Homeland Security

Daily Open Source Infrastructure Report
6 January 2012

Top Stories

- Sub-freezing temperatures cracked rail lines and affected train cars, closing and delaying rail service for many hours in the Washington D.C., New York, and Philadelphia metro areas. – *Washington Post* (See item **18**)
- A bank account-raiding worm is spreading on Facebook, having stolen log-in credentials from more than 45,000 users as it moves across the site, security researchers said. – *The Register* (See item **39**)

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 5, Olney Daily Mail* – (Illinois) **I-64 closes between Grayville and Fairfield.** Illinois State Police announced the closure of Interstate 64 in Illinois January 5. A tanker truck traveling westbound on Interstate 64, beginning at the Indiana-Illinois state line, spilled heated liquid petroleum onto the roadway January 4. As a result, the Illinois Department of Transportation (IDOT) closed both westbound lanes of Interstate 64 between Mile Post 130 and Mile Post 110 until further notice during the clean-up of the spill. It is unclear how much fuel spilled.

Source: http://www.olneydailymail.com/news/x924343105/I-64-closes-between-Grayville-and-Fairfield

2. *January 5, Associated Press* – (New York) **Rail propane cars derail in NY; no leaks reported.** Authorities said no propane leaked when several train tank cars derailed at an industrial site in Painted Post, New York. Emergency officials in Steuben County said six tank cars carrying propane left the tracks around 6:30 p.m. January 4 at a Dresser Rand plant. Authorities said none of the cars overturned and none of the fuel leaked. Traffic had to be detoured around the accident while emergency crews remained at the site.
Source: http://online.wsj.com/article/AP5c7d7489b7d84d08aeef86ed10ae6693.html

3. *January 4, Associated Press* – (California) **Man gets 12 years in prison for green energy scam.** Federal prosecutors said January 4 a Carson, California man has been sentenced to 12 years in prison for getting dozens of people to invest more than $1 million in a non-existent wind-energy technology business. A judge also ordered the man to pay restitution of more than $1 million to victims. The man was convicted of soliciting investments in companies that he falsely claimed would manufacture revolutionary new wind turbines to produce electricity. He falsely told investors the Nigerian government had committed to buying more than $1 billion worth of the windmills, and that the International Monetary Fund was providing financing. Prosecutors said he relied on religious rhetoric and imagery to appeal to investors. The defendant had eight prior criminal convictions, five of which were fraud-related.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/01/04/state/n224207S57.DTL

4. *January 3, Lexington Herald-Leader* – (Kentucky) **Wrecked tanker spills fuel oil on I-75 in Laurel.** Several thousand gallons of fuel oil spilled from a ruptured tanker January 2 after a wreck on Interstate 75 in Laurel County, Kentucky, state police said January 3 in a news release. The wreck happened when one driver lost control of his cargo tanker on the snow-slickened road and hit another car. The interstate was closed for several hours as crews worked to clean up the spilled fuel oil.
Source: http://www.kentucky.com/2012/01/03/2014220/fuel-oil-spills-on-i-75-after.html

[Return to top]

Chemical Industry Sector

5. *January 5, Nashville Tennessean* – (Tennessee; National) **Safety board says Gallatin plant deaths were avoidable.** The U.S. Chemical Safety Board (CSB) will push the Occupational Safety and Health Administration (OSHA) to publish proposed safety rules within the next year to help prevent combustible-dust accidents after such incidents killed five workers in Gallatin, Tennessee, in 2011. A final report was released January 5 detailing the investigation of three fires at the Hoeganaes iron-powders plant in Gallatin that killed five workers. The three explosions occurred in January, March, and May 2011. The CSB said at a news conference January 5 that new,

tougher OSHA standards should be fashioned to specifically include safety measures to control metal dust such as the materials associated with the Gallatin blasts. While the first two explosions were caused by sparks igniting combustible dust loose in the air, the safety board blamed the third accident on hydrogen gas leaking from a poorly maintained pipeline. The CSB, which has the authority to investigate chemical plant accidents and make recommendations (but cannot force implementation), found fault with Hoeganaes for improper recovery of combustible metal dust accumulations. The report also cited a lack of proper maintenance of pipelines. Investigators found the firm had no inspection or maintenance program in place to keep pipes carrying the extremely flammable gas from leaking. Hydrogen is used in the production of the iron powder Hoeganaes makes for the auto industry. The final report criticizes Hoeganaes for not taking action earlier to prevent dust accumulations in the plant, citing evidence the company knew of the hazards as far back as 2008.
Source: http://www.tennessean.com/article/20120105/BUSINESS/301050058/Safety-board-wants-OSHA-speed-workplace-dust-rules?odyssey=nav|head

6. *January 5, Fitchburg Sentinel & Enterprise* – (Massachusetts) **DEP fines Ashburnham plant.** An Ashburnham, Massachusetts manufacturing plant that processes protein from corn meal was fined $29,648 by the Massachusetts Department of Environmental Protection (DEP) for violating air-pollution control regulations, a DEP press release stated January 5. A May DEP inspection of the Flo Chemical Corp.'s plant determined the firm had new and repeat violations of its Air Pollution Control Approval permit. Company officials and DEP administrators negotiated an agreement requiring Flo to pay $15,360 of the penalty and comply with all regulations and approval conditions. The remaining penalty money was suspended pending the company's compliance with a DEP consent order.
Source: http://www.sentinelandenterprise.com/local/ci_19679422

[Return to top]

Nuclear Reactors, Materials and Waste Sector

7. *January 5, Minneapolis Star-Tribune* – (Minnesota) **Busted pipe cited in 500-gallon bleach leak at Xcel nuke plant.** Five hundred gallons of chlorine bleach leaked from a tank January 5 at the Prairie Island nuclear plant near Red Wing, Minnesota, prompting an emergency response from Xcel Energy and delaying classes in two nearby school districts. The leak of sodium hypochloride was discovered by a worker. Xcel said the leak is fully contained within a berm, and a clean-up crew was cleaning up the site January 5. The leak led to the utility declaring an alert, which is the second lowest of four emergency classifications established by the Nuclear Regulatory Commission. As a precaution, schools in the Prescott and Ellsworth districts in Wisconsin delayed the start of classes for 2 hours.
Source: http://www.startribune.com/local/136729298.html

8. *January 4, Kalamazoo Gazette* – (Michigan) **Palisades nuclear plant bumped down in status by NRC; Entergy Nuclear to dispute other findings next week.** Palisades nuclear plant in Covert Township, Michigan has been bumped down a grade level and

will have to go through an extra inspection after a comprehensive review of a May 2011 incident at the plant, according to the Nuclear Regulatory Commission (NRC), which released a final report of that incident January 3. Entergy Nuclear has appealed the action and the report's finding, considered a low- to-moderate safety issue, but the NRC rejected the appeal, an agency spokesperson said. Another review, of a more serious incident in September 2011, is in progress. If the preliminary finding is upheld in that case, the plant could be moved even further down in grade level, the NRC spokesperson said.
Source:
http://www.mlive.com/news/kalamazoo/index.ssf/2012/01/palisades_nuclear_plant_bumped.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+kzgazette_news+(Kalamazoo+Gazette+News+-+MLive.com)

[Return to top]

Critical Manufacturing Sector

9. *January 3, WNDU 16 South Bend* – (Indiana) **Honeywell plant evacuated due to gas leak.** The Honeywell plant in South Bend, Indiana, was evacuated January 3 due to a gas leak. Sources said a propane tank on a fork lift was leaking, which forced the evacuation. More than a dozen emergency vehicles were on the scene, and firefighters used fans to clear the air. At least two Transpo buses were also called in to keep evacuated workers warm.
Source:
http://www.wndu.com/hometop/headlines/Honeywell_plant_evacuated_due_to_a_gas_leak_136593168.html

For another story, see item **5**

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

10. *January 5, Tampa Bay Business Journal* – (Massachusetts) **SEC charges Palm Harbor man with accounting fraud.** The U.S. Securities and Exchange Commission (SEC) January 4 filed an action, accusing JBI Inc. of engaging in a scheme to commit securities and accounting fraud. The complaint also names JBI's chief executive officer and its former chief financial officer. The defendants are accused of stating materially false and inaccurate financial data on the financial statements of JBI for two reporting periods in 2009, and using the overvalued statements in two private capital-raising efforts that raised more than $8.4 million, a statement said. The SEC is seeking

permanent injunctions, disgorgement, and civil penalties.
Source: http://www.bizjournals.com/tampabay/news/2012/01/05/sec-charges-palm-harbor-man-with.html

11. *January 4, Cerritos-Artesia Patch* – (California) **Puffy Coat Bandit strikes Cerritos-area bank.** Four days after taking cash from Union Bank in Glendora, California, the Puffy Coat Bandit has hit another bank, reportedly in Cerritos and has shed his signature jacket, the Cerritos-Artesia Patch reported January 3. The bank robber hit a Chase Bank about 1:45 p.m., according to officials. He operated under the same tactics, carrying a similar binder, wearing a similar knit cap, issuing a demand note and wearing the same expression on his face, an FBI spokeswoman said. There were two changes to the robber's appearance, however. He allegedly was clean shaven and switched out his "puffy coat" for a different type. The robber took an undisclosed amount of cash from the Cerritos bank.
Source: http://cerritos.patch.com/articles/puffy-coat-bandit-strikes-cerritos-area-bank

12. *January 4, KMSP 9 Minneapolis-Saint Paul* – (Minnesota) **Bank robber caught, possibly 'Man in Black'.** The FBI is investigating whether a bank robbery suspect arrested near St. Peter, Minnesota, is the serial robbed dubbed the "Man in Black." The suspect was arrested by St. Peter police after he was seen driving a vehicle suspected in the robbery of Rolling Hills Bank in the town of Brewster January 3. He will be formally charged in connection with the Brewster robbery while the FBI works to determine if he is in fact the man who has committed several bank robberies in the Twin Cities metro. Over the past 2 months, the Man in Black has earned a reputation as the most prolific and elusive serial bank robber in Minnesota since the Fishing Hat Bandit, pulling off half a dozen heists since early November.
Source: http://www.myfoxtwincities.com/dpp/news/man-in-black-caught-jan-4-2011

13. *January 4, Reuters* – (Illinois) **SEC says adviser defrauded investors using LinkedIn.** Securities regulators charged an Illinois-based investment adviser January 4 with using LinkedIn and other social media networking Web sites to lure investors by offering more than $500 billion in fake securities. The Securities and Exchange Commission (SEC) alleged the adviser made the fraudulent offers to sell securities through two sole proprietorships — Anthony Fields & Associates (AFA) and Platinum Securities Brokers. It said the man provided false and misleading information about clients, assets under management and even the history of his firm's business. The SEC said he lied on forms he filed with the commission by claiming to have $400 million in assets under management — when in fact he had none. The SEC also alleged he violated numerous other securities regulations by failing to maintain adequate books and records or carry out proper compliance procedures. He held himself out as a broker-dealer even though he never properly registered with the SEC, the agency said. The SEC's enforcement action against the adviser comes as it has increased scrutiny of the use of social media in the financial services industry. The SEC January 4 used the enforcement case against the adviser as an opportunity to make an example of the issue by warning investors about the dangers of online scams. It also urged investment advisers to be more cautious about their use of social media to attract clients.

Source: http://www.reuters.com/article/2012/01/04/us-sec-socialmedia-fraud-idUSTRE8031VL20120104

14. *January 4, IDG News* – (International) **SpyEye malware borrows Zeus trick to mask fraud.** A powerful bank-fraud software program, SpyEye, has been seen with a feature designed to keep victims in the dark long after fraud has taken place, according to a January 4 report from security vendor Trusteer. SpyEye is notable for its ability to inject new fields into a Web page, a technique called HTML injection, which can ask banking customers for sensitive information they normally would not be asked. The requested data can include logins and passwords or a debit card number. It can also use HTML injection to hide fraudulent transfers of money out of an account by displaying an inaccurate bank balance. Trusteer found SpyEye also hides fraudulent transactions even after a person has logged out and logged back into their account. SpyEye does this by checking its records to see what fraudulent transactions were made with the account, then deleting them from the Web page, said Trusteer's chief executive officer (CEO). The account balance is also altered. It appears SpyEye has borrowed from Zeus, a famous piece of banking malware now commonly available and considered its parent. Trusteer has seen the technique used when a fraudster uses SpyEye to capture debit card details. When that data is obtained, the fraudster conducts a purchase over the Web or phone, and SpyEye masks the transaction, the CEO said. It does not affect, however, the bank's ability to see the fraud, he said.
Source:
http://www.pcworld.com/businesscenter/article/247252/spyeye_malware_borrows_zeus_trick_to_mask_fraud.html

15. *January 4, Reuters* – (Connecticut) **Possible data breach by Wells Fargo investigated.** Connecticut's attorney general is investigating a possible data breach in which Wells Fargo & Co may have disclosed customer Social Security numbers as part of a fraud investigation, Reuters reported January 4. The possible breach is the latest wrinkle in a probe into whether state employees falsified financial data on applications submitted for food benefits issued in the aftermath of Hurricane Irene, which struck the east coast last fall. The state department of social services had sent subpoenas to Wells Fargo seeking financial records as part of the investigation, according to a news release issued by the state attorney general (AG). The fourth-largest U.S. bank then may have provided customers copies of the subpoenas, which included Social Security numbers of multiple individuals, according to the statement. The AG sent a letter to Wells Fargo asking for an explanation of why the bank may have disclosed the information. A Wells Fargo spokesman said the bank's focus is on its customers and other individuals who were affected. The bank will offer them the option of signing up for identity theft protection, he said. The Connecticut governor in December announced an investigation into the benefits, which were made available to low-income Connecticut residents who incurred disaster-related expenses from Irene. An attorney, who represents some of the state employees under investigation, raised questions about the subpoenas in a news conference January 3. He said he knows of two customers who received subpoenas containing a total of 130 names and Social Security numbers.
Source: http://www.chicagotribune.com/business/sns-rt-us-wellsfargo-breachtre804024-20120104,0,2305175.story

For another story, see item **39**

[Return to top]

Transportation Sector

16. *January 5, Associated Press* – (Kentucky; Illinois) **Cairo Bridge reopened after barge hit pier.** A bridge that carries traffic across the Mississippi River between Wycliffe, Kentucky, and Cairo, Illinois, was reopened after a barge struck one of the piers. The Cairo Bridge carries U.S. Routes 51, 60, and 62. A spokesman of the Kentucky Transportation Cabinet said a harbor boat pilot reported he was moving an empty barge when it struck a bridge support at about 1:30 a.m. January 5. The bridge was closed while it was inspected for damage and it was reopened a few hours later. About 5,500 vehicles cross the bridge daily.
Source: http://www.rrstar.com/news/x352573494/Cairo-Bridge-reopened-after-barge-hit-pier

17. *January 5, Associated Press* – (Texas) **Multiple injuries in 40-car Texas pile up.** Authorities said multiple people were injured but no one died in a mass pileup involving as many as 40 vehicles on a highway in Southeast Texas. A Jefferson County Sheriff's Department deputy said at least 10 ambulances were dispatched to the scene of the collision January 5 on Highway 73 just west of Port Arthur, about 80 miles east of Houston. The collisions were caused "by poor visibility due to mixture of fog and smoke from marsh wildfires." Fires swept through dry marshlands in parts of Jefferson County earlier the week of January 2.
Source: http://www.news10.net/news/national/171416/5/Multiple-injuries-in-40-car-Texas-pile-up-

18. *January 4, Washington Post* – (National) **Cracked rails from fast chill cause widespread delays on DC Metro system.** Sub-freezing temperatures caused rush-hour delays on four of Washington Metropolitan Area Transit Authority's (Metro) five lines January 4, cracking sections of rail along two stretches of track and turning an already cold commute into a frigid marathon for some riders in Washington, D.C., Maryland, and Virginia. Temperatures in the region went from 60 degrees January 1 to the 40s January 2 and then dropped to 17 degrees by January 4, according to the National Weather Service. That caused a shock to the steel rails on Metro's tracks, said Metro's chief spokesman. On the Yellow Line, a 4-inch gap opened in a rail along the bridge across the Potomac River, he said, and a quarter-inch gap was found in a rail on the Red Line near the Takoma station. It can be unsafe to run trains over cracked rail lines, so rail service had to be suspended, and inbound and outbound trains shared a single track on both the Yellow and Red lines, the spokesman said. A nearly 40-foot piece of rail was replaced on the Yellow Line after rush hour, he said. The Red Line crack was temporarily bridged with a "splice bar" that held the pieces together so trains could use that section of track. By 1 p.m., a piece of 40-foot rail went into place on the Red Line to permanently replace the cracked rail. On January 3, in Long Island, New York, broken rail lines due to the cold weather caused 30-minute delays, said a spokesman for the Long Island Rail Road. A spokesman for the Southeastern Pennsylvania

Transportation Authority said his transit system has not had cracked-rail problems, but noted sudden changes in temperatures can cause other issues. The change in weather the week of January 2 caused problems with the rail car doors in Philadelphia, which tend to stick when the temperature swings, he said.
Source: http://www.washingtonpost.com/local/commuting/cracked-rails-from-fast-chill-cause-widespread-delays-on-dc-metro-system/2012/01/04/gIQAKKuXbP_story.html

19. *January 3, Billings Gazzette* – (Montana) **A long road of flood repairs still ahead for Montana.** The 2011 floods are in Montana's past, but repairing the damage to roads is proving to be long, jarring, and costly. The state department of transportation lists $41.3 million in repairs on the roads it is responsible for, with much work still to be done. The projects number more than 100 and do not include road repairs on county roads, where the burden of the bill falls on local governments. The state was quick to get roads reopened, but repairs will continue for some time, said the chief of the department's planning, policy, and analysis bureau. In central Montana, where hillsides heavy with water sloughed away, taking half a road with them, solar-powered traffic lights in the middle of nowhere became a common sight, as the transportation department rushed to keep oncoming cars from crowding what little road remained. In Fergus County, the number of weather-affected road areas at one point numbered 139 and included everything from washed-out culverts and landslides to chewed-up pavement and damaged bridges. The cost is expected to be $10 million, or more than six times what the county spends on roads in an average year. Fergus County still has nine bridges needing repairs. Through August 2011, Montana received $24 million from Federal Emergency Management Agency (FEMA) for public infrastructure repairs, though the final deadline for a FEMA request was not until October 11. FEMA approved more $50 million for Montana public assistance requests related to infrastructure.
Source: http://billingsgazette.com/news/state-and-regional/montana/a-long-road-of-flood-repairs-still-ahead-for-montana/article_735f1d07-dc9e-5dcb-9530-f88aa885c8a5.html#ixzz1iatUpW00

For more stories, see items **1**, **2**, and **4**

[Return to top]

Postal and Shipping Sector

20. *January 4, Santa Rosa Press Democrat* – (California) **Three tractor rigs destroyed in fire at FedEx facility in Petaluma.** In Petaluma, California fire officials are investigating an early-morning fire at a FedEx freight building that destroyed three tractor rigs and threatened a fuel tank containing at least 10,000 gallons of diesel fuel, the Santa Rosa Press Democrat reported January 4. Leaking fuel from a saddle tank also found its way into the city storm drain system, though the spill was contained before it reached a nearby creek, a Petaluma fire battalion chief said. Firefighters stopped the blaze about 15 feet short of an above-ground tank containing 10,000-to-20,000 gallons of fuel.

Source: http://www.pressdemocrat.com/article/20120104/ARTICLES/120109865/1033/news?Title=3-tractor-rigs-destroyed-in-fire-at-Petaluma-FedEx-facility&tc=ar

[Return to top]

Agriculture and Food Sector

21. *January 5, Duluth News Tribune* – (Minnesota) **Duluth norovirus outbreak linked to ill food-service employee.** A food worker was the most likely source of the illness that sickened at least 60 people who ate at the Greysolon Plaza Ballroom in Duluth, Minnesota, December 3, the Minnesota Department of Health (MDH) confirmed January 4. That coincided with the preliminary conclusion the MDH reached a week after the incident. "Multiple ill employees were identified, indicating the contamination of ready-to-eat food by an ill food worker was the most likely source of contamination," said a MDH spokesman. The department confirmed the culprit was norovirus, the most common food-related illness in Minnesota. It is often spread by food handlers who do not thoroughly wash their hands. About 250 people attended one event and 100 attended another at the Greysolon December 3, state officials said.
Source: http://www.duluthnewstribune.com/event/article/id/219044/

22. *January 5, Food Safety News* – (Wisconsin; Minnesota; California) **More shredded cheese recalled in Wisconsin.** In another recall of cheese processed in Wisconsin, Bekkum Family Farms of Westby is recalling shredded cheese because it may be contaminated with Listeria monocytogenes, Food Safety News reported January 5. In a news release, Bekkum Family Farms said it was informed by Alpine Slicing & Cheese Conversion, of Monroe, that its cheese was shredded on the same equipment where other cheese had tested positive for Listeria monocytogenes. Alpine processes and packages cheese for other companies. The recalled cheese is labeled "Grumpy Goat Shreds" under the Nordic Creamery brand name. It was sold in stores in Wisconsin, Minnesota, and California beginning November 11.
Source: http://www.foodsafetynews.com/2012/01/more-shredded-cheese-recalled-in-wisconsin/

23. *January 5, Food Safety News* – (National) **Martinelli's recalls certain sparkling cider bottles.** Certain production lots of Martinelli's Gold Medal Sparkling Cider in six-pack shrink-bundled glass bottles are being recalled in the western United States because a defective seal could break the bottle when it is opened, Food Safety News reported January 5. â¨The recalled six-packs have "best-by" dates of April 11 through 14, 2014.
Source: http://www.foodsafetynews.com/2012/01/martinellis-recalls-certain-sparkling-cider-bottles/

For more stories, see items **6** and **29**

[Return to top]

Water Sector

24. *January 4, Associated Press* – (Washington) **Some Seattle residents told to boil drinking water.** Some residents of southeast Seattle, Washington, were advised to boil their tap water until tests confirm it is safe to drink, following a water pipe break. The pipe broke early January 4, affecting as many as 1,300 homes. Seattle Public Utilities said repairs were completed and water service restored by the afternoon. The utility company said it would take at least 24 hours for the drinking water test results. Officials said the break occurred on a smaller pipe where it connects to a 20-inch main. To make the repair, the larger main had to be shut down, resulting in the outage.
Source: http://seattletimes.nwsource.com/html/localnews/2017162241_apwaseattlewatermainbreak2ndldwritethru.html

25. *January 4, Louisville Courier-Journal* – (Kentucky) **Sewage spill could bring fines.** A northern Bullitt County plant that likely spilled several hundred thousand gallons of partially treated sewage since December 31 faces potential penalties from the Kentucky Division of Water (KDW). The Bullitt County Sanitation District's Bullitt Hills plant has one clarifier that broke December 31, said the district manager. He said his crew has had little choice but to let the sewage flow into a tributary of the Tanyard Branch of Floyds Fork. State officials said repairs were completed January 4 and plant effluent could remain dirty for several days. Trucks were vacuuming the stream January 3 and 4, a KDW spokeswoman said. She said the district will likely be cited for discharging the pollution and for not notifying state officials when the breakdown occurred and the spill began. Fines under the Clean Water Act can reach as much as $25,000 per day per violation, though regulators often settle for less. The spokeswoman said the district might have been able to hire a trucking service to haul the sewage to another treatment plant. She said the spill highlights an ongoing concern in Bullitt County and other areas that have grown quickly but have failed to keep their sewage treatment systems up to date.
Source: http://www.courier-journal.com/article/20120104/NEWS01/301040113/Bullitt-County-Sanitation-District-and-Bullitt-Hills-sewage-plant-spill?odyssey=mod|newswell|text||s

26. *January 4, KEZI 9 Eugene* – (Oregon) **Albany wastewater overflows into the Willamette River.** More than 3 inches of rain in 2 days caused Albany, Oregon's wastewater plant to spill close to 1 million gallons of wastewater into the Willamette River, KEZI 9 Eugene reported January 4. City officials said the pipeline could not handle the heavy flow during the downpour. The sanitary overflow started early December 30 and lasted about 13 hours. City officials were investigating what went wrong, and trying to figure out a solution, possibly up-sizing the pipes, to prevent a similar event from happening again. Public works has until the end of the week of January 2 to submit a written report on the incident to the Oregon Department of Environmental Quality, which will then determine if the city will be fined.
Source: http://kezi.com/news/local/235297

27. *January 4, Mobile Press-Register* – (Alabama) **20,000-gallon sewer overflow in Mobile blamed on grease blockage.** Mobile Area Water & Sewer System (MAWSS) responded to a sanitary sewer overflow January 4 in Mobile, Alabama. About 19,945 gallons of wastewater overflowed into Montlimar Creek as the result of a grease blockage, health officials said. MAWSS crews cleared the blockage and were taking steps to prevent future overflows at the location.
Source: http://blog.al.com/live/2012/01/grease_blockage_blamed_for_sew.html

[Return to top]

Public Health and Healthcare Sector

28. *January 4, Atlanta Journal-Constitution* – (Georgia) **Atlanta man used HIV patients' data to defraud Medicaid.** An Atlanta man who volunteered to help HIV patients to obtain personal information and defraud Georgia's Medicaid program was sentenced by state prosecutors January 4. He claimed that between June 2005 and November 2009 he was providing case management services to HIV patients in DeKalb County, which included getting HIV sufferers to needed medical, social, nutritional and education services. Prosecutors said he did not provide any of those services. Instead, he used HIV patients' Social Security numbers and personal information to bill Medicaid for services he did not provide. Some of the personal information was gained by holding charity events, such as a toy giveaway, for HIV patients that required them to provide personal data before they could participate. In some cases, he paid HIV patients directly for personal data. He was sentenced to 15 years after pleading guilty to defrauding Medicaid of more than $300,000 and falsifying documents to hide his crime. He operated Northwest Ministry Inc., which was created in 2000 as a non-profit corporation to provide support services for homeless and economically disadvantaged individuals and families, which included child care, health care, temporary shelter, and help for HIV sufferers.
Source: http://www.ajc.com/news/dekalb/atlanta-man-used-hiv-1289237.html

29. *January 4, U.S. Food and Drug Administration* – (National) **FDA to protect important class of antimicrobial drugs for treating human illness.** The U.S. Food and Drug Administration (FDA) issued an order January 4 that prohibits certain uses of the cephalosporin class of antimicrobial drugs in cattle, swine, chickens and turkeys effective April 5, 2012. The FDA is taking this action to preserve the effectiveness of cephalosporin drugs for treating disease in humans. Prohibiting these uses is intended to reduce cephalosporin resistance in bacterial pathogens. Cephalosporins are commonly used in humans to treat pneumonia as well as to treat skin and soft tissue infections. In addition, they are used in the treatment of pelvic inflammatory disease, diabetic foot infections, and urinary tract infections. In its order, the FDA is prohibiting "extralabel" or unapproved uses of cephalosporins in cattle, swine, chickens and turkeys, the so-called major species of food-producing animals. Specifically, the prohibited uses include: using cephalosporin drugs at unapproved dose levels, frequencies, durations, or routes of administration; using cephalosporin drugs in cattle, swine, chickens or turkeys that are not approved for use in that species (e.g., cephalosporin drugs intended for humans or companion animals); using cephalosporin

drugs for disease prevention.
Source:
http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm285704.htm

30. *January 4, Santa Barbara Noozhawk* – (California) **Drug investigation links Santa Barbara doctor's prescriptions to 11 patient deaths.** A Santa Barbara, California physician faces a federal criminal complaint of distribution of controlled substances outside the scope of professional practice and without legitimate medical purpose. He was arrested January 4 by the Drug Enforcement Administration (DEA). The 75-page affidavit from the U.S. attorney's office in Los Angeles details the lengthy investigation by the DEA, Santa Barbara police and the Santa Barbara County Sheriff's Department, outlining dozens of cases, including 11 drug-related patient deaths. According to the affidavit, "profound" doses of drugs such as OxyContin, Fentanyl and Dilaudid were prescribed for common physical conditions, including back pain and menstrual cramps. The document said some of the patients required emergency room visits shortly after leaving the physician's office. It said he prescribed 2,087 pills to 1 27-year-old in the 6 weeks before his or her death and the bottles, mostly empty or nearly empty, were found on the scene by first responders. Some Santa Barbara-area pharmacies grew suspicious of the physician's practice and have therefore "blacklisted" him and refuse to fill his prescriptions. CVS stopped filling his narcotic prescriptions in 2008, although the pharmacy continued filling "maintenance medications" such as Lipitor, a cholesterol drug. According to the affidavit, patients filled his prescriptions in 48 California cities outside Santa Barbara County and even in other states as far away as Utah and North Carolina. He also gave some pills out directly from the clinic, and DEA agents cleared out the drugs when they raided his office. The special agent who wrote the report also found a record of the narcotics the physician ordered directly to his office, which included more than 20,000 dosage units of hydrocodone each year since 2008.
Source: http://www.noozhawk.com/article/010412_prescription_drugs_arrest/

[Return to top]

Government Facilities Sector

31. *January 5, Fitchburg Sentinel & Enterprise* – (Massachusetts) **Police: Teen posted FHS threat online.** A former student of Fitchburg High School in Fitchburg, Massachusetts, was arraigned January 4 in district court on charges he posted a series of messages on Facebook about shooting up the school and killing everyone inside, the Fitchburg Sentinel & Enterprise reported January 5. The teenager is charged with making a bomb or hijack threat. Police arrested him January 3 after a parent of a friend noticed several threatening status updates. His messages included direct statements and references that can be interpreted as threats, an assistant district attorney said. The high school principal said the teen had missed so many days of school that he was removed from the enrollment list.
Source: http://www.sentinelandenterprise.com/topstory/ci_19679532

32. *January 4, CBS News; Associated Press* – (Texas) **8th-grader killed by Texas police had pellet gun.** Police said the weapon a Texas eighth-grader pointed at officers in a school hallway in Brownsville, Texas, January 4 before they killed him was a pellet gun that looked like a real handgun. The interim Brownsville police chief said the 15-year-old had "plenty of opportunities" to lower the weapon but "didn't want to." He said two officers fired three shots and struck the teen at least twice. The interim police chief said before the confrontation with police, the teen walked into a Cummings Middle School classroom and punched another boy in the nose. He said he does not know why the teen brandished the weapon, but the initial call to police said a student had a gun.
Source: http://www.cbsnews.com/8301-201_162-57352546/8th-grader-killed-by-texas-police-had-pellet-gun/

[Return to top]

Emergency Services Sector

33. *January 5, Associated Press* – (Utah) **Utah shooting: 6 police officers shot while serving search warrant.** Gunfire erupted as anti-drug police served a search warrant in an Ogden, Utah neighborhood, fatally wounding one officer and injuring five other officers and a suspect, authorities said. The shots rang out late January 4 as police converged at a residence, a police spokesman said. The six officers were hospitalized along with a suspect. Ogden police said in a statement early January 5 that one agent died from his wounds following the shooting. Five police officers from multiple agencies remain hospitalized with serious to critical injuries. The sole suspect in the shooting is at a local hospital under guard, with non-life threatening injuries. The Ogden Standard-Examiner reported that more police responded upon word of at least one officer shot. The paper said police surrounded the suspect near a backyard shed. The residence was secured after the arrest.
Source: http://www.huffingtonpost.com/2012/01/05/utah-shooting-police-officers-wounded_n_1185321.html

34. *January 5, Chicago Sun Tiimes* – (Illinois) **Misfiring warning siren blares at 4 a.m.** West Dundee, Illinois' emergency warning siren began sounding at about 4 a.m. January 4 and did not stop for almost an hour. Thousands of people in northern Kane County, along the Elgin-West Dundee-Sleepy Hollow border were affected. Dispatchers at the QuadCom emergency dispatch center in Carpentersville tried shutting down the siren by remote control, but it did not work. A fire truck was sent to the scene. The village manager said the firefighters arrived within a few minutes and in effect "pulled the plug" on the siren, interrupting its connection to ComEd power lines. But that only made the siren switch over to its reserve battery, and it kept blaring until finally shutting down about an hour later.
Source: http://beaconnews.suntimes.com/news/9817841-418/misfiring-warning-siren-blares-at-at-4-am.html

35. *January 4, Birmingham News* – (Florida) **Suspicious package prompts evacuation of Escambia County sheriff's office; other Gulf Coast region news.** A suspicious

package forced the evacuation of the Escambia County, Florida sheriff's office early January 4, NorthEscambia.com reported. A man received a suspicious package delivered to his address with no name on it and took it to the sheriff's office. The package also included instructions asking the recipient to mail it to the Ukraine. A bomb-sniffing dog alerted authorities to the potential of possible explosives in the package material, forcing the evacuation of about 150 employees from the building. A robot was used to remove the package from the building.
Source: http://blog.al.com/live/2012/01/suspicious_package_prompts_eva.html

[Return to top]

Information Technology Sector

36. *January 5, The Register* – (International) **Sites knocked offline by OpenDNS freeze on Google.** Innocent Web sites were blocked and labelled phishers January 4 following an apparent conflict between OpenDNS and Google's Content Delivery Network (CDN). OpenDNS — a popular domain name lookup service — sparked the outage by blocking access to googleapis.com, Google's collection of useful scripts and apps for Web developers. According to reports, a flood of errors hit pages that used Google-hosted jQuery and hundreds of thousands of sites fell over. Visitors to Web sites were confronted with a message saying: "Phishing site blocked. Phishing is a fraudulent attempt to get you to provide personal information under false pretenses." Other visitors were greeted with a 404 error. Web design and hosting specialist Brit-Net told The Register the outage lasted nearly 3 hours. As sites and service providers struggled to get back online, they employed fallback scripts and re-routed traffic to CDN. The cause of the problem with OpenDNS seemed to be the googleapi.com security certificates, according to a Brit-Net researcher.
Source: http://www.theregister.co.uk/2012/01/05/google_opendns_clash/

37. *January 5, Threatpost* – (International) **New version of OpenSSL fixes six flaws.** A new version of the OpenSSL package has been released, fixing six vulnerabilities, including a plaintext recovery attack on the DTLS implementation. There are two other cryptographic flaws fixed in OpenSSL 1.0.0f, and a few other less-serious problems. The most problematic of the vulnerabilities fixed in the new version is the one that enables the plaintext recovery attack, which was discovered by a pair of security researchers who found a way to extend the CBC padding oracle attack. The attack enables someone to exploit the problem with OpenSSL's DTLS implementation to recover the plaintext version of an encrypted message.
Source: http://threatpost.com/en_us/blogs/new-version-openssl-fixes-six-flaws-010512

38. *January 5, Softpedia* – (International) **New AOL Instant Messenger raises privacy concerns, EFF reports.** The Electronic Frontier Foundation (EFF) analyzed the preview version of the latest AOL Instant Messenger and concluded users should not install it due to serious privacy concerns. The first issue is conversation logs are stored by default and secondly, all private instant messages are scanned for URLs, which means all the chats are fetched to AOL's servers in Virginia. AOL's decisions to move some of their services to the cloud, where data is usually stored in a plain text form,

raises serious concerns because cybercriminals and law enforcement agencies could access it if they have a warrant. The customers' privacy is at stake because in both scenarios their private conversations may become exposed even without their knowledge. Regarding the fact conversations are fetched to their servers to be scanned for URLs raises concerns with the EFF because AOL gives no clear indication on how this process occurs in their terms of service or privacy policies. The foundation believes the company should not only give users initial notice with an opt-in check box, but also explain to them in clear and specific terms how information is handled. AOL promised to disable this functionality for conversations that are marked to be "off the record." However, the "off the record" feature is available only for customers who utilize the latest version of the program.
Source: http://news.softpedia.com/news/New-AOL-Instant-Messenger-Raises-Privacy-Concerns-EFF-Reports-244551.shtml

39. *January 5, The Register* – (International) **Worm slurps 45,000 Facebook passwords.** A bank account-raiding worm has started spreading on Facebook, stealing log-in credentials as it moves across the site, security researchers said. Evidence recovered from a command-and-control server used to coordinate the evolving Ramnit worm confirms the malware already stole 45,000 Facebook passwords and associated e-mail addresses. Experts from Seculert, who found the controller node, supplied Facebook with a list of all the stolen credentials found on the server. Most of the victims are from either the United Kingdom or France. Ramnit differs from other worms that use Facebook to spread because it relies on multiple infection techniques, and it only recently extended onto social networks. "Ramnit started as a file infector worm which steals FTP credentials and browser cookies, then added some financial-stealing capabilities, and now recently added Facebook worm capabilities," the CTO at Seculert said. "We suspect that they use the Facebook logins to post on a victim's friends' wall links to malicious Web sites which download Ramnit," he added. Ramnit first appeared in April 2010. By July 2011, variants of the malware accounted for 17.3 percent of all new malicious software infections, according to Symantec. In August 2011, Trusteer reported variants of Ramnit were packing sophisticated banking log-in credential snaffling capabilities — technologies culled from the leak of the source code of the Zeus cybercrime toolkit at around the same time. The new Ramnit configuration was able to bypass two-factor authentication and transaction-signing systems used by financial institutions to protect online banking sessions. The same technology might also be used to bypass two-factor authentication mechanisms to gain remote access to corporate networks, Seculert warns.
Source: http://www.theregister.co.uk/2012/01/05/ramnit_social_networking/

40. *January 4, H Security* – (International) **Apache Struts update closes critical holes.** The Apache Struts developers released version 2.3.1.1 of their open source framework for Java-based Web applications. The update closes critical holes in Struts 2, fixing four old and well-known security vulnerabilities that could be exploited by an attacker to circumvent restrictions by using dynamic method invocation (DMI) to inject and execute malicious Java code. Versions 2.1.0 to 2.3.1 of Struts are affected; upgrading to 2.3.1.1 corrects the issues. Alternatively, the security advisory provides instructions for changing a configuration file that mitigates the problem.

Source: http://www.h-online.com/security/news/item/Apache-Struts-update-closes-critical-holes-1403697.html

For another story, see item **14**

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

41. *January 3, New Orleans Times-Picayune* – (Louisiana) **Ex-AT&T employee accused of stealing copper wire from company sites.** An ex-AT&T employee who had been allegedly stealing spools of copper wire from his former employer for weeks was arrested after being caught inside a storage site near Covington, Louisiana, a spokesman from the St. Tammany Parish Sheriff's Office said January 3. Deputies have booked the man with breaking into the telecommunication firm's facilities on the north shore at least 17 times and pilfering the equipment during 16 of those occasions, an agency spokesman said. Investigators began probing a series of copper thefts from AT&T complexes at the beginning of November, the spokesman said. Many sheriff's divisions subsequently staked out the company's site. On December 28, the suspect was supposedly spotted in the storage yard. He allegedly threw a punch at a deputy who confronted him before he was subdued, the spokesman said. The sheriff's office jailed the suspect in connection with the break-ins, the thefts, and resisting arrest. It expects to add more counts as the investigation develops. Investigators suspect the man was selling the copper to recycling businesses. The suspect worked at AT&T 4 years ago, but no other details of his employment were available.
Source: http://www.nola.com/crime/index.ssf/2012/01/ex-att_employee_accused_of_ste.html

For another story, see item **38**

[Return to top]

Commercial Facilities Sector

42. *January 5, Associated Press* – (California) **2 men commit suicide by releasing chemicals in car.** Investigators said two Southern California men committed suicide by releasing household chemicals inside a parked car January 2. An Inglewood police official said officers responding to reports of a suspicious car in a parking structure found the men. Investigators told City News Service the deaths were apparently caused by mixing household chemicals. The parking structure was evacuated and a Los

Angeles County hazardous materials squad was called in because of the potential danger.
Source: http://www.mercurynews.com/breaking-news/ci_19679661

43. *January 5, Associated Press* – (Montana) **Wildfires at Montana Indian Reservation force evacuations.** Two wildfires raging January 4 on Montana's Blackfeet Indian Reservation burned thousands of acres, forced hundreds to evacuate, and destroyed several buildings, officials said January 5. Fueled by strong winds, the two fires started and together had grown to at least 45,000 acres. At least 300 people were forced to leave their homes, and officers were working to evacuate additional residents in the fires' eastward path. One fire started southeast of Browning burned about 8 miles east to the community of Blackfoot, a tribal spokesman said. Another fire erupted around the same time about 10 miles away. The Blackfeet Law Enforcement chief told the Great Falls Tribune the fires were started by what was believed to be power lines that were blown over by high winds. One fire that burned east of Browning had already been put out.
Source: http://www.firehouse.com/news/10603872/wildfires-at-montana-indian-reservation-force-evacuations

44. *January 4, Boston Globe* – (Massachusetts) **Fall River police make arrest in mill fire.** Fall River, Massachusetts police arrested a convicted arsonist in connection with a fire that razed an empty mill building January 3. Police said the suspect was seen in the crowd watching the fire at the King Phillip Mill complex. Police said he fled when he saw officers, who smelled accelerant on his clothes. Police said he was seen on surveillance video loading into a car items from the mill which were allegedly found later in his home. The Herald News reported the suspect is facing charges including attempted murder, because the building manager was inside at the time of the fire.
Source:
http://www.boston.com/news/local/massachusetts/articles/2012/01/04/fall_river_police_make_arrest_in_mill_fire/

45. *January 4, Lakeland Ledger* – (Florida) **Pair of businesses destroyed in Winter Haven blaze.** Two Winter Haven, Florida businesses were destroyed and a street closed for nearly 3 hours while fire crews battled a commercial fire January 4. One of the owners of Cox Motor Sales Inc. said the fire swept through her business along with the greenhouse owned by O'Connor's Flower Haven. A Winter Haven fire investigator said at least three to four cars in the Cox lot were destroyed as well.
Source: http://www.theledger.com/article/20120104/NEWS/120109768?tc=ar

46. *January 3, KGTV 10 San Diego* – (California) **Vandals hit Jehovah's Witness Kingdom Hall for 3rd time.** Authorities are looking for the person or people who tried to set fire to a place of worship in San Diego for the third time in 2 weeks. Firefighters and police were called to the Kingdom Hall of Jehovah's Witnesses in the University Heights area January 3. The most recent time, authorities said the intruders cut a hole through a fence and poured gasoline inside the hall but were unable to start a fire. A fire heavily damaged the building December 30. The first fire was reported around December 20. Intruders pried open the doors, stole audio equipment, and then set the

fire, which did minimal damage. Initially, police thought the fire was set to conceal the break in. A reward of up to $10,000 has been offered from Crime Stoppers and the Bureau of Alcohol, Tobacco, Firearms, and Explosives.
Source: http://www.10news.com/news/30122472/detail.html?source=sand

47. *January 2, Associated Press* – (Iowa) **Police arrest Occupy activists at Des Moines hotel.** Des Moines, Iowa police arrested about a dozen Occupy the Caucuses activists who lay on the floor of a downtown hotel lobby after failing to meet with Democratic Party officials January 2. Police were called to the hotel after activists demanded to meet with Democratic officials. The party earlier announced it was setting up a headquarters at the hotel to get their message out during the caucuses. No Democratic officials met with the protesters, prompting them to lie on the floor. Police said they charged about a dozen people with trespassing. Police arrested protesters almost daily for a week at candidate offices and Democratic Party headquarters.
Source: http://www.kcautv.com/story/16430768/police-arrest-occupy-activists-at-des-moines-hotel

[Return to top]

National Monuments and Icons Sector

48. *January 5, Associated Press* – (Washington) **Mount Rainier National Park to reopen Saturday.** Mount Rainier National Park will reopen to the public January 7, nearly a week after a park ranger was shot to death trying to stop a vehicle inside the park. The ranger had set up a roadblock on New Year's Day to stop a vehicle that blew through a checkpoint that Mount Rainier rangers use to determine whether vehicles are equipped with chains for winter driving. The driver of that vehicle shot the ranger while she was in her car and then fled on foot. Searchers found the body of the suspect in a snowy creek January 2 with a handgun and rifle nearby. An autopsy showed he had hypothermia and drowned. Police said the suspect was an Iraq war veteran, and had been involved in an earlier shooting at a party early January 1 in Skyway, Washington. Both shootings were under investigation January 4. In a statement, the park said that all services would be available January 7 except for snow play.
Source:
http://www.boston.com/news/nation/articles/2012/01/05/mount_rainier_national_park_to_reopen_saturday/

49. *January 5, Jacksonvile Florida Times-Union* – (Georgia) **Firefighters working 45-acre blaze on Cumberland Island.** Firefighters from three agencies are working to contain the 45-acre Hickory Hill Fire that is burning on the east side of Cumberland Island in Georgia, an official said. On January 4, Camden County 911 informed Cumberland Island National Seashore fire management officials that there was visible smoke on the island, a chief interpretive ranger at the park said in a news release. Crews from the National Park Service, Camden County Fire and Rescue, and the Georgia Forestry Commission responded quickly to contain and monitor the fire. To ensure the safety of visitors and firefighters, Cumberland Island has closed areas that are most directly affected by the fire, the park superintendent said. The cause of the fire

is under investigation.
Source: http://jacksonville.com/news/georgia/2012-01-05/story/firefighters-working-45-acre-blaze-cumberland-island

[Return to top]

Dams Sector

50. *January 4, KCAU 9 Sioux City* – (South Dakota) **Gavins Point spillway likely to remain open through February.** The U. S. Army Corps of Engineers announced that releases will likely continue through the spillway at the Gavins Point Project in South Dakota through the end of February, KCAU 9 Sioux City reported January 4. Releases are expected to be around 22,000 cubic feet per second (cfs) to help gain additional reservoir system storage in preparation for the 2012 runoff season. As water continues to be released through the spillway, hazardous conditions exist for any vessel in the area,and boaters are urged to use caution.
Source: http://www.kcautv.com/story/16446526/spillway-likely-to-remain-open-through-february

[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 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