.m. Eastern Time, the Web sites for the Central Bank of the United Arab Emirates and Arab Bank were both offline. In a note posted to Pastebin, IDF Team said its attacks were in retaliation for a January 18 hack of Israel's Anti-Drug Authority Web site, which IDF called terrorist activity and "attempts to disrupt the normal course of life in Israel." If the attacks on Israeli sites don't stop, IDF Team pledged to also target stock market and government Web sites, such as the Arab Emirates Web portal at government.ae, as well as "sites related to the country's economy and even security." According to the Financial Times, the January 19 bank attacks were likely distributed denial of service (DDoS) attacks.
Source: http://www.pcmag.com/article2/0,2817,2399095,00.asp

For another story, see item **34**

[Return to top]

Transportation Sector

22. *January 20, Associated Press* – (Washington; Oregon) **Deadly storm grips Northwest in ice, snow.** A monster Pacific Northwest storm coated the Seattle area in a thick layer of ice January 19 and brought much of the state to a standstill, sending hundreds of cars spinning out of control, temporarily shutting down the airport and knocking down so many trees that members of the Washington State Patrol brought chain saws to work. Amtrak suspended train service January 19 between Seattle and Portland, Oregon. Officials in Spokane declared a snow emergency, banning parking along arterials and bus routes beginning that evening. Freezing rain and ice pellets caused numerous accidents in the Seattle area. The state patrol said it had responded to about 2,300 accidents in a 24-hour period ending at 9 a.m. January 19. The state transportation department closed one highway because of falling trees that also took out power lines. Ice closed Sea-Tac Airport completely in the early morning before one runway was reopened. Washington's governor declared a state of emergency, authorizing the use of National Guard troops if necessary. Authorities also worried about flooding in the coming days as temperatures warm up.
Source: http://www.google.com/hostednews/ap/article/ALeqM5iEUQVqCD98ykHu-Vf3YULsam3qOg?docId=162906a20f5d4087827020f92f749b55

23. *January 20, St. Louis Post-Dispatch* – (Missouri) **School bus thefts mystify police in Jefferson and St. Louis counties.** At least one full-size regulation school bus has disappeared each month since September — plus one in May — from five locations in south St. Louis County or Jefferson County, Missouri. "It's not your usual stolen vehicle," said a sergeant with the St. Louis County police auto crime unit. "Most vehicles come up recovered, and not having these school buses surface anywhere is unusual too." The FBI was notified. Officials said that new, each bus is worth about $60,000. Exactly when these were stolen is hard to pinpoint because they went missing on weekends or when school was otherwise not in session. The most recent theft is so far the only one at least partially caught on video. In that case, Jefferson County deputies believe the thieves used bolt cutters to sever chains securing the gates and then fastened them again with new padlocks.
Source: http://www.stltoday.com/news/local/crime-and-courts/series-of-school-bus-thefts-mystifies-police-in-jefferson-st/article_49fd3268-f123-54e8-95c3-c01b3a69a749.html

24. *January 19, Associated Press* – (California) **Man charged in S.F. subway SUV ride incident.** A man was arrested on suspicion of driving under the influence January 19 over allegations he shut down San Francisco's subway system for more than 2 hours after driving his SUV onto the underground tracks, police said. He also has been charged with driving on train tracks and failure to obey a traffic sign. His vehicle entered a tunnel on Church Street shortly before 6 a.m. and traveled eastward almost to the Van Ness Station, said a spokesman for the city's Municipal Transportation Agency. A municipal manager said he saw the SUV going about 40 mph into the tunnel and chased it down. All underground train lines were shut down during the morning commute while crews removed the vehicle and inspected the system. Trains resumed service by 8:15 a.m. Some damage was done to the tracks, but crews planned to make

repairs with trains moving slower through the affected area.
Source: http://www.cbsnews.com/8301-201_162-57362493/man-charged-in-s.f-subway-suv-ride-incident/

25. *January 19, Molokai Dispatch* – (Hawaii) **Security measures planned for ship's visit.** The U.S. Coast Guard will be establishing a temporary security zone at Kaunakakai Harbor as the 36-passenger vessel, the Safari Explorer, resumes docking at the wharf January 21. The security zone will be enforced 1 hour prior to the vessel's arrival and departure to the harbor, for the protection of "people, vessels and facilities in and around Kaunakakai Harbor during potential non-compliant protests involving the ... Safari Explorer," according to Docket No. USCG–2011–1159, published in the January 13 issue of the Federal Register. The rule is effective January 19, 2012 through May 15, 2012. Citing protesters who blocked the entrance to the wharf November 26 on small boats and surfboards, the security zone regulation seeks to ensure the safety of all involved during future port calls.
Source: http://themolokaidispatch.com/security-measures-planned-ship-s-visit

26. *January 19, Journal of Commerce* – (Louisiana) **Army Corps to fix Mississippi River-Gulf chokepoint.** The U.S. Army Corps of Engineers will begin clearing a chokepoint at the mouth of the Mississippi River that has restricted cargo shipments from the Midwest since last spring. The Corps will get an additional $55 million from a disaster relief bill to dredge the river between New Orleans and the Gulf of Mexico to its authorized 45-foot depth and 750-foot width, the Port of New Orleans said January 19. The project is part of the Corps' overall maintenance dredging budget of $1.72 billion. Port officials said the river has never fully recovered from the effect of massive flooding in the Midwest that scoured some 19.6 million square feet of topsoil and dumped them at the mouth of the river. The reduction in vessel draft to 46 feet forced ships to carry less cargo and cost carriers nearly $600,000 per trip.
Source: http://www.joc.com/portsterminals/army-corps-fix-port-new-orleans-chokepoint

For more stories, see items **2**, **3**, **8**, **9**, **32**, **41**, and **44**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

27. *January 20, KTLA 5 Los Angeles* – (California) **'Fast food bandit' wanted in series of holdups.** The Los Angeles Police Department's (LAPD) northeast division detectives are looking for a "fast food bandit" whom they believe is responsible for a rash of holdups at fast food restaurants, KTLA 5 Los Angeles reported January 20. Over the

past few weeks, the robber hit six different fast food restaurants and one Radio Shack, and the pattern of his behavior has been consistent. “This individual is quick,” said an LAPD detective. “He goes in, and either simulates a handgun or is armed with a handgun. He asks for cash, then quickly walks out.” The robberies occurred in the Lincoln Heights and Cypress Park areas among others, generally at establishments in close proximity to the 110 Freeway. Most occurred in the 4 p.m. to 10 p.m. time period — a concern to detectives because that is commonly when families might be dining at the restaurants and could be vulnerable to harm. In one instance, the suspect kicked restaurant employees, indicating to police he is brazen and dangerous.
Source: http://www.ktla.com/news/landing/ktla-fast-food-robber-silver-lake,0,56749.story?track=rss

28. *January 20, Food Safety News* – (National) **CDC mum about fast-food chain in Salmonella outbreak.** Salmonella Enteritidis infections centered in Texas and Oklahoma, but also spread over 8 other states, sickened 68 people who ate at a Mexican-style fast food restaurant chain in October and November 2011, the Centers for Disease Control and Prevention (CDC) reported January 19. The CDC did not identify the restaurant chain, nor did it explain why it was reporting this outbreak for the first time now, nearly 2 months after it occurred. The investigation report was labeled “final update,” although it was also the first announcement of the multi-state outbreak. No specific food or ingredient was determined to be responsible for the illnesses. The CDC said investigators concluded that whatever the food source was, it likely was contaminated before it reached the fast-food restaurant outlets.
Source: http://www.foodsafetynews.com/2012/01/cdc-mum-about-fast-food-mexican-chain-in-salmonella-outbreak/

29. *January 20, Food Safety News* – (Southeast) **Winn-Dixie, Leasa recall sprouts.** After Leasa Industries of Miami announced it was recalling 346 cases of its alfalfa sprouts because they might be contaminated with Salmonella, the Winn-Dixie Stores chain said it was removing all Leasa-branded sprouts from its shelves, Food Safety News reported January 20. Routine sample testing January 9 revealed the presence of Salmonella in the alfalfa sprouts, Leasa said in its recall notice. The company said it is working with the Florida Department of Agriculture and the U.S. Food and Drug Administration to investigate the problem. The recalled sprouts were distributed in Florida, Georgia, Alabama, Louisiana, and Mississippi through retail stores and food service companies from January 4 though January 8.
Source: http://www.foodsafetynews.com/2012/01/winn-dixie-leasa-recall-sprouts/

30. *January 20, Mobile Press-Register* – (National; International) **Cheese sold by Mediterranean specialty markets recalled for listeria contamination.** Kradjian Imp Co, of Glendale, California, is recalling Cedar Tree brand Tresse Cheese and Cedar Tree brand Shinglish cheese because they have the potential to be contaminated with Listeria monocytogenes, the Mobile Press-Register reported January 20. The cheese was distributed in California, Washington, Minnesota, Nevada, Oklahoma, Texas, Tennessee, Arizona, and Michigan to Mediterranean specialty markets. Both cheese were manufactured by Fromagerie Marie Kade in Quebec, Canada.
Source: http://blog.al.com/live/2012/01/cheese_sold_by_mediterranean_s.html

For another story, see item **44**

[Return to top]

Water Sector

31. *January 19, Reuters* – (Pennsylvania) **EPA to test water near Penn. fracking site.** Regulators at the U.S. Environmental Protection Agency (EPA) said January 19 they will perform water tests at about 60 homes in Dimock, Pennsylvania where residents say natural gas drilling has polluted wells. The EPA also plans to truck water to four homes in the town where some households have relied on water deliveries since drilling by Cabot Oil & Gas Corp began 3 years ago, it said in a statement. The tests, which will begin in the coming days, are being carried out "to further assess whether any residents are being exposed to hazardous substances that cause health concerns," the agency said. The announcement represents a reversal for the EPA, which 6 weeks ago declared the water in the 1,400-person town safe to drink before receiving more data provided by residents. It is also the clearest sign yet regulators are concerned about the effect of drilling on drinking water there. A Cabot spokesman said the company has tested and sampled water from more than 2,000 wells in the area over the past several years and does not have data showing drilling is the cause of "alleged health concerns purported by the EPA." Dimock residents began complaining of cloudy, foul-smelling water in 2008 after Cabot began fracking nearby. The company trucked water to a dozen Dimock households for 3 years until November when state regulators agreed it could stop. Since then, residents have relied on water deliveries arranged by environmental groups including Water Defense and Sierra Club, though the sporadic deliveries have barely been enough. Some have been using pond water for showers.
Source: http://www.reuters.com/article/2012/01/20/us-usa-fracking-pennsylvania-idUSTRE80I29A20120120

32. *January 19, Bloomington-Normal Pantagraph* – (Illinois) **City: Water main break caused sinkhole that snared Dist. 87 school bus.** A sinkhole that trapped a school bus carrying 13 children in Bloomington, Illinois, January 18 was caused by a water main break. It was the city's eighth in less than 3 weeks and the third on West Oakland Avenue in that same period. City crews patched the water main that night. However, in examining the hole created by the leaking water, the city discovered it may have another problem with a sewer pipe buried about 2 feet below the water main, the deputy city manager said. She said the city would continue to examine the sewer pipe but expects to have the road open to through traffic again by January 27. Though the frequency of water main breaks typically increases in winter months, this winter's mild temperatures rule out weather as a major contributing factor, the manager added. The most recent break adds to the city's tally that already this year is nearly half of the 17 main breaks seen in all of 2011 –- a jump compared to the eight to 13 seen each year from 2007 to 2010. The city does not perform routine inspections of its water pipes because the buried system — which cannot be scanned from the inside by video without contaminating drinking water — is difficult to inspect.
Source: http://www.pantagraph.com/news/local/city-water-main-break-caused-sinkhole-that-snared-bus/article_b737e06c-4307-11e1-8a47-0019bb2963f4.html

For more stories, see items **3**, **4**, and **44**

[Return to top]

Public Health and Healthcare Sector

33. *January 19, KSPR 33 Springfield* – (Missouri) **Fire Marshal: Woman charged with setting a fire inside Cox North Hospital claims she was fighting terrorism.** A Springfield, Missouri woman is charged with arson, accused of setting a fire inside Cox North Hospital. According to court documents, she told investigators she set the fire in retaliation for "the hospital placing nanobots inside her body." An investigator said she also claimed to be "fighting terrorism." According to court documents, she admitted starting the fire and described how she set it using an accelerant.
Source: http://articles.kspr.com/2012-01-19/fire-marshal_30645368

34. *January 19, KMSP 9 Minneapolis/Saint Paul* – (Minnesota) **Minn. debt collector had medical records on stolen laptop.** The Minnesota attorney general filed a lawsuit January 17 against a debt collector accused of failing to protect the confidential information of 23,500 hospital patients after a company laptop was stolen from a rental car parked in the Seven Corners area of Minneapolis. The lawsuit alleges Accretive Health, Inc. failed to protect the confidentiality of patient health care records, and failed to disclose its involvement in their health care. The two affected Minnesota hospital systems are Fairview Health Services and North Memorial Health Care. The lawsuit alleges Accretive gained access to sensitive patient data through contracts with the hospitals and numerically scored patients' risk of hospitalization and medical complexity, graded their "frailty," compiled per-patient profit and loss reports, and identified patients deemed to be "outliers." The lawsuit includes a screenshot Fairview sent to a Minnesota patient who requested to know what data of theirs was on the stolen laptop. The screen shot has personal identity information, including name, address, date of birth, and Social Security number. It also includes a checklist to denote whether the patient has 22 different chronic medical conditions. The lawsuit also asks Accretive to disclose whether it has sent health data about Minnesota patients to its "Shared Services Blended Shore Center of Excellence" in India. The lawsuit further seeks an injunction that restricts how Accretive treats and uses patient data going forward, and to hold Accretive accountable for its violations of state and federal health privacy laws, debt collection laws, and consumer fraud laws.
Source: http://www.myfoxtwincities.com/dpp/news/stolen-laptop-debt-collector-lawsuit-jan-19-2012

For another story, see item **37**

[Return to top]

Government Facilities Sector

35. *January 20, USA Today; Associated Press* – (International) **FBI probes breach of Justice Website tied to Megaupload case.** Federal authorities said they were

investigating disruptions to the U.S. Department of Justice (DOJ) Web site and threats to the site maintained by the FBI believed to be prompted by the arrests of four suspects as part of an Internet piracy investigation, USA Today and the Associated Press reported January 20. The DOJ site was back online January 20 after being hit January 19, shortly after the agency accused Megaupload.com of costing copyright holders more than $500 million in lost revenue from pirated films, music, and other content. Before federal authorities shut down Megaupload.com, one of the world's most popular file-sharing sites, a statement was posted saying the allegations were "grotesquely overblown." A short time later, an alliance of hackers known as "Anonymous" claimed credit for attacks on the DOJ site. In a written statement, the DOJ said its Web server experienced a "significant increase in activity, resulting in a degradation in service. The department is working to ensure the website is available while we investigate the origins of this activity, which is being treated as a malicious act until we can fully identify the root cause of the disruption."
Source: http://www.usatoday.com/tech/news/story/2012-01-20/megaupload-arrests-FBI/52697186/1

36. *January 19, Nextgov* – (International) **A 2006 cyber breach may have impaired Symantec's government customers.** Revelations that hackers stole the master keys to Symantec's antivirus programs in 2006 suggest the firm's former federal customers and current remote access users may be dealing with vulnerable software. Reuters reported January 17 that earlier in January, hackers released some of the source code and planned to release more, although it was not clear why they were doing this 6 years after the theft, the news service said. The maker of popular computer security products disclosed intruders obtained the source code — the underpinnings of software — for Norton Antivirus Corporate Edition, which was used by government agencies. Of the compromised offerings, only pcAnywhere, which is not suited for organization-wide use, is still on the market. The tool allows one computer to remotely control another computer. The Defense and Veterans Affairs departments have solicited pcAnywhere products, according to the government procurement Web site FedBizOpps.gov. The Defense, Veterans Affairs, Commerce, Homeland Security, and State departments, along with the General Services Administration, all purchased Symantec items since January 2006, the site states.
Source: http://www.nextgov.com/nextgov/ng_20120119_8488.php

37. *January 19, Nextgov* – (International) **Software upgrade knocks out Defense health record system.** The Military Health System (MHS) shut down the Armed Forces Health Longitudinal Technology Application (AHLTA) clinical data repository (CDR) — which stores 9.7 million electronic records for active-duty and retired military personnel and their families — after experiencing problems with a commercial software package that manages data storage, a top MHS official told Nextgov January 19. This shutdown, in turn, forced military clinicians to use the AHLTA electronic health record system in "local mode," without access to the main record database. The AHLTA repository was taken offline January 17 and was restored about 10 hours later, according the MHS program executive officer for Joint Medical Information Systems. She said the CDR was taken offline "in order to correct a problem with a version upgrade to storage services that was loaded over the weekend," which included January

16. She did not identify the commercial software package. AHLTA supports 77,000 clinical users in 63 military hospitals, 413 clinics, 15 deployed hospitals, and 63 Navy ships.
Source: http://www.nextgov.com/nextgov/ng_20120119_5458.php

38. *January 19, Arizona Republic News* – (Arizona; International) **ASU system back online after breach.** Arizona State University (ASU) restored service at its online computer system January 19 after shutting it down the day before because of a security breach. January 18, ASU students and employees were told in a security text alert that the university's ASURITE system may have been compromised and all online services were suspended. ASURITE is the university's main online system, where students and employees log in with passwords and access classes and other services. There are more 300,000 accounts on the system. ASU officials said an encrypted file containing user names and passwords was downloaded January 18 by an unknown person outside the school. There is no evidence any data was compromised, but all online services were shut down as a precaution. An ASU spokeswoman said no private information, such as Social Security numbers or bank accounts, was available in the file.
Source: http://tucsoncitizen.com/arizona-news/2012/01/19/asu-system-back-online-after-breach/

For more stories, see items **2** and **47**

[Return to top]

Emergency Services Sector

39. *January 20, Associated Press* – (Virginia) **Va. tech agency falters, leaving State Police network down for 5 hours.** A network outage crippled Virginia State Police for 5 hours January 19, leaving the force unable to perform background checks, run fingerprints, or register sex offenders. State police reported the problem to the Virginia Information Technologies Agency (VITA) around 1:30 p.m., a spokeswoman said. The network remained down until around 6:30 p.m., when most features were restored. In the meantime, troopers did not know if the person they pulled over was wanted by police, if the car was stolen, or if the person was a known criminal. It also meant those who went to purchase firearms were turned away because dealers could not perform the necessary background checks. It is the latest in series of periodic outages and snafus involving the state's computer system, which is run by the VITA through a 10-year, $2.4 billion contract with Northrop Grumman Corp.
Source: http://www.newsleader.com/article/20120120/NEWS01/120120001/Va-tech-agency-falters-leaving-State-Police-network-down-5-hours

40. *January 20, Lorain Morning Journal* – (Ohio; New York; Michigan) **Suspected hoax prompts Coast Guard search.** The U.S. Coast Guard (USCG) was investigating a suspected hoax that launched a 2-hour search and rescue operation near the shores of Avon Lake, Ohio. The USCG received about 11 Mayday calls on a radio distress channel about 3 a.m. January 19. Coast Guard Sector Buffalo, New York, issued an urgent marine information broadcast asking area boaters to respond if anyone saw

anything. The man believed to be sending the distress calls was then heard blowing in to the radio, repeating the broadcast information broadcast and "not sounding like a person who was in actual distress," according to a USCG petty officer. Despite this, the Guard dispatched a 25-foot rescue boat from Cleveland and a Dolphin helicopter from Air Station Detroit. The search location was narrowed to a half mile off Avon Lake by obtaining a line of bearing from the distress calls' signal hitting radio towers. "They weren't able to find anybody," the petty officer said. The helicopter was called off when it decided the call was bogus. The USCG canceled the search around 5:30 a.m.
Source: http://morningjournal.com/articles/2012/01/20/news/doc4f18ec542d54e755959947.txt?viewmode=fullstory

41. *January 20, Fort Wayne News-Sentinel* – (Indiana) **Fatal crash, wrecked meth truck close parts of I-69.** Hazardous road conditions kept Indiana State Police (ISP) and emergency crews busy for much of January 19, with at least two wrecks, including a fatality, closing portions of Interstate 69 for hours. A crash killed one person and blocked the southbound lanes of I-69 near the 83 mile marker in Huntington County, according to an ISP spokesman. Police expected a lengthy closure, and southbound traffic was being diverted to U.S. 224 at the 86 mile marker while emergency crews worked. Early January 19, a northbound truck carrying methamphetamine-related chemicals slid through the median near the 99 mile marker, closing the southbound lanes for more than 3 hours. The truck belonged to Summitt Environmental, a Michigan company used by state police to transport and dispose of chemicals that have been seized in meth raids. The driver of the truck was transported to Lutheran Hospital but was not hurt badly, the ISP spokesman said. Traffic could not start moving until a backup truck arrived to take the spilled chemicals. However, he said none of the chemicals presented a serious hazard.
Source: http://www.news-sentinel.com/apps/pbcs.dll/article?AID=/20120119/NEWS/120119482/-1/LIVING

42. *January 19, WCSC 5 Charleston* – (South Carolina) **Perimeter secure at Lieber prison; Facility still locked down.** Nearly 200 law enforcement officers who were guarding the perimeter of Lieber Correctional Institute in Ridgeville, South Carolina for 10 hours had left their post by the morning of January 19. Officials said the perimeter was secure, but the prison remained on lockdown January 19 after inmates started a riot inside the facility. According to a Department of Corrections spokesman, two correctional officers were overpowered by some inmates who were able to take away the officer's keys and radios. The spokesman said it is believed that one officer was released by the inmates. One officer was taken to the hospital for stitches late January 18, and the second was treated at the scene. None of the injuries are life threatening. Authorities said the inmates were loose in the Ashley A Dorm of Lieber, which houses more than 200 inmates. The inmates were gassed for about an hour before riot police entered the building. At one point there were about 200 outside law enforcement officers at the prison.
Source: http://www.wmbfnews.com/story/16550900/lieber-correctional-institute-on-lockdown

43. *January 18, Coos Bay World* – (Oregon) **Douglas County 911 system experiencing problems.** The Douglas County, Oregon 911 center experienced an outage January 18, making it difficult for some residents to dial 911 across the county. The Douglas County Sheriff's Department urged citizens to go to their local police or fire department for help. Problems were mainly occurring with land lines, and the sheriff's office said 911 should be able to be reached with a cell phone. Officials mid-morning January 18 they did not have an estimate of when the system would be functioning normally.
Source: http://theworldlink.com/news/local/douglas-county-system-experiencing-problems/article_2b713e1a-4204-11e1-af19-001871e3ce6c.html

For more stories, see items **2**, **6**, **22**, and **49**

[Return to top]

Information Technology Sector

44. *January 19, Wired* – (International) **Hoping to teach a lesson, researchers release exploits for critical infrastructure software.** A group of researchers discovered serious security holes in six top industrial control systems used in critical infrastructure and manufacturing facilities and, thanks to exploit modules they released January 19, have also made it easy for hackers to attack the systems before they are patched or taken offline. The vulnerabilities were found in widely used programmable logic controllers (PLCs) made by General Electric, Rockwell Automation, Schneider Modicon, Koyo Electronics, and Schweitzer Engineering Laboratories. PLCs are used in industrial control systems to control functions in critical infrastructure such as water, power, and chemical plants; gas pipelines and nuclear facilities; as well as in manufacturing facilities such as food processing plants and automobile and aircraft assembly lines. The vulnerabilities, which vary among the products examined, include backdoors, lack of authentication and encryption, and weak password storage that would allow attackers to gain access to the systems. The security weaknesses also make it possible to send malicious commands to the devices to crash or halt them, and to interfere with specific critical processes controlled by them, such as the opening and closing of valves. As part of the project, the researchers worked with Rapid7 to release Metasploit exploit modules to attack some of the vulnerabilities. Metasploit is a tool used by computer security professionals to test if their networks contain specific vulnerabilities. Hackers also use the same exploit tool to find and gain access to vulnerable systems.
Source: http://www.wired.com/threatlevel/2012/01/scada-exploits/

45. *January 19, H Security* – (International) **OpenSSL fixes DoS bug in recent bug fix.** The OpenSSL developers have released versions 1.0.0g and 0.9.8t to address a denial of service (DoS) issue introduced by one of the six fixes included in the version they released earlier in January. The problem was created by the fix for a critical vulnerability in the CBC ("Cipher block chaining") encryption mode which enabled plaintext recovery of OpenSSL's implementation of DTLS (Datagram TLS). Accordingly, the advisory notes the DoS flaw only affects users using DTLS

applications that use OpenSSL 1.0.0f and 0.9.8s. The developers credit a researcher from Cisco Systems for discovering the bug and preparing the fix for it.
Source: http://www.h-online.com/security/news/item/OpenSSL-fixes-DoS-bug-in-recent-bug-fix-1417352.html

For more stories, see items **17**, **21**, **35**, **36**, **37**, **38**, **39**, and **46**

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

46. *January 19, KVOA 4 Tuscon* – (Arizona) **Copper thieves target Century Link.** A $1,000 reward is being offered for information leading to an arrest in the case of copper theft from Century Link, KVOA 4 Tucson reported January 19. The phone, Internet, and TV company said copper was stolen from more than 80 sites in Pima County, Arizona, and the Phoenix area. Forty-three of those sites are in Tucson alone. The vice president and general manager of Century Link said the theft has cost the company hundreds of thousands of dollars, but has really impacted its customers. "[W]e're most concerned about the outages this causes for people that rely on the service day in and day out." Each theft causes hours of service outage for thousands of customers and takes crews several hours to repair. Authorities from throughout Pima County are investigating. A deputy said the Pima County's Sheriff's Office is looking at 11 cases from Century Link alone. Century Link believes citizens may not contact authorities because, in some instances, the thieves are driving utility type trucks posing as landscapers. "The thieves typically target areas that are a little bit more rural. Where they probably stand a better chance of doing this and some of the theft has actually taken place in the middle of the day," the vice president said.
Source: http://www.kvoa.com/news/copper-thieves-target-century-link/

[Return to top]

Commercial Facilities Sector

47. *January 20, Associated Press* – (Nevada) **26 homes lost in Reno fire and 2,000 evacuated.** Firefighters worked January 20 to hold the line on a fast-moving brush fire that tore through the Reno, Nevada, area, destroying at least 20 homes and forcing thousands of residents to flee. The fire started January 19 and fueled by wind gusts reaching 82 mph, grew to more than 6 square miles in size before firefighters stopped its surge toward Reno. The fire was holding steady at about 3,700 acres and was 50 percent contained, a spokesman with the Sierra Fire Protection District said January 20.

More than 10,000 people were told to leave their homes during the height of the fire, and about 2,000 of them remained under evacuation orders January 20. At least 700 people were expected to fight the fire, including law enforcement, crews from the National Guard, and firefighters from California. Twenty homes were destroyed, but a full assessment might reveal even more damage. There was one fatality in the fire area, according to the fire chief, but he said an autopsy would be needed to determine the cause of death. About 300 elementary school students were taken to an evacuation center, and deputies went door to door asking people to leave their homes in Pleasant Valley, Old Washoe Valley, and Saint James Village, a Washoe County sheriff's deputy said. The fire was "almost a carbon copy" of a huge wildfire on the edge of the Sierra foothills that destroyed 30 homes in southwest Reno in November. That fire burned about 3 square miles and forced the evacuation of 10,000 people.
Source: http://www.foxnews.com/us/2012/01/20/more-than-20-homes-destroyed-by-reno-wildfire/

48. *January 20, Springfield News-Leader* – (Missouri) **Homeless shelter residents displaced for weeks after fire.** About 150 people were evacuated from the Missouri Hotel in Springfield January 20 after a fire started on the second floor. The fire was reported at the hotel, which serves homeless families. The hotel's executive director said two rooms were completely destroyed by the fire. There is smoke and water damage throughout the building. The executive director said he does not know how long it will be before residents can move back in.
Source: http://www.news-leader.com/article/20120120/NEWS01/120120001/0/NEWS06/?odyssey=nav|head

49. *January 20, Jersey Journal* – (New Jersey) **Man missing after all-night Union City fire.** An eight-alarm fire in Union City, New Jersey, raged for nearly 9 hours January 18 into January 19, displaced 70 residents, and injured 13 firefighters. A man also remains unaccounted for, officials said January 19. The fire tore a path of destruction through six adjacent, mostly 3-story buildings, leaving half a city block in ruin. The condition of the building was deemed too dangerous to allow firefighters to search for the missing man. North Hudson Regional Fire & Rescue firefighters were assisted in battling the fire by firefighters from seven other departments. The affected buildings all have commercial spaces on the ground floor. An official said 13 firefighters were treated for minor injuries. The injuries were mostly related to smoke inhalation, as well as slipping and falling on ice formed by the water used to fight the blaze.
Source: http://www.nj.com/jjournal-news/index.ssf/2012/01/one_man_missing_after_all-nigh.html

50. *January 19, KTVK 3 Phoenix* – (Arizona; California) **Teen accused in Peoria smoke-shop murders.** A 15-year-old believed to be responsible for a shooting at a Peoria, Arizona, smoke shop that left two people dead and a third wounded was taken into custody in Los Angeles January 19. A Maricopa County attorney filed first-degree murder charges against the juvenile. Two Los Angeles patrol officers detained the teen after recognizing him from a police bulletin, according to a Peoria police spokesman. The teen is suspected of shooting three people at Euphorium Emporium January 17. A man and a woman died at the scene. Another man ran out of the store after being shot.

He was airlifted to a local hospital for treatment of a non-fatal gunshot wound. Police said the suspect took his stepfather's gun to rob the smoke shop. After the shootings, they believe the teen stole $300 plus another gun from the store, and then stole a truck. Officers found the truck abandoned January 18.
Source: http://www.azfamily.com/news/Teen-accused-in-Peoria-smoke-shop-shooting-arrested-in-LA-137702758.html

51. *January 19, KLEW 3 Lewiston* – (Idaho) **Explosion damages Moscow apartment building.** An explosion severely damaged a Moscow, Idaho, apartment building, leaving one person with a minor injury and all of the tenants without a home January 19. Fire officials said they responded to a gas explosion in the attic of a 2-story apartment building. The fire chief said he does not believe the explosion was natural gas-related, and noted methane might have been the cause. The entire structure was damaged by the blast and all tenants were evacuated. Fire officials think the building will have to be demolished.
Source: http://www.klewtv.com/Explosion-damages-Moscow-apartment-building-137721013.html

For another story, see item **2**

[Return to top]

National Monuments and Icons Sector

52. *January 19, Suwannee Democrat* – (Florida) **L.A. Bennett wildfire 80 percent contained.** The L.A. Bennett Wildfire in Lafayette County is now 80 percent contained, according to a wildfire mitigation specialist with the Florida Forest Service. The L.A. Bennett Wildfire began from unknown causes January 17 and was originally reported by the Florida Forest Service as affecting 50 acres of land near Hines Highway and South Canal. Later that afternoon, the fire was upgraded to 100 plus acres. It continued to grow and an hour later it was upgraded to 150 plus acres as crews worked to slow it. A helicopter was brought in to dump buckets of water on the fire. By January 17 evening, the fire had spread to over 300 acres and it was 50 percent contained, threatening no structures and no evacuations had been ordered. On January 18 afternoon, the fire had spread further, even with the rain that was falling, and was affecting more than 462 acres. At that time, the forest service said the fire was still only 50 percent contained. With the constant rainfall all day January 18, the wildfire mitigation specialist stated January 19 the fire had been 80 percent contained.
Source: http://suwanneedemocrat.com/mayo/x1070344586/UPDATE-L-A-Bennett-Wildfire-80-percent-contained

[Return to top]

Dams Sector

53. *January 20, Daily Iowan* – (Iowa) **Iowa City officials: $4M flood levee plans underway.** Iowa City officials said plans to build a $4 million flood levee are

underway, the Daily Iowan reported January 20. The proposed project — estimated to be completed in 2013 — would build a levee spanning from Highway 6 south to the CRANDIC railroad bridge on the east side of the Iowa River. The city commissioned the East Side Levee Project in response to the extensive damage sustained during the floods of 1993 and 2008. MMS Consultants said the project is in its preliminary design phase. The top of the levee is predicted to be 14 feet across and almost 648 feet above sea level. Federal Emergency Management Agency rules require levees to be built at least 3 feet higher than a 100-year flood elevation of 644.5 feet. Engineers are also dealing with how to drain water from flooding and rain, proposals for combinations of pump stations and storm sewers, and a specific gate to drain water that closes as the river level rises. Iowa City officials expect the final design to be finished between December 2012 and March 2013, with potential for the project being finished later in 2013.
Source: http://www.dailyiowan.com/2012/01/20/Metro/26586.html

54. *January 19, Arizona Republic News* – (Arizona) **Tempe lake rubber to be replaced by steel dam.** The Tempe, Arizona, City Council voted unanimously January 19 to replace Town Lake's west-end rubber dam with a hydraulically operated steel dam. The vote marks the beginning of the council's difficult task of determining how the city will fund construction of the $35.4 million dam. In addition to construction costs, Tempe must factor for funding the estimated $32.7 million it will cost to maintain and operate the dam over a 50-year life cycle. The three preliminary options for funding construction that the city has reviewed so far include seeking voter approval to sell bonds, selling city property, seeking a lease-purchase agreement, or a combination of these options.
Source: http://www.azcentral.com/12news/news/articles/2012/01/19/20120119tempe-lake-rubber-replaced-steel-dam.html

[Return to top]

Department of Homeland Security (DHS)
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 cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2267
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