Daily Open Source Infrastructure Report
18 January 2012

Top Stories

- Many of the 146 people sickened with norovirus in Wheeling, Illinois, may have been exposed at Bob Chinn's Crab House, the Cook County Health Department said. – *Food Safety News* (See item **25**)
- Popular online shoe retailer Zappos.com said January 15 that hackers accessed its network and stole account information from as many as 24 million customers. – *Fox News* (See item **52**)

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 17, Claims Journal* – (Mississippi; Alabama) **4 accused in Mississippi Chevron refinery thefts.** Three people suspected of stealing equipment and trucks from Chevron's Pascagoula Refinery, in Mississippi, were in custody, a fourth was still being sought. A local sheriff told the Biloxi Sun Herald the investigation was launched

January 3 after reports of thefts of several pieces of equipment, along with one of Chevron's Ford F-150 pickup trucks. The investigation expanded to include deputies from the Mobile County Sheriff's Department in Alabama after a vehicle matching the description of the stolen truck fled a traffic stop. That man has since been apprehended, but the fourth still remains at large.
Source: http://www.claimsjournal.com/news/southeast/2012/01/17/198924.htm

2. *January 16, Associated Press* – (Alaska) **Fuel transfer launched from Russian tanker at iced-in Alaska town.** Crews began transferring 1.3 million gallons of fuel January 16 from a Russian fuel tanker in the Bering Sea to the iced-in Alaska city of Nome. The offloading began near sundown after crews safety-tested two transfer hoses with pressurized air. The hoses connect to a pipeline that leads to storage tanks in town. State officials said the transfer must start during daylight, but can continue in darkness. Nome has just 5 hours of daylight this time of year. The transfer could be finished within 36 hours if everything goes smoothly, but it could take as long as 5 days. Before the hoses could be laid out, the ice disturbed by the tanker's journey had to freeze again so workers could create a roadway. Personnel will walk the entire length of hosing every 30 minutes to check for leaks. Each segment of hose has its own spill containment area, and extra absorbent boom will be on hand in case of a spill. The U.S. Coast Guard is monitoring the effort, working with state, federal, local and tribal representatives.
Source: http://www.washingtonpost.com/national/russian-tanker-arrives-at-iced-in-alaska-town-to-transfer-fuel-to-residents/2012/01/16/gIQAgj2h2P_story.html?tid=pm_national_pop

3. *January 16, WJW 8 Cleveland* – (Ohio) **Residents remain displaced by Wellington gas leak.** Dozens of people in Wellington, Ohio, were still not allowed to return home the evening of January 16 after a massive gasoline leak from an underground pipe. About 70 people were evacuated from 30 homes January 12 after a pipe sprung a leak spilling 116,760 gallons of gasoline, according to Sunoco Logistics. "The spill right now is contained, we are in clean up mode. We have dozens of pieces of heavy equipment as well as dozens of people from Sunoco Logistics and contractors as well as local authorities out there working to clean it up," a Sunoco Logistics spokesman said. The gasoline pipeline, owned by Sunoco Logistics, runs from Toledo to Allegheny and because of the spill has been shut down. Sonoco Logistics, the Environmental Protection Agency and other agencies were expected to have people on hand at a community meeting January 16 to answer questions from the public.
Source: http://www.fox8.com/news/wjw-news-wellington-gas-leak,0,6583644.story

For more stories, see items **47** and **53**

[Return to top]

Chemical Industry Sector

4. *January 14, Jackson County Floridan* – (Florida) **Train with chemical car derails in Grand Ridge.** Eight cars on a CSX train derailed in Grand Ridge, Florida, before 7:30

a.m. January 14. The train contained several chemical shipments, bringing responses from a many area agencies, including police, fire, and emergency management. As of noon January 14, the only chemical that spilled was PVC pellets. The Jackson County sheriff said the pellets would be vacuumed up by environmental services. The Jackson County fire chief said there was a slim chance righting the cars would cause another spill, as CSX planned to stabilize the cars first. About 400 feet of track must be replaced. The fire chief said CSX planned to fix the track and bring in special equipment to put the cars back on the track. A CSX spokesman said crews were on their way to have service restored by the morning of January 15. He said the two-locomotive, 48-car train was headed from New Orleans to Waycross, Georgia.
Source: http://www2.jcfloridan.com/news/2012/jan/14/train-chemical-car-ar-3046013/

5. *January 13, Abilene Reporter-News* – (Texas) **Zoltek assessed penalty by state environmental regulators — again.** State environmental regulators have assessed a $32,660 penalty against Zoltek Corp., an Abilene, Texas manufacturer of carbon fiber. It marks the second time in 3 years the company has agreed to pay a penalty, each time after investigators found an excess of hydrogen cyanide and other pollutants released into the air. The most recent penalty was proposed after an August 2010 investigation found two separate instances in June of 2010 in which performance tests revealed excess emissions of about 231 pounds of hydrogen cyanide. Zoltek is seeking a permit amendment that would increase allowable furnace emissions to 2,200 pounds annually. Hydrogen cyanide is produced by Zoltek as a waste gas in the making of carbon fibers, strong and lightweight materials that can be used in automotive panels and wind turbine blades, among other uses. The firm has already taken steps to reduce emissions that include preventive maintenance, repairs, and installing new equipment.
Source: http://www.reporternews.com/news/2012/jan/13/zoltek-assessed-penalty-by-state-environmental/

For more stories, see items **28**, **32**, and **47**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *January 13, KWCH 12 Wichita* – (Kansas) **Wolf Creek nuclear power plant loses power.** The Wolf Creek nuclear power plant near Burlington, Kansas, shut down January 13 due to a loss of power. Both of the plant's emergency diesel generators automatically started, supplying power to all safety-related equipment. "The safety features of the plant responded as they should, and station operators have ensured that the plant is in a safe condition." said the plant's president and chief executive officer. However, due to the power loss, Wolf Creek declared a notification of unusual event, the least serious of four emergency classifications according to the Nuclear Regulatory Commission.
Source: http://www.kwch.com/news/kwch-news-kah-wolf-creek-nuclear-power-plant-loses-power-20120113,0,371173.story

[Return to top]

Critical Manufacturing Sector

7. *January 16, Pittsburgh Post-Gazette* – (Pennsylvania) **Fire shuts down part of USS Irvin Plant.** No one was injured in a fire January 16 at U.S. Steel's Irvin Plant in West Mifflin, Pennsylvania, but the blaze shut down the plant's pickle line, where sheet steel goes through an acid treatment to prepare the surface for further finishing, according to a company spokeswoman. The fire started about noon and was extinguished about 2:30 p.m. by U.S. Steel workers, including the company's hazardous materials team, with help from the West Mifflin and Glassport fire departments. Company officials said the plant's 84-inch pickle line was idle and was being investigated to see what repairs are needed, but the rest of the plant was operating normally. The state department of environmental protection and the Allegheny County Health Department were notified of the incident.
   Source: http://www.post-gazette.com/pg/12016/1203795-55.stm

8. *January 16, CBS News* – (National; International) **Thousands of Minis and Mini Coopers recalled.** BMW announced January 16 the recall of nearly 89,000 of its Mini and Mini Cooper cars in the United States, and more than 235,000 worldwide. The company said a water pump that cools the turbocharger in some models has a circuit board that can malfunction and overheat. "In an extreme case, this overheating can lead to a smoldering of the water pump and eventually can create a vehicle fire," according to a BMW spokeswoman. She said about 12 fires have been reported to the National Highway Transportation Safety Administration, though none have resulted in accidents or injuries. The fires started when the vehicles were standing still. The recalled models include: 2007-11 Mini Cooper S; 2008-11 Mini Cooper Clubman; 2009-11 Mini Cooper S Convertible; 2009-11 Mini JCW; 2009-11 Mini JCW Clubman; 2009-11 Mini JCW Convertible; and the 2011 Mini Cooper S Countryman.
   Source: http://www.cbsnews.com/8301-500395_162-57359874/thousands-of-minis-and-mini-coopers-recalled/

For another story, see item **47**

[Return to top]

Defense Industrial Base Sector

See item **47**

[Return to top]

Banking and Finance Sector

9. *January 16, Reuters* – (International) **Israel rattled as hackers hit bourse, banks, El Al.** Hackers disrupted online access to the Tel Aviv Stock Exchange (TASE), El Al Airlines, and three banks January 16 in what the government described as a cyber-offensive against Israel. The attacks came just days after an unidentified hacker,

proclaiming Palestinian sympathies, posted the details of thousands of Israeli credit card holders and other personal information on the Internet in a mass theft. Stock trading and El Al flights operated normally despite the disruption, which occurred as Israeli media reported pro-Palestinian hackers had threatened to shut down the TASE stock exchange and airline Web sites. While apparently confined to areas causing only limited inconvenience, the attacks caused particular alarm in a country that depends on high-tech systems for much of its defense against hostile neighbors. Officials insisted, however, that they pose no immediate security threat. The First International Bank of Israel (FIBI) and two subsidiary banks, Massad and Otzar Hahayal, said their marketing sites had been hacked but that sites providing online services to clients were unaffected. Israel's third-largest bank, Discount, said it had been spared attack, but that it was temporarily shutting down foreign access to its Web site as a precaution. The Tel Aviv bourse Web site could only be accessed intermittently, but screen-based trading was not hit. There was no claim of responsibility for the incidents.
Source: http://www.reuters.com/article/2012/01/16/israel-hackers-idUSL6E8CG26X20120116

10. *January 16, NJtoday.net* – (New Jersey) **PSE&G warns about payment scam targeted to Spanish-speaking customers.** Public Service Electric and Gas Company (PSE&G) is alerting its customers not to be defrauded by a scam in which individuals misrepresenting themselves as PSE&G employees threaten to turn off electric and gas service if payment is not made to them that day, NJtoday.net reported January 16. The scam involves payments using Green Dot MoneyPaks and seems to be targeting Hispanic neighborhoods in PSE&G's service territory. A Spanish-speaking individual pretending to be a PSE&G employee calls customers saying they "work for PSE&G in the disconnect collection department." They tell customers their account is in arrears and their utility service will be discontinued unless they make a payment using a prepaid debit card. Customers are told to purchase a Green Dot MoneyPak at any convenience store, use cash to put money onto the card, and then provide the number on the card to the person who called them. Customers are advised that if they do not immediately call back and provide the MoneyPak information, their service will be turned off that day. Typically, after the customer provides that MoneyPak number, the scammer transfers the funds to a prepaid card, and cashes it in at an ATM. PSE&G is working with law enforcement to investigate the matter, and is also reaching out to its contacts at local community service agencies asking them to spread the word to their clients. The Better Business Bureau also is warning customers to be on guard for a rising tide of scams involving MoneyPaks, which can be used to fund PayPal accounts and to pay phone, cable, or other utility bills, or credit card bills.
Source: http://njtoday.net/2012/01/16/pseg-warns-about-payment-scam-targeted-to-spanish-speaking-customers/

11. *January 13, Courthouse News Service* – (Texas) **Oilman pleads guilty to securities fraud.** An oil company executive pleaded guilty in a Dallas court to felonies in his operation of Western Pipeline Corp., federal prosecutors said the week of January 9. The defendant was the fifth defendant convicted in the case. He pleaded guilty to conspiracy to commit securities fraud and securities fraud. He faces up to 5 years in prison and a $250,000 fine on each count. He was majority owner of Western Pipeline

from October 2006 to July 2007. He raised money from investors by selling and causing others, including four co-conspirators to sell investments in purported oil and gas development projects, the U.S. attorney's office said in a statement announcing the plea. Prosecutors said the owner and his co-conspirators misled, deceived, and defrauded investors by misrepresenting and failing to disclose material facts. The co-conspirators assumed false identities when communicating with prospective investors and posed as investors in past Western Pipeline oil and gas development projects that supposedly had been successful. The co-conspirators have all pleaded guilty to securities fraud or conspiracy charges, the U.S. attorney's office said. In 2008, investors sued Western Pipeline and several of the co-defendants in Dallas County Court, claiming they had been swindled out of $18 million.
Source: http://www.courthousenews.com/2012/01/13/43013.htm

12. *January 13, New York Times* – (National) **Ex-S.E.C. official settles conflict-of-interest case.** A former enforcement official for the Securities and Exchange Commission (SEC) who was accused of blocking or closing at least three investigations into the activities of the Stanford Financial Group, which authorities claim was a $7 billion Ponzi scheme, has settled civil charges brought by the Justice Department accusing him of violating conflict-of-interest rules by later representing Stanford before the commission, the New York Times reported January 13. A U.S. attorney in Texas announced January 13 that the former official, who from 1998 to 2005 served as the enforcement director for the SEC's Fort Worth, Texas regional office, had agreed to a civil settlement that would result in payment of a $50,000 fine. That is the maximum fine for a violation of federal conflict-of-interest rules. A separate civil case involving the employee continues at the SEC. Government officials said at a Congressional hearing last May the official was the subject of a criminal investigation into his work for Stanford, which was also the subject of much of a 150-page report by the SEC's inspector general issued in March 2010. That report found he frequently discouraged or halted further investigation into Stanford Financial by SEC staff, and that he subsequently represented the firm in talks with SEC officials about other or continuing investigations.
Source: http://www.nytimes.com/2012/01/14/business/ex-sec-official-settles-conflict-case.html?_r=1

13. *January 13, U.S. Department of Justice* – (Florida) **Altamonte Springs man convicted of bank fraud.** A U.S. attorney announced January 13 that a federal jury in Florida January 11, found a man guilty of one count of conspiracy to commit bank fraud, six counts of bank fraud, and one count of making a false statement. He faces a maximum penalty of 30 years in prison. According to evidence, the members of the conspiracy set up bank accounts over the Internet using stolen identities. Those accounts were then funded by unauthorized wire transfers made from accounts at other banks. Before the banks could detect the scheme, the conspirators sent the fraud proceeds to accounts in central Florida either by wire transfer or a check that would be deposited. The defendant participated in the scheme by withdrawing some of the fraud proceeds into a central Florida bank account. He also recruited other individuals in central Florida to provide their bank accounts to be used for receipt of the proceeds from the scheme. After funds were transferred to those accounts, he took the individuals he recruited to

multiple bank locations, and over the course of several days, supervised them in the withdrawal of thousands of dollars in fraudulent proceeds. The six bank fraud counts represent more than $396,000 in fraudulent transactions. Two men connected to the scheme have each pled guilty to one count of conspiracy to commit wire and bank fraud, and one count of aggravated identity theft.
Source: http://www.justice.gov/usao/flm/press/2012/jan/2012011_Prophete.html

For more stories, see items **17**, **35**, **46**, and **52**

[Return to top]

Transportation Sector

14. *January 17, Associated Press* – (International) **Italian captain being placed under house arrest.** A lawyer said the captain who allegedly abandoned the crippled Costa Concordia cruise liner off of an island of the coast of Italy January 13 will be released from jail and placed under house arrest, the Associated Press reported January 17. Sky TG24 TV and the Italian news agency ANSA quoted the defense lawyer as saying a judge turned down prosecutors' request to keep the captain of the ship run by an Italian operator and owned by Miami-based Carnival Corp., in jail. However, the lawyer said the judge also rejected a defense bid to set the captain free. Prosecutors accused the captain of the ship of manslaughter, causing a shipwreck, and abandoning his ship before all passengers were evacuated during its grounding. The death toll rose to 11 January 17 when 5 bodies — 4 men and 1 woman — were recovered from the submerged portion of the ship, which ran into a reef, then capsized near the Tuscan island of Giglio. Prior to that discovery, the coast guard raised the number of missing to 25 passengers and 4 crew members. The Costa Concordia was carrying more than 4,200 people when it hit the reef after the captain made an unauthorized deviation from the ship's programmed course, apparently as a favor to his chief waiter, who hailed from the island. The captain insisted he stay aboard until the ship was evacuated. However, a recording of his conversation with an Italian coast guard captain indicates he fled before all passengers were off — and then resisted repeat orders to return. Earlier January 17, Italian naval divers exploded holes in the hull of the grounded cruise ship, trying to speed up the search for the missing while seas were still calm. A Dutch shipwreck salvage firm said it would take engineers and divers 2 to 4 weeks to extract the 500,000 gallons of fuel aboard the ship. Preliminary phases of the fuel extraction could begin as early as January 18 if approved by Italian officials, the company said. Smit, a Netherlands-based salvage company, said no fuel leaked from any of the ship's tanks and the tanks appeared intact. Carnival estimated preliminary losses from having the Concordia out of operation at least through 2012 would be between $85 million and $95 million, along with other costs.
Source: http://www.google.com/hostednews/ap/article/ALeqM5go5FJsdl6HYO7C3zGcQRL3H_Q_FA?docId=93237025c8f2405a98fd31323571274f

15. *January 16, Chicago Sun-Times Media Wire* – (Illinois) **Alleged railroad yard thief nabbed.** The Cook County, Illinois Sheriff's Office announced January 16 the arrest of

a man who allegedly helped steal more than $100,000 in property from a South Side Chicago railroad yard. One of three suspects in a January 11 theft at the Canadian National rail yard was arrested January 14, the sheriff's office said in a release. Authorities learned January 11 about a possible theft where three people allegedly removed railroad ties and other scrap metal, the release said. The property was valued at about $100,000. A witness positively identified a getaway vehicle used in the crime, the release said. On January 12, authorities found the suspect and his vehicle, presumably the getaway vehicle. He was charged with one count of felony theft and one count of criminal trespass to real property. Detectives were eventually able to recover some of the items stolen from the rail yard at local scrap yards, the release said.
Source: http://abclocal.go.com/wls/story?section=news/local&id=8507977

16. *January 16, Fairbanks Daily News-Miner* – (Alaska) **Helicopter accident holds up flights at Fairbanks airport.** The Fairbanks, Alaska International Airport's runway was closed for about 2 hours January 15 after a rotor strike by a helicopter involved in cold weather testing at the airport. None of the three people in the helicopter were injured but it did cause significant damage to the helicopter, a spokeswoman said. Many flights from Anchorage and Seattle were delayed, canceled, or diverted to Anchorage due to the accident. Airport officials could not move the damaged helicopter until the Federal Aviation Administration and National Transportation Safety Board, who are investigating, showed up.
Source: http://newsminer.com/bookmark/17180669-Helicopter-accident-holds-up-flights-at-Fairbanks-airport

For more stories, see items **4**, **9**, **29**, **47**, **51**, and **57**

[Return to top]

Postal and Shipping Sector

17. *January 17, Daily Wilton* – (Connecticut) **Wave of identity theft hits Weston.** The Weston Police Department is advising all residents to be on the lookout for suspicious activity in their bank accounts and in their neighborhood after receiving several reports of mail and identify theft in recent weeks, the Daily Wilton reported January 13. The calls started coming into the police headquarters right before the holidays in 2011, and ranged from stolen mail to unauthorized credit card use, a detective said. There have been six incidents of mail theft and four incidents of unauthorized financial activity in Weston in less than a month — and in a small town such as Weston, that is a big increase. In the mail thefts, thieves are looking for cash or any private data that could lead to accessing personal information.
Source: http://www.thedailywilton.com/news/wave-identity-theft-hits-weston

18. *January 17, Door County Advocate* – (Wisconsin) **Mailbox vandalism exploding in Door County.** Vandals have exploded several mailboxes in Door County, Wisconsin, including two chemical explosions in mailboxes in the city of Sturgeon Bay. There have been seven reports of mailbox damage in metal and plastic mailboxes that included melting and burning one down, the Door County Advocate reported January

17. A homeowner found a rolled-up paper towel saturated with lighter fluid. An unknown person set it on fire, then placed it in the mailbox causing the plastic to melt. Makers of the bombs found in mailboxes in the city are using aluminum foil and chemicals in a plastic bottle, where gas builds up and causes an explosion, a Sturgeon Bay police lieutenant stated. Police have not found any connection as to how the vandals choose the mailboxes they target and so far have no suspects. Someone reaching into the mailbox or the person setting the bomb can be seriously injured, he said.
Source:
http://www.doorcountyadvocate.com/article/20120117/ADV01/120116107/Mailbox-vandalism-exploding-Door-County?odyssey=nav|head

[Return to top]

Agriculture and Food Sector

19. *January 17, New York Daily News* – (Georgia) **New Orleans Saints fan accused of shooting two men who were cheering for San Francisco 49ers outside Applebee's in Georgia.** An angry fan of the New Orleans Saints National Football League team in Georgia took his rage too far when he shot two men cheering for the San Francisco 49ers on the day of San Francisco's NFL playoff victory over New Orleans, police said. The suspect was arrested in the January 14 shooting outside an Applebee's in Duluth. One victim suffered a minor wound to his head, while the other is in critical condition after being shot in the stomach, according to multiple reports. The suspect became enraged when the victims, who were watching the game in Applebee's, cheered after the Niners scored, police said. The suspect faces several charges, including two counts of aggravated assault.
Source: http://www.nydailynews.com/news/national/orleans-saints-fan-accused-shooting-pair-san-francisco-49ers-fans-applebee-georgia-article-1.1007344

20. *January 17, WSOC 9 Charlotte* – (North Carolina) **Suspect in slaying of pregnant woman returned to Charlotte.** Police homicide detectives from Charlotte-Mecklenburg, North Carolina, traveled to Fayetteville to question and pick up a homicide suspect accused of killing a pregnant woman who was working at a restaurant that he robbed. The suspect, who also worked at the restaurant, was returned to Charlotte January 17 and charged with murder and two counts of robbery with a dangerous weapon. Fayetteville police caught up with the suspect January 16 and arrested him in connection with the robbery and slaying of the woman who was working at the Flying Biscuit Cafe in the Ballantyne area of Charlotte. Her body was found near a trash bin in the Stonecrest Shopping Center January 14. Police said the suspect robbed the restaurant, killed the woman, and stole her car. The restaurant was closed but plans to reopen later the week of January 16.
Source: http://www.wsoctv.com/news/30225081/detail.html

21. *January 15, Food Safety News* – (National) **Recall: Diced beef with broken conveyor belt bits.** RSW Distributors of Forest City, North Carolina, is recalling 3,104 pounds of seasoned diced beef that may contain pieces of a damaged conveyor belt, the U.S.

Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) announced January 14. Some of the beef was sent to schools. The FSIS said it instructed the company to hold the diced beef, produced December 9, after a conveyor belt broke during processing. However, the meat was inadvertently shipped, including to schools in South Carolina, Tennessee, and Washington that are part of the USDA's National School Lunch Program.
Source: http://www.foodsafetynews.com/2012/01/meat-damaged-by-belt-failure-recalled-after-mistakenly-shipped/

22. *January 14, Food Safety News* – (Michigan) **E. coli outbreak in Michigan linked to restaurant employee.** Seven people were sickened and four were hospitalized in an outbreak of E. coli O157:H7 linked to a restaurant in Houghton, Michigan. According to a story January 13 in the Houghton Daily Mining Gazette, some of the illnesses were lab-confirmed earlier in January, which alerted health department officials to the outbreak. So far, according to the newspaper, the common factor linking the E. coli infections is that those sickened ate at the Ambassador Restaurant. The Western Upper Peninsula Health Department medical director said the source of the infection was apparently an ill food handler who was asymptomatic.
Source: http://www.foodsafetynews.com/2012/01/e-coli-outbreak-in-michigan-linked-to-restaurant-employee/

23. *January 14, Food Safety News* – (National) **Allergen alert: Barbecue sauce with anchovies.** Herbadashery of Casper, Wyoming, is recalling certain bottles of barbecue dipping sauce because the labels do not specify that the sauce contains anchovies, an allergen, Food Safety News reported January 14. The recall was initiated after an onsite U.S. Food and Drug Administration inspection November 23, found one ingredient, Worcestershire sauce, included anchovies. The recall is for Pine Ridge BBQ and Dipping Sauce, and Pine Ridge Jalapeno BBQ and Dipping Sauce manufactured after January 1, 2011, and distributed through Internet sales and in retail stores from January 1 to September 1.
Source: http://www.foodsafetynews.com/2012/01/allergen-alert-barbecue-sauce-with-anchovies/

24. *January 14, Food Safety News* – (National) **Allergen alert: Stuffed clams with milk, wheat, eggs.** Price Chopper Supermarkets is recalling stuffed clams from its seafood departments because three ingredients — milk, wheat, and eggs — are allergens and are not listed on the label, Food Safety News reported January 14. The recall is for Gourmet Stuffed Clams, sold chain-wide in Price Chopper seafood departments between September 30 and December 30, 2011. According to the company's news release, the store-generated label was updated December 30, 2011 to correctly reflect all of the ingredients contained in the product. The news release did not explain whether the recalled clams would still be available in stores.
Source: http://www.foodsafetynews.com/2012/01/allergen-alert-stuffed-clams-with-milk-wheat-eggs/

25. *January 14, Food Safety News* – (Illinois) **146 norovirus cases linked to Illinois restaurant.** Many of 146 people sickened with norovirus in Wheeling, Illinois, may

have been exposed at Bob Chinn's Crab House, the Cook County Health Department said January 13. Bob Chinn's, which bills itself as the nation's fourth busiest restaurant, closed its doors January 10, after receiving complaints from customers who said they had become sick, and then reopened January 11. "We worked with the [Cook County Department of] Public Health to clean and sanitize the restaurant," said a restaurant spokesman. "We've satisfied all of the requirements, and they've allowed us to reopen." A health department spokeswoman said her agency received dozens of calls from people who said they became sick after eating at the restaurant, but that it is unclear whether the eatery is the source of illness in all of those cases.
Source: http://www.foodsafetynews.com/2012/01/146-norovirus-cases-linked-to-illinois-restaurant/

26. *January 13, Associated Press* – (Missouri) **Missouri meat company Alma Meats expands recall.** A western Missouri meat company expanded its recall to include 137 pounds of cooked head sausage. The Missouri Department of Agriculture (MDA) announced January 12 the sausage was produced September 15, 2011 by Alma Meats. It was distributed within Lafayette County and to 4-K Cheese and Meat in Cole Camp, and The Cheese Store in Sweet Springs. The announcement came after the MDA announced the week of January 2 that inspectors found records indicating Alma sold meat that was improperly handled and not inspected. The initial recall included 320 pounds of meat, including summer sausage, snack sticks, beef jerky, and roast pork. Alma is no longer able to process meat for retail or wholesale distribution, but it will continue to process meat for livestock owners.
Source: http://www.boston.com/business/articles/2012/01/13/missouri_meat_company_alma_meats_expands_recall/

27. *January 13, Wired* – (International) **New animal virus takes northern Europe by surprise.** Scientists in northern Europe are scrambling to learn more about a new virus that causes fetal malformations and stillbirths in cattle, sheep, and goats, Wired reported January 13. For now, scientists do not know about the virus' origins or why it is suddenly causing an outbreak; in order to speed up the process, they want to share the virus and protocols for detecting it with anyone interested in studying the disease or developing diagnostic tools and vaccines. The virus, provisionally named "Schmallenberg virus" after the German town from which the first positive samples came, was detected in November 2011 in dairy cows that showed signs of infection with fever and a drastic reduction in milk production. Now, the virus has also been detected in sheep and goats, and it has shown up at dozens of farms in the Netherlands, and in Belgium. According to the European Commission's Standing Committee on the Food Chain and Animal Health, cases have been detected on 20 farms in Germany, 52 in the Netherlands, and 14 in Belgium. Many more suspected cases are being investigated.
Source: http://www.wired.com/wiredscience/2012/01/new-animal-virus/

For another story, see item **47**

[Return to top]

Water Sector

28. *January 17, Associated Press* – (Virginia) **EPA proposes $160,265 fine for Culpeper over chlorine gas leak, town negotiates with agency.** The town of Culpeper, Virginia faces a potential $160,265 civil fine for a 2008 chlorine gas leak at its sewer plant from the U.S. Environmental Protection Agency (EPA). In a November 15 letter, the agency cited failure to immediately notify the National Response Center and state emergency response commission of the leak. The EPA also said the town lacks proper risk management or written safety procedures to deal with chlorine gas. The Culpeper environmental services director said town officials are negotiating with the EPA. The leak occurred in May 2008 as two employees were charging a chlorine cylinder. Since then, the sewer plant has been upgraded and chlorine is no longer used.
Source:
http://www.therepublic.com/view/story/17fd421c5d1b461c901dc4378604ccb0/VA--Culpeper-Leak-Fine/

29. *January 16, Miami Herald* – (Florida) **Report: Sewage pipe in sorry shape.** An aging pipeline carrying 25 millions gallons of raw sewage a day under Government Cut in Port of Miami has at least three sections so brittle that a consultant has warned Miami-Dade County, Florida, it could potentially rupture under normal working conditions. County engineers acknowledge it will make an on-going $32 million job to replace the line before a major Port of Miami dredging project more complicated and expensive. The weakest segments are close to the spot contractors had targeted to drill into the existing concrete pipe to connect to a new shaft. The findings significantly raise the risk of the fragile pipe crumbling during that critical phase of work. “If this were to fail, I think it would be a catastrophic event,” said the director of the Miami-Dade Water and Sewer Department. He expects new proposals and estimates back from contractors within weeks.
Source: http://www.miamiherald.com/2012/01/13/2588431/report-sewage-pipe-in-sorry-shape.html

30. *January 12, Harrisburg Daily Register* – (Illinois) **New pump motors installed in Harrisburg sub-levee.** A crew from Vandevanter Engineering of Fenton, Missouri, installed two motors in the new pumping station at Harrisburg, Illinois, Sewerage Treatment Plant’s sub-levee January 11, an addition that will boost the pumping capacity to a level that is expected to save the plant from future flooding danger. The pumping station will use two 20,000 gallon per minute motors with impellers to pump water into a pipe buried about a foot beneath the surface of the main levee. The new pumps are expected to more rapidly lower water flowing from Pankey Branch to the original pumping station.
Source: http://www.dailyregister.com/news/x338369234/New-pump-motors-installed-in-Harrisburg-sub-levee

For more stories, see items **47** and **56**

[Return to top]

Public Health and Healthcare Sector

31. *January 16, DOTmed.com* – (National) **FDA fingers.** The Food and Drug Administration (DOT) said January 12 a preliminary investigation suggests "improper usage" of CardioGen-82 generators led to the increased patient radiation exposure that triggered last summer's product recall. In a safety announcement, the FDA said ongoing tests carried out by the nuclear medicine agent's manufacturer, Bracco Diagnostics Inc., have shown manufacturing "deficiencies" noted by the agency do not seem related to the heightened radiation exposure detected in some patients. The CardioGen-82 generator was recalled in July, after three patients set off very sensitive radiation detectors at the U.S. border. It turned out the patients had all undergone PET stress tests using the substance several months earlier. The FDA said the problem that led to the recall, which was voluntarily ordered by Bracco, was likely caused by a "strontium breakthrough," meaning radioactive strontium isotopes used to create the PET agent were inadvertently injected into the patients. "None of the tested generators showed signs of [strontium] breakthrough. FDA continues to work with the manufacturer to resolve their manufacturing deficiencies," the agency said.
Source: http://www.dotmed.com/news/story/17843/

32. *January 15, Bloomberg* – (National) **Drug shortages raise risk of cancer counterfeits, U.S. says.** Shortages of some injectable cancer drugs have created an opening for dangerous unapproved versions of Roche Holding AG's Herceptin and Amgen Inc.'s Neupogen to be sold to clinics and other health-care providers. The Food and Drug Administration (FDA) issued a notice January 13 warning providers to avoid direct solicitations from unproven sources and only buy drugs through approved channels. Unapproved versions of Roche's Rituxan and AstraZeneca Plc's Faslodex have also been sold. The quality of such products is often jeopardized, putting patients at risk, the agency said. Though some injectable cancer medications are in short supply, none of the unapproved products are on the shortage list. "Amgen is aware of and is cooperating with the FDA on investigations related to the illegal importation of Amgen product that is approved for sale in other regions, but unapproved for sale in the U.S. and being sold on the Internet and directly to U.S. clinics," a spokeswoman for the Thousand Oaks, California-based company said in an e-mail.
Source: http://www.businessweek.com/news/2012-01-15/drug-shortages-raise-risk-of-cancer-counterfeits-u-s-says.html

[Return to top]

Government Facilities Sector

33. *January 17, City News Service* – (California) **San Diego elementry school closed after arson fire.** An fire caused an estimated $600,000 damage to the gymnasium, cafeteria, and possibly administration building of an elementary school in the University Heights area of San Diego January 17, authorities said. The fire at Alice Birney Elementary School was reported January 16, according to a San Diego fire-rescue dispatcher. About 50 firefighters responded to the incident, the San Diego fire-rescue battalion

chief said, noting it took about 20 minutes to control the fire.
Source: http://www.kpbs.org/news/2012/jan/17/fire-damages-university-city-elementry-school/

34. *January 17, WTMJ 4 Milwaukee* – (Wisconsin) **City of Milwaukee phone service interrupted.** A spokeswoman for the the City of Milwaukee said January 17 the phone service for many of its offices had been interrupted. People were not able to call in to any city office that includes a 286 prefix. That office includes many Milwaukee Fire non-emergency numbers. Service for Milwaukee Police and 911 was believed not to be affected. According to a spokeswoman, the telecommunications staff was working with AT&T to try and solve the problem.
Source: http://www.todaystmj4.com/news/local/137484353.html

35. *January 14, Softpedia* – (International) **San Francisco college exposed to hackers since 1999.** City College of San Francisco staff members noticed computers found in a lab were infected with a computer virus. A thorough investigation found the institution's networks were plagued with malicious software from more than a decade ago, Softpedia reported January 14. Originating from countries such as Russia, Iran, the United States, and China, the malware was harvesting sensitive information and sending it to people who controlled the viruses, the San Francisco Chronicle reported. City college's CTO shut down the first lab that was found to be infected, but he soon realized the problem was much more serious than initially believed, some of the threats being present since 1999. While some of the data collected by the malicious software was unimportant, such as lesson plans, other information that the viruses could have accessed represented sensitive information, such as banking information.
Source: http://news.softpedia.com/news/San-Francisco-College-Exposed-to-Hackers-Since-1999-246558.shtml

36. *January 13, WPEC 12 West Palm Beach* – (Florida) **Suspicious package found at St. Lucie County Clerk of Courts office.** State health officials investigated a package that forced the evacuation of a building in Fort Pierce, Florida, January 13. The clerk of courts office was on lockdown for a few hours when a suspicious package was discovered. Sheriff's officials, fire-rescue, and haz-mat crews were called to the scene. The package was delivered to the fourth floor of the clerk of courts office. Three St. Lucie County deputies, and five clerk of courts employees were taken to the hospital as a precaution.
Source: http://www.cbs12.com/articles/pierce-4738061-courts-office.html

37. *January 12, WJZ 13 Baltimore* – (Maryland) **Scarlet fever outbreak at southwest Baltimore school; 3 students confirmed sick.** A warning was issued from the Baltimore City Health Department about a confirmed outbreak of scarlet fever at George Washington Elementary in southwest Baltimore, WJZ 13 Baltimore reported January 12. Doctors said it is extremely contagious in kids. The school is sanitizing the area that was exposed. The city school system told WJZ three students in the same class contracted the illness. It prompted the school system to send a letter to parents and guardians. Scarlet fever is a rash illness caused by the Streptococcus bacteria. Symptoms usually appear 1 to 5 days after exposure and include rash on the neck and

chest, high fever, sore throat, and swollen glands. The bacteria is spread from person-to-person contact, and by respiratory secretions like sneezing and coughing. Doctors said while scarlet fever is highly contagious, it is also very treatable, most often with antibiotics.
Source: http://baltimore.cbslocal.com/2012/01/12/scarlet-fever-outbreak-at-southwest-baltimore-school-3-students-confirmed-sick/?hpt=us_bn5

For more stories, see items **21** and **51**

[Return to top]

Emergency Services Sector

38. *January 17, KTBS 3 Shreveport* – (Georgia) **Cops: Jailed man smuggled gun in rectum.** Corrections officials in Onslow County, Georgia said they think they have solved the mystery of how a man managed to smuggle a .38-caliber handgun into his jail cell: He used his rectum. According to a news release, the Onslow County Sheriff's Office said the 10-inch-long weapon was found in the jail cell of an inmate, following his arrest a day before on drug-related charges during a traffic stop. Investigators said the inmate was also a wanted fugitive on a murder warrant out of Atlanta. Corrections officials told MSNBC the inmate underwent a strip search during his booking, but that nothing turned up. Authorities said the handgun was discovered in the jail cell toilet after he told corrections staff he found the weapon in his cell. Deputies said the gun was test fired and found to be operational.
Source: http://www.ktbs.com/news/30230011/detail.html

39. *January 17, Associated Press* – (Maryland) **3 arrested in theft of police items from cruiser in Montgomery Co.** Three people were arrested January 16, after an off-duty police officer caught the group stealing a police radio and vest from his cruiser, Montgomery County, Maryland police said. The three suspects, two men and a juvenile, fled in a maroon minivan that was reported stolen January 15 and were then involved in a hit-and-run accident, police said. The suspects abandoned the minivan, and police apprehended them in Silver Spring.
Source: http://www.baltimoresun.com/news/breaking/bal-md-ap-montgomery-police-theft-0117,0,2835581.story

40. *January 16, Baltimore Sun* – (Maryland) **State Police arrest six members of Occupy Baltimore.** Maryland State Police arrested six members of Occupy Baltimore January 16 for allegedly trespassing on the state-owned site of a proposed juvenile detention center in East Baltimore. The arrests of four men and two women came about 2 hours after they began erecting a plywood structure — painted red and representing a schoolhouse — inside the fenced site at East Madison and Graves streets near the city's complex of jails and prisons. A state police spokesman said the six individuals were told they were entering private property, which is owned by the Maryland Department of Public Safety and Correctional Services. Several troopers stationed inside the site tried to negotiate with the protesters building the structure, encouraging them to leave, he said. The six individuals had erected four walls and six roof trusses before they were

arrested. They were being processed at central booking and each was charged with trespassing, the spokesman said. He stated troopers were securing the area January 16 when members of Occupy Baltimore pulled up and started moving materials over the chain link fence.
Source: http://articles.baltimoresun.com/2012-01-16/news/bs-md-ci-occupy-school-20120116-13_1_juvenile-detention-center-chain-link-fence-arrest

41. *January 14, Associated Press* – (Arizona) **Inmate crew finds riot grenades along I-10 in Benson, 1 accidentally detonates.** Members of an Arizona Department of Corrections inmate work crew found three riot grenades under a tree alongside Interstate 10 in Benson, and one went off. The Cochise County Sheriff's Office said in a release the grenade went off January 12 after an inmate picked it up and its safety pin caught on a branch. The inmate threw the grenade over the highway fence, and it exploded. Deputies found two other grenades, one in working order. The sheriff's office said the riot grenades contained small rubber balls and chemical spray. None had serial numbers or markings, and no packaging material that could help identify their source was found.
Source: http://www.therepublic.com/view/story/e52d892e605b43c4ac5e6639652a90c3/AZ--Grenades-Found/

42. *January 12, Cullman Times* – (Alabama) **EMA office hit by lightning strike.** A storm late January 10 caused little damage across Cullman County, Alabama, but it did produce a lightning bolt that landed directly on the Emergency Management Agency's SE office — knocking out everything from the Internet connection to the hard-wired phone system. With cell phones and wireless Internet cards as the only means of communication, the (EMA) office seemed more akin to a mobile command center than the area's disaster coordination hub following the January 10 storm. The Cullman County EMA director said most of the communication issues were ironed out by the evening of January 11, though it could take some time until everything is repaired.
Source: http://www.cullmantimes.com/local/x2145132459/EMA-office-hit-by-lightning-strike

For more stories, see items **34**, **36**, and **53**

[Return to top]

Information Technology Sector

43. *January 17, H Security* – (International) **Apache Tomcat developers advise updates to avoid DoS.** The Apache Tomcat developers are advising users of the 7.0.x, 6.0.x, and 5.5.x branches of the Java servlet and JSP container to update to the latest released versions 7.0.23, 6.0.35, and 5.5.35. Recent investigations revealed inefficiencies in how large numbers of parameters and parameter values were handled by Tomcat. Analysis of the recent hash collision denial-of-service vulnerability allowed the developers to identify "unrelated inefficiencies" which could be exploited by a specially crafted request, causing large amounts of CPU to be consumed. To address the issue, the

developers modified the code to efficiently process large numbers of parameters and values.
Source: http://www.h-online.com/security/news/item/Apache-Tomcat-developers-advise-updates-to-avoid-DoS-1414580.html

44. *January 16, H Security* – (International) **Critical hole in McAfee products still open after more than 180 days.** Zero Day Initiative (ZDI) released information on a security problem in McAfee's Security-as-a-Service products (SaaS). The vulnerability broker said it told McAfee about the hole in April 2011, and it now decided to publicly release the information because the vendor still has not provided a patch. The flaw is contained in the myCIOScn.dll program library. In this library, the MyCioScan.Scan.ShowReport() method insufficiently filters user input and executes embedded commands within the context of the browser. The flaw can be exploited when a user opens a specially crafted file or Web page. ZDI rates the issue as very severe and has given it a CVSS score of 9 –- maximum severity is 10. ZDI's advisory does not state exactly which products are affected. McAfee's range of SaaS products includes "SaaS Email Encryption" for encrypting e-mails, and "Vulnerability Assessment SaaS," which checks software for potential vulnerabilities.
Source: http://www.h-online.com/security/news/item/Critical-hole-in-McAfee-products-still-open-after-more-than-180-days-1413775.html

45. *January 16, H Security* – (International) **Linux developers fix a homemade network problem.** Linux kernels 3.0.17, 3.1.9, and 3.2.1 fix a problem with the handling of IGMP packets that was introduced with updates in Linux 2.6.36. An IGMPv3 protocol packet being processed soon after the processing of an IGMPv2 packet could lead to a system crash caused by a kernel panic. On January 6, a researcher reported strange crashes of his Linux notebook in the Debian bug database. A Debian developer found the problem was caused by a division by 0 that can occur with IGMP packets that have a Maximum Response Time of 0. As a result, Linux systems running a kernel version from 2.6.36 or later, up until the patched versions, can be crashed remotely using certain IGMP packets if a program has registered to receive multicast packets from the network. Typical examples for such programs include the avahi mDNS server or media players, such as VLC, that support RTP. Active attacks should technically only be possible within local networks, because IGMP broadcasts are usually not routed beyond network boundaries. However, the Debian developer pointed out particular unicast packets may serve for attacks via the Internet unless they are blocked by a firewall. As a fix was released, distributors should soon offer updated kernel packages that no longer contain the vulnerability.
Source: http://www.h-online.com/security/news/item/Linux-developers-fix-a-homemade-network-problem-1414033.html

46. *January 13, IDG News Service* – (International) **Facebook chat phishing attack impersonates Facebook security team.** A new phishing attack spreading through Facebook chat modifies hijacked accounts to impersonate the social network's security team. The attackers replace the profile picture of compromised accounts with the Facebook logo and change their names to a variation of "Facebook Security" written with special Unicode characters, said a Kaspersky Lab expert. Facebook claims

changing the profile name can take up to 24 hours and is subject to confirmation. However, in the expert's tests the change occurred almost instantly and required only the password. This was also confirmed by a victim whose profile name was modified within 5 minutes of their account being compromised, he said. After the victim's profile name and picture get changed, the attackers send out a chat message to all of their contacts informing them their accounts will be suspended unless they re-confirm their information. The rogue messages appear to be signed by "The Facebook Team" and contain a link to a phishing page hosted on an external domain. The Web page mimics Facebook's design and asks for name, e-mail, password, security question, country, birth date, and other information needed to hijack the account. However, the attack does not stop there. According to the expert, a second form asks users for their credit card details and billing address. This is unusual for Facebook phishing attacks, the majority of which target only social networking account information.
Source:
http://www.computerworld.com/s/article/9223432/Facebook_chat_phishing_attack_impersonates_Facebook_security_team?taxonomyId=17

47. *January 13, Infosecurity* – (International) **Open Automation Software plugs DoS flaw in ICS application.** Open Automation Software issued a patch for a vulnerability to its OPC Systems.NET industrial control system application that could be used for a denial of service attack. The vulnerability is remotely exploitable by sending a malformed .NET remote procedural call packet to cause a denial of service through Port 58723/TCP, explained the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in an advisory. All versions of OPC Systems.NET prior to version 5.0 are affected. There are public exploits that target this vulnerability, which requires a moderate skill level to exploit, the advisory said. OPC Systems.NET is a human-machine interface application deployed across several sectors, including manufacturing, information technology, energy, water and wastewater, defense, and others. A researcher publicly reported the vulnerability in OPC Systems.NET along with proof-of-concept exploit code. This report was released without coordination with Open Automation Software, ICS-CERT, or any other coordinating entity known to ICS-CERT, the advisory noted. ICS-CERT worked with Open Automation Software to fix the security hole, a fix which the researcher confirmed is effective, the advisory said.
Source: http://www.infosecurity-magazine.com/view/23217/

48. *January 13, msnbc.com* – (International) **Popular live-blogging site says data files were breached.** CoveritLive, a popular, Web-based live-blogging program used worldwide, said January 13 it discovered "certain proprietary data files" of its users "were accessed without authorization," but "no financial account information has been compromised. We have not yet determined if, or to what extent, CoveritLive account information (i.e., user names, email addresses and/or passwords) was accessed," Demand Media, which bought CoveritLive in 2011, said in an e-mail to its users. Those users include bloggers, journalists, and mainstream media organizations, including msnbc.com, FoxNews.com, ESPN, and the BBC. Many people use CoveritLive's free services, but there are premium accounts. Live-blogged events hosted by CoveritLive draw more than 60 million people every month, the company says, 60 percent of whom

are from outside the United States. CoveritLive said the files were breached "starting on or about" January 7, and an investigation is "ongoing." In the meantime, as a "precautionary measure," all users were asked to re-set their passwords January 14.
Source: http://technolog.msnbc.msn.com/_news/2012/01/13/10152434-popular-live-blogging-site-says-data-files-were-breached

49. *January 13, Threatpost* – (International) **Smashing the Linux heap.** A researcher found there is a heap allocator in the Linux kernel that is extremely exploitable. The security consultant at Virtual Security Research, who does work on Linux kernel research, investigated heap allocators in the operating system's kernel. There are three main allocators: SLUB, SLAB, and SLOB. The researcher focused on SLOB, mainly because there has not been as much research done on it. In a talk at the Infiltrate conference, the researcher said he found virtually nothing in the way of methods to mitigate exploit attempts. SLOB is mainly used in embedded systems, favored there because of its small footprint, he said. Any given system will only have one allocator, and SLOB is used in Linux systems on many routers and switches and also in some firmware systems. In his talk, he presented several possible overflow scenarios that could be exploitable, ranging from the simple to the highly complex.
Source: http://threatpost.com/en_us/blogs/smashing-linux-heap-011312

For more stories, see items **9**, **35**, **50**, and **52**

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

50. *January 17, H Security* – (International) **T-Mobile USA hacked.** A group of hackers that goes by the name "TeaMp0isoN" claims to have obtained access credentials belonging to staff at US Deutsche Telekom subsidiary T-Mobile USA, H Security reported January 17. To back up their claim, the hackers posted data to the Pastebin anonymous text hosting service. One member of the group told Softpedia the hack involved exploiting SQL injection vulnerabilities on the t-mobile.com and newsroom.t-mobile.com Web sites. According to T-Mobile, the problem was limited to the T-Mobile USA newsroom. This would limit the scale of any problems arising as a result -- the intruders may be able to publish fake press releases. Based on the information provided, private customer data was never at risk. Most of the passwords consist of a simple six-digit number composed of two numbers repeated such as "112112." T-Mobile USA said it has now fixed the vulnerabilities.
Source: http://www.h-online.com/security/news/item/T-Mobile-USA-hacked-1414307.html

51. *January 13, IDG News Service* – (National) **Federal body concludes LightSquared can't work with GPS.** A key federal agency involved in testing the proposed LightSquared Long-Term Evolution (LTE) network has concluded there is no practical way to solve interference between that network and the Global Positioning System (GPS), possibly dealing a crippling blow to the startup carrier's hopes for a terrestrial mobile network. In a memo released January 13, the National Space-Based Positioning, Navigation, and Timing Executive Committee (PNT ExComm) said the nine federal agencies that make up the body had concluded unanimously that none of LightSquared's proposals would overcome significant interference with GPS. LightSquared in 2010 received a waiver from the Federal Communications Commission (FCC) allowing it to operate a terrestrial LTE network on frequencies that have until now been devoted to much weaker satellite signals. The PNT ExComm has been involved in testing and results analysis at the request of the FCC and the National Telecommunications and Information Administration (NTIA). Both the original and modified proposals by LightSquared would cause harmful interference to many GPS receivers, the PNT ExComm chairs said in the memo. The agency also said a Federal Aviation Administration analysis had concluded the network would be incompatible with aircraft safety systems.
    Source: http://www.computerworld.com/s/article/9223447/Federal_body_concludes_LightSquared_can_t_work_with_GPS

For another story, see item **46**

[Return to top]

Commercial Facilities Sector

52. *January 16, Fox News* – (International) **Hackers zap Zappos: Info from 24 million users stolen.** Popular online shoe retailer Zappos.com said January 15 that hackers accessed its network and stole account information from as many as 24 million customers. Credit card information was not stolen, the company CEO said in a statement sent to users, but e-mail addresses, billing, and shipping addresses, phone numbers, the last four digits from credit cards — and more — may have been compromised. The company said it already reset the passwords for existing customers to prevent abuse of the stolen data.
    Source: http://www.foxnews.com/scitech/2012/01/16/zappos-zapped-hackers-steal-info-from-24-million-users/?test=latestnews

53. *January 16, New York Daily News* – (New York) **2 firefighters blown 30 feet as gas leak sparks fireball in Rockland County.** Two Rockland County, New York firefighters were seriously burned January 16 when a townhouse they were evacuating exploded because of leaking gas, authorities said. Two volunteer firefighters were knocking on the front door of the home in West Haverstraw when the massive blast tossed them nearly 30 feet and destroyed the building. The gas leak that set off the explosion was apparently caused by a crew of Verizon contract workers, who ruptured the gas main while digging. The gas swept through sewers and into the townhouses as

firefighters and utility workers were evacuating the buildings. Two utility workers checking storm drains for gas when the explosion hit suffered less serious injuries, officials said. Hundreds of people were evacuated from their homes after the explosion. Most were expected to be allowed back January 17.
Source: http://www.nydailynews.com/new-york/2-firefighters-blown-30-feet-gas-leak-sparks-fireball-rockland-county-article-1.1007314

54. *January 15, Elyria Chronicle-Telegram* – (Ohio) **Huge blaze engulfs Columbia complex.** Firefighters from nine area departments battled a fire believed to have caused extensive damage to a large building in Columbia Township, Ohio, January 14 that housed a number of businesses and the township Eagles club. A Columbia Township fire official said as he and groups of firefighters kept entering and leaving the corrugated steel building, smoke grew so thick that it obscured firefighters and vehicles. An estimated 30 to 40 firefighters from 7 departments in Lorain, Medina, and Cuyahoga counties provided mutual aid. Plumes of thick smoke could be seen half a mile away. Smoke continued to clear and then thicken again as firefighters kept running into hot spots.
Source: http://chronicle.northcoastnow.com/2012/01/15/huge-blaze-engulfs-columbia-complex/

55. *January 14, Kansas City Star* – (Missouri) **Two wounded at Independence Center mall.** Police in Independence, Missouri, were searching for several shooters January 14 who opened fire and wounded two people — a man and a woman — at the Independence Center Mall. The quick series of shots described by many customers apparently followed a fight among as many as four individuals near the Sears department store, said a police captain. Units from several area law enforcement agencies converged on the shopping center after Independence police began receiving calls reporting the shots and locked down the building. Among them were the Kansas City and Blue Springs police departments, the Jackson County sheriff's office, and the Missouri State Highway Patrol.
Source: http://www.kansascity.com/2012/01/14/3370884/two-shot-at-independence-center.html

For more stories, see items **2** and **48**

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

56. *January 17, Associated Press* – (South Dakota) **Repairs planned for Pierre causeway.** A causeway that connects the city of Pierre, South Dakota, to LaFramboise

Island on the Missouri River will be rebuilt. Parts of the causeway were washed away last spring and summer by Missouri River flooding. Now the U.S. Army Corps of Engineers said it will spend up to $2 million for repairs. The causeway provides access to four city drinking water wells on LaFramboise Island that have not been used since last year's flooding. The Oahe Dam project manager is hopeful the rebuilding will be finished this year. The mayor of Pierre said the city will pay part of the repair cost.
Source: http://www.therepublic.com/view/story/39e6f9579874499c92bb70fac75e83f4/SD--Causeway-Construction/

57. *January 13, KOMO 4 Seattle* – (Washington) **Hole found under Ballard Locks, closure coming.** The U.S. Army Corps of Engineers found a hole under the foundation of the 95-year-old Ballard Locks in Seattle, and began a 60-day, $1.3 million repair job January 13 to fill the hole and prevent further erosion. The hole, or scour, was caused by moving water eroding the foundation under the small lock, according to the Corps. "There have been scour problems documented in a nearby area for 30 years," a hydraulic engineer said in a press release. Repair work will likely mean the Ballard Locks will be closed to all visitor and vessel traffic for a few days during the final week of January.
Source: http://ballard.komonews.com/news/public-spaces/708588-hole-found-under-ballard-locks-closure-coming

58. *January 12, New Orleans Times-Picayune* – (Louisiana) **Louisiana coastal restoration 50-year blueprint released.** Declaring Louisiana's loss of coastal wetlands "nothing short of a national emergency," state officials January 12 released a $50-billion, 50-year strategy for rebuilding land and increasing protection from storm surge for coastal communities that they say can be paid for with money the state is reasonably sure it will receive. The strategy is outlined in the Coastal Protection and Restoration Authority's draft 5-year master plan update, which for the first time contains maps showing the location and scope of proposed projects, and maps showing what the state's coastline will look like in 2061 if they are built. Lists of the projects also show their cost. The state has lost 1,883 square miles of land during the past 80 years, and the authority chairman said it is impossible to return the state's coastline to its 1930s condition. Even having a coastline in 2061 that resembles the current one might be impossible, he said. The plan calls for allocating half of the $50 billion to risk-reduction projects such as levees, and half to restoration projects.
Source: http://www.nola.com/environment/index.ssf/2012/01/louisiana_releases_50-year_blu.html

For another story, see item **30**

[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