Daily Open Source Infrastructure Report
26 October 2012

Top Stories

- A toxic cloud formed after 300 gallons of hydrochloric acid leaked at a storage facility near Texas City, Texas. The cloud forced thousands of residents indoors and sent nine people to hospitals, an emergency management official said October 25. – *CNN* (See item 2)
- The United States filed a civil mortgage fraud lawsuit against Bank of America, accusing it of selling thousands of toxic home loans to Fannie Mae and Freddie Mac that went into default and caused more than $1 billion of losses, Reuters reported October 24. – *Reuters* (See item 10)
- A fraud ring that attacked financial transfer systems in an attempt to target wealthy high-end banking customers used a complicated web of malware and compromised servers in several countries to steal an estimated $78 million earlier in 2012, according to an analysis by McAfee and Guardian Analytics. – *Threatpost* (See item 14)
- A federal cyber emergency response team issued a warning that DomainKeys Identified Mail (DKIM) verifiers that use low-grade encryption are open to being spoofed and need to be upgraded. This problem was found to affect some of the biggest companies in the tech industry and several large banks. – *The Register* (See item 45)

Fast Jump Menu

Energy Sector

1. *October 24, Atlanta Business Chronicle* – (National) **Midwest drought idles Georgia ethanol plant.** Georgia's only major producer of corn ethanol is temporarily shutting down its plant near Camilla, Georgia, citing the impact the drought in the Midwest is having on corn prices. Southwest Georgia Ethanol LLC (SWGE) announced October 24, that 2012's poor harvest not only is resulting in negative "crush margins" — a term for profitability in the ethanol business — but also is producing lower quality corn. "SWGE modeled all possible scenarios of slowing production and deemed it in SWGE's best financial interest to idle production until the markets return to levels conducive to profits," the company wrote in a news release.
   Source: http://www.bizjournals.com/atlanta/news/2012/10/24/midwest-drought-idles-georgia-ethanol.html

For more stories, see items **24** and **55**

[Return to top]

Chemical Industry Sector

2. *October 25, CNN* – (Texas) **Toxic cloud forces thousands in southeast Texas to stay indoors.** A toxic cloud that formed after 300 gallons of hydrochloric acid leaked at a southeast Texas storage facility sent nine people to hospitals and forced thousands of residents indoors, an emergency management official said October 25. Four firefighters were among those who were hospitalized for exposure after a tank ruptured at a storage facility near the Port of Texas City, a spokesman of the local emergency management office said. More than 45,000 residents of Texas City were ordered to remain indoors, turn off air conditioning units, and make sure all windows and doors were closed until the vapor cloud dissipated. Officials did not immediately detail what caused the tank to rupture at the Dallas Group of America's facility near the port. City officials were

working to clean up the leak, the spokesman told KTRK 13 Houston. None of those exposed to the chemical cloud sustained life-threatening injuries, according to KTRK 13 Houston.
Source: http://www.cnn.com/2012/10/25/us/texas-chemical-leak/index.html

For another story, see item **18**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

3. *October 25, Associated Press* – (International) **Japan nuke plant water worries rise.** Japan's crippled Fukushima Daiichi nuclear power plant is struggling to find space to store tens of thousands of tons of highly contaminated water used to cool the broken reactors, the manager of the water treatment team told the Associated Press October 25. About 200,000 tons of radioactive water is being stored in hundreds of tanks built around the plant. Operator Tokyo Electric Power Co. (TEPCO) already chopped down trees to make room for more tanks and predicts the volume of water will more than triple within three years. TEPCO is close to running a new treatment system that could make the water safe enough to release into the ocean. But in the meantime its tanks are filling up — mostly because leaks in reactor facilities are allowing ground water to pour in. Outside experts worry if contaminated water is released, there will be lasting impact on the environment. They fear, because of the reactor leaks and water flowing from one part of the plant to another, which may already be happening.
Source: http://www.businessweek.com/ap/2012-10-25/ap-interview-japan-nuke-plant-water-worries-rise

4. *October 25, Bluefield Daily Telegraph* – (Virginia) **Va. reactor shutdown due to circuit card failure.** Dominion Virginia Power is replacing a faulty electronic circuit card that caused a reactor to shut down at its North Anna power station in Louisa County, Virginia, the Bluefield Daily Telegraph reported October 25. Unit 2 at the plant tripped automatically October 24. A Dominion Virginia Power spokesman said that the circuit card failed, causing four valves to close. The valves control the flow of steam in the turbine system. He said the reactor was expected to be back on line soon.
Source: http://bdtonline.com/vanews/x1200650098/Va-reactor-shutdown-due-to-circuit-card-failure

For another story, see item **20**

[Return to top]

Critical Manufacturing Sector

5. *October 25, WCNC 22 Charlotte* – (North Carolina) **Fire damages Freightliner plant in Gastonia.** Officials were investigating a fire that broke out at a Freightliner plant in Gastonia, North Carolina, October 25. The first arriving fire engine encountered heavy smoke and called a second alarm, according to officials. The fire was deep within the

building, involving the filtration system of a multi-unit welding area. Estimated equipment damage was $75,000 to $100,000, with no significant damage to the building. The manager estimated $1 million of lost production time, according to officials.
Source: http://www.wcnc.com/news/local/Fire-damages-plant-in-Gastonia-Co--175759841.html

For another story, see item **39**

[Return to top]

Defense Industrial Base Sector

6. *October 24, San Antonio Express* – (International) **Woman gets two years for exporting sensitive parts to Iran.** A Taiwanese woman was sentenced October 24 in San Antonio to 2 years in federal prison for providing sensitive military parts to Iran that authorities claim might be used against the United States. She pleaded guilty in July to a conspiracy charge for circumventing regulations barring the export of certain materials to Iran, which is on a list of countries that the U.S. designates as state sponsors of terrorism. From October 2007 to June 2011, the woman worked with an accomplice from Iran and an accomplice from the United Arab Emirates. They reportedly bought or attempted to buy from companies around the world more than 105,000 parts, valued at about $2.6 million. The woman and her partners conducted 599 transactions with 63 different U.S. companies for parts without notifying them the items were being shipped to Iran. The parts included underwater locator beacons, crystal oscillators used in military and aerospace applications, test cells for measuring electromagnetic radiation, broadband high-range signal amplifiers, RF network design and spectrum management software, and other equipment for military applications made to withstand rugged conditions.
Source: http://www.mysanantonio.com/news/local_news/article/Woman-gets-two-years-for-exporting-sensitive-3978433.php

For another story, see item **39**

[Return to top]

Banking and Finance Sector

7. *October 25, Help Net Security* – (District of Columbia) **Banker pleads guilty to sharing personal information of account-holders.** A former personal banker from Washington, D.C., pleaded guilty to conspiracy to commit bank fraud for his role in an identity theft scheme involving $121,400 in forged checks, Help Net Security reported October 25. According to a statement of offense, he and others participated in the scheme from November 2009 until January 2010, conspiring to steal funds from the accounts of customers of Wachovia Bank, now operating as Wells Fargo Bank. He began participating in the scheme after he was approached by another person at the bank branch where he worked. The person offered to pay him for providing the type of

customer information that would be needed to fraudulently obtain funds from customer accounts with balances of at least $15,000. He subsequently obtained this information concerning the accounts of seven customers, including their dates of births, addresses, telephone numbers, and Social Security numbers, then turned over the information and received $2,000 in cash. Various members of the conspiracy obtained $72,800 and attempted to obtain another $48,600 by forging checks drawn on five of the accounts targeted by the banker.
Source: http://www.net-security.org/secworld.php?id=13839

8. *October 24, American Banker* – (International) **ATMs may be top targets for crime: Verizon report.** More than half of intrusions in the financial industry in a recent study led by Verizon involved tampering with ATMs, the company said in a report published October 24. Overall, 61 percent of security threats involved physical tampering, including the installation of skimming and camera devices on ATMs. Roughly one in four threats involved malware that captures user names and passwords. Another 22 percent involved hacking. According to the study, 56 percent of data breaches compromised ATMs. Another 21 percent of attacks compromised database servers, while 13 percent involved Web servers. Overall, 96 percent of threats to banks originated externally and emanated mostly from professional criminal organizations in Eastern Europe and elsewhere, according to the study. Still, 9 percent of breaches involved employees of the target company, one of the highest rates of internal breaches among industries the group examined. Insiders were people who typically handled financial transactions, such as bank tellers and loan officers, the study found.
Source: http://www.americanbanker.com/issues/177_206/atm-may-be-top-targets-for-crime-1053833-1.html

9. *October 24, Las Vegas Review-Journal* – (Nevada; California) **Henderson man faces charges in $15 million Ponzi scheme.** A Henderson, Nevada man is facing federal charges in Los Angeles in what authorities allege is a $15 million Ponzi scheme, the Las Vegas Review-Journal reported October 24. The man was arrested in Las Vegas on charges including mail and wire fraud in the investment scheme, the Los Angeles U.S. Attorney's Office said in a news release. According to the indictment, the man falsely told investors he was producing earnings of 1 percent to 5 percent a week through a commodity futures trading program. In reality, his trading activity was unprofitable, causing him to lose nearly all the money he used to trade commodities. Federal authorities think he took in at least $15 million in the scheme and that his investors lost at least $9 million. He solicited investments through Nevada-based companies, including Axcess Automation LLC, and a hedge fund he called Axcess Fund LP. In addition to the fraud allegations, he is accused of lying to the U.S. Securities and Exchange Commission.
Source: http://www.lvrj.com/news/henderson-man-faces-charges-in-15-million-ponzi-scheme-175704591.html

10. *October 24, Reuters* – (National) **U.S. sues BofA over alleged mortgage fraud.** The United States filed a civil mortgage fraud lawsuit against Bank of America, accusing it of selling thousands of toxic home loans to Fannie Mae and Freddie Mac that went into default and caused more than $1 billion of losses, Reuters reported October 24. The

case, originally brought by a whistleblower, is the U.S. Department of Justice's first civil fraud lawsuit over mortgage loans sold to Fannie Mae or Freddie Mac. According to a complaint filed in Manhattan federal court, Countrywide in 2007 invented a scheme known as the "Hustle" designed to speed up processing of residential home loans. Operating under the motto "Loans Move Forward, Never Backward," mortgage executives tried to eliminate "toll gates" designed to ensure that loans were sound and not tainted by fraud, the government said. This resulted in "defect rates" that were roughly nine times the industry norm, but Countrywide concealed this from Fannie Mae and Freddie Mac, and even awarded bonuses to staff to "rebut" the problems being discovered, it added. The scheme ran through 2009 and caused "countless" foreclosures, the lawsuit alleged.
Source: http://bottomline.nbcnews.com/_news/2012/10/24/14671246-us-sues-bofa-over-alleged-mortgage-fraud?lite

11. *October 24, Dark Reading* – (National) **Barnes & Noble stores targeted in nationwide payment card-skimming scam.** Rogue PIN pad devices discovered at more than 60 Barnes & Noble stores nationwide appeared to be the handiwork of a well-orchestrated financial fraud scheme that rigged just one device at each store, Dark Reading reported October 24. The retail bookseller revealed that it had halted use of all PIN pad devices in most of its 700 stores as of September 14 in the U.S. and that the FBI is investigating the case. The compromised PIN pad devices represent less than 1 percent of the total number of these devices in Barnes & Noble stores, according to the retailer. The compromised devices were found in some stores in California, Connecticut, Florida, New Jersey, New York, Illinois, Massachusetts, Pennsylvania, and Rhode Island. Somehow, the criminals were able to gain physical access to the devices, which Barnes & Noble described as having been tampered with and implanted with "bugs" that let the fraudsters capture credit card and debit card PIN numbers. Barnes & Noble declined to provide details on the type or features in the rigged devices.
Source: http://www.darkreading.com/insider-threat/167801100/security/attacks-breaches/240009697/barnes-noble-stores-targeted-in-nationwide-payment-card-skimming-scam.html

12. *October 24, Softpedia* – (International) **Lloyds TSB scams: Account payment review notifications and errors.** Lloyds TSB customers should be on the lookout for two particular phishing emails, Softpedia reported October 24. One of them is entitled "Error on your account" and the other one "Account payment review notification." In both cases, users who take the bait and click on the links are directed to compromised Web sites that host cleverly designed fake Lloyds TSB Web pages. At the time of writing, the hijacked sites' owners — one of the sites belongs to an educational institution from China and the other one is a Ukrainian site — had removed the phishing pages. However, Internet users must still be cautious when receiving such messages since the cybercriminals can easily hijack other Web sites and resume their operation.
Source: http://news.softpedia.com/news/Lloyds-TSB-Scams-Account-Payment-Review-Notifications-and-Errors-301812.shtml

13. *October 24, Canton Press-News* – (Ohio) **Aultman Hospital reports data breach.** Aultman Hospital in Canton, Ohio, recently learned that an unidentified third party gained unauthorized access to credit card and debit card information relating to some purchases at the hospital's gift shop between February and September 2012, the Canton Press-News reported October 24. Upon learning of the security breach, Aultman Hospital took immediate steps to investigate and resolve the situation. Aultman notified the appropriate law enforcement authorities, including the Secret Service and the Canton Police Department. Aultman replaced the hardware affected by the breach, and retained a forensic auditor to assist with the ongoing investigation. Currently, Aultman did not know how many individuals were affected by the breach, but the breach appeared limited to the gift shop.
Source: http://www.the-press-news.com/local business/2012/10/24/aultman-hospital-reports-data-breach

14. *October 24, Threatpost* – (International) **Operation High Roller banked on fast-flux botnet to steal millions.** A fraud ring that attacked financial transfer systems in an attempt to target wealthy high-end banking customers used a complicated web of malware and compromised servers in several countries to steal an estimated $78 million earlier in 2012, Threatpost reported October 24. While the attacks targeted financial systems, the victims seem to be limited to companies involved in manufacturing, import-export businesses, and State or local governments. Operation High Roller was at its peak during the spring, using automated fast-flux techniques to move command and control and malware servers from host to host, using providers in Kemerovo, Russia, as well as other hosts in Albania, Scottsdale, Arizona, and San Jose, California. All of them had ties to servers in Albania and China and relied on a cocktail of the Zeus trojan and variants SpyEye and Ice IX, according to McAfee and Guardian Analytics who jointly discovered the fraud ring in February and completed a deeper analysis of the operation the week of October 22. "With no human participation required, each attack moves quickly and scales neatly. This operation combines an insider level of understanding of banking transaction systems with both custom and off the shelf malicious code..." one of the report's authors said. Victims were generally lured in via phishing campaigns and were infected by malware adept at bypassing even two-factor authentication and other security devices in place. McAfee also found connections to the owners of a Pittsburgh pizza restaurant who owned domains originally hosted on the Chinese server hosting other Zeus malware. McAfee speculated that either the owners' identities were stolen or they were involved in the scheme and the restaurant is a front for money laundering.
Source: http://threatpost.com/en_us/blogs/operation-high-roller-banked-fast-flux-botnet-steal-millions-102412

For more stories, see items **17**, **38**, and **45**

[Return to top]

Transportation Sector

15. *October 25, KWTX 10 Waco* – (Texas) **Interstate reopened after fatal early-morning crash.** Interstate 35 in McLennan County, Texas, reopened October 25, after being closed for 6 hours due to a crash that claimed the life of a construction worker and injured four others. A Department of Public Safety (DPS) trooper said that a man died October 25, when he was run over by a construction truck that had been struck by a southbound tractor-trailer. The trooper said an 18-wheeler crashed into the back of a crush truck that was being filled with construction debris on the shoulder of the Interstate at mile marker 345. The DPS was still searching for the truck driver who struck the man.
Source: http://www.kwtx.com/home/headlines/One-Person--175757451.html

16. *October 24, Los Angeles Times* – (National) **US Airways fined $354,500 over jet fuel pump.** The Federal Aviation Administration (FAA) proposed a $354,500 civil penalty against US Airways Inc. for operating a jet on hundreds of flights without completing required testing on a new fuel pump, the Los Angeles Times reported October 24. The Tempe, Arizona-based airline has 30 days to respond to the proposed fine. The federal agency said the airline operated a Boeing 757 jet on 916 flights after replacing a leaking engine fuel pump on August 3, 2010. The FAA said the airline failed to carry out federally required tests and inspections before the airline began to carry passengers. The plane flew between August 3, and December 3, 2010, with the new fuel pump without performing the tests and inspection, the FAA said. A spokeswoman for the airline said it operated the airline in compliance with FAA rules.
Source: http://www.latimes.com/business/money/la-fi-mo-us-airways-fined-20121024,0,5164760.story

[Return to top]

Postal and Shipping Sector

17. *October 24, Associated Press* – (Alabama) **Postal worker indicted in refund fraud conspiracy.** A Postal Service mail carrier in Montgomery, Alabama, was indicted in what authorities called a stolen identity refund fraud conspiracy, the Associated Press reported October 24. The U.S. Department of Justice said the carrier was charged with conspiring to file false claims, mail fraud, aggravated identity theft, and embezzlement from the mail. The indictment claimed that members of the conspiracy filed false tax returns using stolen identities from various locations including the northern district of Alabama. The fraudulent tax refunds were directed to debit cards that were mailed to addresses on the carrier's postal route; he is accused of retrieving the debit cards from the mail and providing them to a co-conspirator.
Source: http://www.chron.com/news/crime/article/Postal-worker-indicted-in-refund-fraud-conspiracy-3979209.php

For another story, see item **55**

[Return to top]

Agriculture and Food Sector

18. *October 25, KOLR 10 Springfield* – (Missouri) **Chemical spill contained at mustard plant; 3 employees treated for burns.** A chemical spill at the French's Mustard plant in northeast Springfield, Missouri, sent three employees to the hospital October 25. A report said a pipe burst at the plant, spewing out sodium hydroxide, a cleaning acid, that may have exposed up to 20 people inside the building. Three people complained of contact burns or redness after being exposed to the chemical and were taken to a local hospital. The spill was contained, but HAZMAT crews remained on scene to investigate what caused the pipe burst.
Source: http://ozarksfirst.com/fulltext?nxd_id=719622

19. *October 24, Food Safety News* – (National) **More cases linked to Salmonella peanut butter outbreak.** The number of Salmonella Bredeney infections linked to peanut products from New Mexico based Sunland, Inc. rose again October 24, reaching 38, up from the 35 cases last reported by the Centers for Disease Control and Prevention (CDC). The newly counted cases occurred in California, where there were two cases, and New Mexico, where there was one case, according to the CDC's latest report. Health officials continued to investigate whether any other Sunland products may be contaminated.
Source: http://www.foodsafetynews.com/2012/10/more-cases-linked-to-salmonella-peanut-butter-outbreak/

20. *October 24, Santa Monica Patch* – (California) **Radioactive medical waste in dumpster closes Albertsons.** October 24, a HAZMAT team investigated radioactive medical waste detected in a trash bin behind an Albertsons in Santa Monica, California, temporarily closing the grocery store. The radioactive source was a bag of medical grade Iodine 131 used to treat thyroid cancer, according to the Santa Monica fire chief. The store was not evacuated because readings inside the store were normal, but new customers were not allowed to go inside, the fire chief said. The radiation signal was picked up by city trash collector. The bag of Iodine 131 and all of the dumpster's trash were taken to a landfill.
Source: http://santamonica.patch.com/articles/hazmat-team-called-to-albertsons

21. *October 24, U.S. Department of Labor* – (Oregon) **Craft brewer cited by US Labor Department's OSHA for safety hazards at New Hampshire brewery following fatality caused by April keg explosion.** October 24, the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) announced that it cited Craft Brew Alliance Inc. with 14 alleged serious violations of workplace safety standards following the April 24 death of an employee at the company's Redhook Brewery in Portsmouth, Oregon. The employee was using a compressed air line to purge liquid from the interior of a plastic keg when the keg exploded and fatally struck him. An investigation by OSHA's Concord Area Office determined that the explosion resulted from excess air pressure. The cleanout line lacked an air regulator that would have limited its air pressure to less than 60 pounds per square inch, which is the maximum air pressure limit recommended by keg manufacturers. In this case, OSHA also found that other employees who used the cleanout line were exposed to the same hazard while

cleaning out steel kegs. Craft Brew Alliance Inc. faced a total of $63,500 in proposed fines.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23163

[Return to top]

Water Sector

22. *October 25, Associated Press* – (Iowa) **Residents of Pilot Mount in central Iowa urged to boil drinking water from emergency well.** State officials asked residents of Pilot Mound, Iowa, to boil their drinking and use bottled water for infants after an emergency because the town resorted to using an emergency well. The Iowa Department of Natural Resources issued the alert October 24. Officials said the town started using water from an emergency well after the primary well could not meet the demand. Since the emergency well was not tested recently, the water quality was not known. Boiled or bottled water should be used for drinking, making ice, brushing teeth, and food preparation until further notice. Only bottled water should be used for babies under 6 months old. Residents were also asked to conserve water because of a potential water shortage.
Source:
http://www.therepublic.com/view/story/9b1cf42f05fe480b9837f01a93da64f0/IA--Water-Alert-Pilot-Mound

23. *October 24, Fairbanks Daily News-Miner* – (Alaska) **Fairbanks-based mining company fined $12,000 for wastewater violations.** A Fairbanks-based mining company was fined $12,000 by the State of Alaska for illegally discharging wastewater from its operations in 2011, the Fairbanks News Miner reported October 24. CCR Mining Co. discharged wastewater from its mine site into Harrison Creek once in August 2011 and twice in September 2011, according to the Alaska Department of Environmental Conservation (DEC). The creek, located 83 miles northeast of Fairbanks, drains into Birch Creek, which is designated as a National Wild and Scenic River. CCR Mining's permit did not authorize the discharge of water from its mining operations. Other alleged violations included failure to report the discharges and failure to mitigate them. A DEC program manager said the discharges were reported by Bureau of Land Management biologists who were conducting fish habitat surveys in the area. Birch Creek is listed by the Alaska Department of Fish and Game as an important spawning, rearing, or migration waterway for anadromous fishes. The discharges exceeded State standards for turbidity, according to DEC.
Source: http://newsminer.com/bookmark/20605399-Fairbanks-based-mining-company-fined-12-000-for-wastewater-violations

24. *October 24, U.S. Environmental Protection Agency* – (New York) **EPA takes legal action against western New York gas stations to protect ground water from petroleum contamination.** The U.S. Environmental Protection Agency (EPA) issued a legal complaint to the owner and operator of 17 underground storage tanks at 6

gasoline stations in western New York for violating federal regulations, according to a October 24 news release. The complaint, which seeks $42,295 in penalties, was issued to United Refining Company for violations at its Kwik Fill stations in Dunkirk, Westfield, Jamestown, Fredonia, and Rochester, New York. In addition to paying penalties, the complaint requires the facilities to come into full compliance with the environmental regulations. The complaint alleges the company failed to: upgrade piping at one service station, keep adequate records of corrosion protection at one service station, ensure equipment was running properly at one service station, and keep adequate records of release detection monitoring at three service stations. In a separate action, the EPA reached an agreement with the NOCO Energy Corporation to settle violations involving 39 underground storage tanks at 13 stations in the Buffalo area and in Rochester.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/17b8deca94fdb08885257aa1005b48a3!OpenDocument

25. *October 24, U.S. Environmental Protection Agency* – (New Jersey) **EPA completes building demolition at toxic site in Garfield, N.J.** October 24, the U.S. Environmental Protection Agency (EPA) announced that it demolished the E.C. Electroplating building at the Garfield Ground Water Contamination Superfund site in Garfield, New Jersey. Areas underneath the building are contaminated with hexavalent chromium that is reaching the basements of some area residences and businesses through the ground water. The EPA will continue to assess and, if needed, clean up nearby basements. The demolition of the building will allow the EPA to remove contaminated soil that is a likely source of chromium contamination in the ground water. The EPA's sampling showed the parts of the E.C. Electroplating building above the foundation slab were not contaminated with hexavalent chromium, but two basements and the soil under the structure were contaminated. The structure was demolished to access the contaminated soil underneath. The industrial materials and building debris left at the E.C. Electroplating site were removed and disposed of at facilities licensed to receive the waste. As part of its longer-term work, the EPA established a network of ground water monitoring wells to determine the extent of chromium contamination in the ground water.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/54abb82849012e1085257aa10061ec9a!OpenDocument

[Return to top]

Public Health and Healthcare Sector

26. *October 25, Times of Trenton* – (New Jersey) **Former Lawrence doctor admits to falsifying prescriptions, medical records.** A former Lawrence Township, New Jersey doctor pleaded guilty October 24 to writing fake prescriptions for narcotic pain killers in the names of patients he never examined in 2008 and creating fake medical records to cover it up. He admitted to all the charges in the indictment against him including second-degree distribution of oxycodone, second-degree conspiracy, third-degree

fraudulently obtaining a controlled dangerous substance, and fourth-degree falsification of medical records. Another man who was already convicted in the case and has completed his sentence took the prescriptions written by the doctor to a Bordentown City pharmacy to be filled. He told both the Lawrence Township doctor and employees of the pharmacy that he was a State corrections employee obtaining prescriptions for people living at a halfway house. The doctor claimed that he was duped by him.
Source:
http://www.nj.com/mercer/index.ssf/2012/10/former_lawrence_doctor_admits.html

27. *October 25, WKYT 27 Lexington* – (Kentucky) **Patients evacuated after hospital fire.** A fire October 25 forced some evacuations at a hospital in Morgan County, Kentucky. The fire broke out inside Morgan County ARH. Fire crews said the fire started inside a portable x-ray machine. The machine melted, but that was the only damage reported inside the hospital. About a dozen patients had to be evacuated for fear that smoke would spread.
Source: http://www.wkyt.com/wymt/home/headlines/Patients-evacuated-after-hospital-fire--175717861.html

28. *October 25, Daily Iowan* – (Iowa) **Audit reports $272,000 fraud by former UIHC employee.** A State Audit Report revealed at the State Board of Regents meeting October 24 in Iowa City, Iowa, that a former University of Iowa Hospital and Clinics (UIHC) employee allegedly improperly disbursed roughly $270,000 over a 9-year period. The majority of the disbursements included roughly $200,000 of equipment bought with department funds by her procurement card that she subsequently sold on eBay. The 200-page audit also reported that she deposited university rebates into a personal bank account to make personal purchases along with altering information that led to her being overly reimbursed for department purchases. The auditor discovered several concerns when addressing the policies and procedures within the department, including a lack of inventory records and control over inventory, along with a lack of administrative action that occurred after discovery of the employee's first improper use of the University PCard in 2006 when the university paid $839 in personal expenses for her trip to North Carolina for an IT training event. Despite the department's knowledge of this, she was not restricted from her PCard, which allows her access to UIHC finances. The audit report recommended the UIHC department "strengthen overall controls and overall operations, such as enhancing controls over purchases made with department funds." The investigation was taken to proper legal authorities, including the Johnson County County Attorney's Office, and the investigation remains ongoing.
Source: http://www.dailyiowan.com/2012/10/25/Metro/30539.html

29. *October 24, Ridgewood-Glen Rock Patch* – (New Jersey) **Chiropractor cracks, pleads guilty to insurance fraud again.** A former chiropractor admitted guilt in running an auto insurance fraud scheme for the third time in a decade, a Passaic County, New Jersey prosecutor announced October 24. According to prosecutors, the chiropractor paid "runners" to steer accident victims to Hamilton Rehabilitation Center in Paterson and then submitted over 30 fraudulent personal injury claims to automobile insurers from December 2010 and February 2011. As a co-owner, he shared in the profits from the faulty claims, receiving between $500 and $75,000. He has previous convictions for

similar schemes in 2003 in Essex County and in Massachusetts in 2008. The State suspended his license to practice in 2005. Three other employees of Hamilton Rehabilitation Center were also indicted for their alleged roles in the scheme.
Source: http://ridgewood.patch.com/articles/chiropractor-cracks-pleads-guilty-to-insurance-fraud-again

30. *October 24, St. Paul Pioneer Press* – (Minnesota) **North Oaks couple pleads guilty to mail fraud.** A couple in North Oaks, Minnesota, pleaded guilty to one count of mail fraud October 24, admitting they gave false information when they applied for benefits for their disabled children. Over a 5-year period, the couple stole approximately $369,000 in State and federal Medicaid money, according to the U.S. Attorney's Office. The couple also defrauded the Social Security Administration of $80,000. They prepared false tax forms and also gave false information in written applications and during in-person interviews for benefits, according to prosecutors.
Source: http://www.twincities.com/localnews/ci_21846958/north-oaks-couple-pleads-guilty-mail-fraud

For another story, see item **13**

[Return to top]

Government Facilities Sector

31. *October 25, CNN* – (New Mexico) **Suspects at large after shooting at Air Force base annex.** A group of people got into a fight with a U.S. airman October 25 inside a gated housing area of an Air Force base in New Mexico. One of them grabbed his gun and shot him, police said. Authorities in Albuquerque were searching for the suspects. The airman was in stable and satisfactory condition, according to a spokesman for Albuquerque police. SWAT and K-9 units were helping in the search. The airman was on patrol in the Maxwell housing area of Kirtland Air Force Base, which is separate from the base itself, when he noticed the suspicious group and approached them, according to a base spokesman.
Source: http://news.blogs.cnn.com/2012/10/25/suspects-at-large-after-shooting-at-air-force-base-annex/?hpt=hp_t3

32. *October 24, Houston Business Journal* – (Texas) **Lone Star College evacuates Tomball campus due to bomb threat.** Lone Star College System issued the all-clear following the evacuation of its Tomball, Texas campus October 24, due to a bomb threat. Normal operations would resume October 25. All classes and operations at the Tomball campus were canceled as a precautionary measure. Those on campus were advised to evacuate, and those off campus were instructed to stay away. Bomb squads from Montgomery and Harris counties swept the entire campus.
Source: http://www.bizjournals.com/houston/news/2012/10/24/lone-star-college-evacuates-tomball.html

33. *October 23, GovInfoSecurity* – (National) **Vermont .gov Website blamed for spam.** The head of Vermont's Department of Labor said the State is not taking any

immediate action to disable code in its computers that allowed spammers the week of October 15 to send unwanted emails that appeared to come from the U.S. federal government and were sent to tens of thousands of consumers. The federal government uses the URL shortening service bit.ly to create short URLs for .gov and .mil Web addresses. The shortened URLs use the 1.USA.gov domain extension, which appeared in the spam message. The 1.USA.gov URL is designed only to redirect users to .gov and .mil Web sites. In most instances, governments disable open redirect to prevent redirected messages from being sent to non-.gov or non-.mil addresses. However, Vermont did not disable open redirect for its labor.vermont.gov site, and that allowed spammers to exploit it, resulting in unsolicited emails being sent to unsuspecting consumers, an analyst with an IT security provider said in a blog posting. The Vermont Labor commissioner said the State is in the processes of replacing the Labor Department's Web site, which could occur within weeks, and suggested the problem will vanish when the new Web site becomes active. The commissioner said the State did not take immediate action to disable open redirect because no real damage — which she defines as the unauthorized release of confidential and/or personally identifiable information — occurred. "If there's a reason we need to pull it quicker, we can, but no one is advising that we have to do that," she said.
Source: http://www.govinfosecurity.com/vermont-gov-website-blamed-for-spam-a-5222?rf=2012-10-24-eg

For more stories, see items **47** and **55**

[Return to top]

Emergency Services Sector

34. *October 25, Pittsburgh Tribune-Review* – (Pennsylvania) **After HIPAA complaint, officials review emergency-alert system.** In the wake of an allegation that personal medical information was disclosed by the former police chief, Monroeville, Pennsylvania officials took a closer look at who receives emergency-alert information from the dispatch center via texts and emails, the Pittsburgh Tribune-Review reported October 25. The assistant police chief filed a written complaint that accused the former chief of passing along details about an emergency medical call to someone who was not involved in the emergency. The U.S. Department of Health and Human Services was asked in August to investigate the situation. The former chief retired in 2010 but remained on a list of first responders who receive direct alerts of fire and medical emergencies. When officials realized the first-responders list was outdated, the former chief and at least 10 other names were purged from the list, and direct texts and emails were put on hold for about a week as fire departments submitted new contact lists, said the current police chief. Though officials agree that the list should be updated from time to time, they maintained that the situation did not violate the Health Insurance Portability and Accountability Act (HIPAA), as is alleged in the complaint.
Source: http://triblive.com/neighborhoods/2805293-74/list-chief-responders-emergency-fire-harvey-polnar-department-information-medical#axzz2AJjnhHtI

35. *October 25, Associated Press* – (North Dakota) **Error sounds emergency sirens in Casselton.** Repair crews in the North Dakota town of Casselton are trying to figure out why emergency sirens inexplicably went off October 23. Residents heard the tone of emergency sirens ringing throughout Casselton with no explanation. Public works crews were able to silence the sirens by manually disabling the siren. The Casselton auditor said a repair crew was on its way to the city, and she expects work to be finished by October 25.
Source: http://bismarcktribune.com/news/state-and-regional/error-sounds-emergency-sirens-in-casselton/article_00a0baca-1e5a-11e2-b0c9-001a4bcf887a.html

36. *October 24, WILX 10 Onondaga* – (Michigan) **Task force looking into 911 call center issues.** A newly formed task force is investigating problems with Michigan's Ingham County consolidated 9-1-1 dispatch center, including what callers believe to be dropped calls and malfunctioning equipment, WILX 10 Onondaga reported October 24. Police, firefighters, and the dispatchers themselves are worried dropped calls, malfunctioning equipment, and a lack of oversight could put lives at risk. The City of Lansing and county leaders met October 24 to talk about what first-responders are dealing with. A council member said there are a variety of concerns the task force is looking at. Firefighters have kept a log of the problem calls. They reported 36 with issues out of 12,000 total calls. The task force has just begun looking into the call center concerns. The Lansing mayor is expecting a report in several weeks.
Source: http://www.wilx.com/news/headlines/Task-Force-Looking-Into-911-Call-Center-Issues-175691211.html

[Return to top]

Information Technology Sector

37. *October 25, Softpedia* – (International) **Imperva experts reveal the best practices and tactics to mitigate insider threats.** Insider threats have become a major issue, and many information security solutions providers have focused their efforts on precisely determining how such threats can be mitigated. Security firm Imperva contributed to this research with a report that examines the legal, psychological, and technological tactics deployed by some high-profile organizations to address these risks. A report published by Imperva in 2010 revealed that approximately 70 percent of employees planned to take copies of work-related files when leaving the organizations they worked for. Furthermore, according to the FBI, the U.S. economy suffers losses of over $13 billion each year because of insider threats. "The digital information age offers unfettered access for any actor trusted enough to enter our enterprise walls," the co-founder and CTO of Imperva explained. "For most organizations, insider threats have moved beyond risk into reality; however, many threat vectors can be protected against with a measured approach to business security." After analyzing the tactics and best practices employed by 40 organizations considered to be highly effective at preventing insider threats, experts determined that making a case for business security, employee education, control access with checks and balances, and security organizing are key elements. Furthermore, all employees with administrative and super user rights should be monitored constantly. IT operations, IT security, Human Resources, and legal

departments should be organized to implement security processes into the business workflow.
Source: http://news.softpedia.com/news/Imperva-Experts-Reveal-the-Best-Practices-and-Tactics-to-Mitigate-Insider-Threats-302141.shtml

38. *October 25, Softpedia* – (International) **Advanced malware allows cybercriminals to empty a bank account in one go.** Security firm AVG released its Community Powered Threat Report for the third quarter of 2012. The study focuses on the 2.0 version of the Blackhole exploit kit, the evolution of malware and other threats that marked the past quarter. According to AVG, the Blackhole exploit kit leads both the toolkit and the malware markets with a share of almost 76 percent, respectively 63 percent. Considering that the crimekit's authors launched the 2.0 version, experts say its market share will grow even further and the attacks it utilizes in will become even more "aggressive" because of the advanced evasion techniques recently integrated into it. "Blackhole is a sophisticated and powerful exploit kit, mainly because it is polymorphic and its code is heavily obfuscated to evade detection by anti-virus solutions. The rapid update capabilities of the kit have also made it challenging for traditional antivirus vendors to track, which are the main reasons it has a high success rate," said the CTO at AVG Technologies. "Through our multi-layered security approach with real-time analysis at the endpoint, AVG has been detecting a much higher rate of Blackhole Toolkit-based attacks than other toolkits, as Blackhole's creator seeks to stay ahead of their competition," he added.
Source: http://news.softpedia.com/news/Advanced-Malware-Allows-Cybercriminals-to-Empty-a-Bank-Account-in-One-Go-302135.shtml

39. *October 25, Softpedia* – (National) **RSA, AMD, Intel, Lockheed Martin and Honeywell team up for cyber security alliance.** IT industry companies Advanced Micro Devices (AMD), Honeywell, Intel Corporation, Lockheed Martin, and RSA/EMC joined forces to form a non-profit research consortium known as Cyber Security Research Alliance (CSRA). Cybersecurity has become an important issue not only for private organizations, but also for governments. Major economic powers, including the United States, are focusing many of their resources on enhancing both their defensive and offensive capabilities and most of them have realized that collaboration with the private sector is vital. The consortium will focus on developing viable approaches to technology transfers, tackling cybersecurity R&D activities, and prioritizing the challenges posed by cybersecurity based on the collaboration of all stakeholders. The CSRA hopes to bring together all the key actors in an effort to address national cybersecurity R&D, and bridge the existent gap between the private sector and the government. Currently, the CSRA is also collaborating with the U.S. National Institute of Standards and Technology to arrange a symposium in early 2013 to bring together academia and researchers from both private and government sectors.
Source: http://news.softpedia.com/news/RSA-AMD-Intel-Lockheed-Martin-and-Honeywell-Team-Up-for-Cyber-Security-Alliance-302273.shtml

40. *October 25, Help Net Security* – (International) **Phishing Websites proliferate at record speed.** A new phishing survey released by the Anti-Phishing Working Group (APWG) reveals that while the uptime of phishing Web sites dropped during the first

half of 2012, cybercriminals were driving substantial increases in the numbers of phishing Web sites they established to steal from consumers. Meanwhile, cybercriminals are increasingly using hacked Web servers of existing, legitimate Web sites to host phishing Web sites, pointing up the need for Web site owners and hosting services need to be on guard. APWG found that average uptimes of phishing attacks dropped to a record low of 23 hours and 10 minutes in the first half of 2012, about half of what it was in late 2011, and by far the lowest since the report series was inaugurated in January 2008. The uptimes of phishing attacks are a vital measure of how damaging they are, and are a measure of the success of mitigation efforts. The longer a phishing attack remains active, the more money the victims and target institutions lose. However, the study's authors also found that there were more phishing attacks in the period — at least 93,462, up 12 percent from the second half of 2011.
Source: http://www.net-security.org/secworld.php?id=13837

41. *October 24, Ars Technica* – (International) **Phony certificates fool faulty crypto in apps from AIM, Chase, and more.** Researchers uncovered defects in a wide range of applications running on computers, smartphones, and Web servers that could make them susceptible to attacks exposing passwords, credit card numbers, and other sensitive data. The Trillian and AIM instant messaging applications and an Android app offered by Chase Bank are three apps identified as vulnerable to man-in-the-middle (MitM) attacks. The weak implementations caused the programs to initiate encrypted communications without first assessing the validity of the digital certificates on the other end. As a result, one of the fundamental guarantees of the secure sockets layer (SSL) — that the computer on the other end of the connection belongs to the party claiming ownership — was fundamentally compromised.
Source: http://arstechnica.com/security/2012/10/faulty-ssl-fooled-by-phony-certificates/

42. *October 24, V3.co.uk* – (International) **Focus: McAfee updates Endpoint Security to battle emerging threats.** McAfee updated its Endpoint Security platform as part of an ongoing effort to block a new generation of advanced persistent threats (APTs). The company said that the update would better equip systems to block highly sophisticated attack techniques, such as the use of master boot record (MBR) sabotage techniques and the use of zero-day flaws for intrusion attempts. The senior vice president and general manager of Endpoint Security for McAfee told reporters the update would look to not only expand the scope of protections for Endpoint Security, but also the new form factors. In addition to the MBR protections introduced in a Deep Defender update, McAfee is updating the Enterprise Mobility manager to add support for iOS 6 devices and adding to the whitelisting protections on the McAfee Application Control administrator tool.
Source: http://www.v3.co.uk/v3-uk/news/2219444/focus-mcafee-updates-endpoint-security-to-battle-emerging-threats

43. *October 24, Government Computer News* – (International) **Hackers' new superweapon adds firepower to DDoS attacks.** Hackers now have access to what is dubbed the High Orbit Ion Cannon (HOIC). HOIC is a free-to-download, open-source program that can turn any user of any skill level into a powerful hacker, at least in

terms of a distributed denial-of-service (DDoS) attack. It was designed to be extremely easy to use — the user simply types in the URL of the target, sets the HOIC to operate in supercharged or normal mode, and then launches the attack. The program sends traffic to that URL in an attempt to overload the site and disable it.
Source: http://gcn.com/articles/2012/10/24/hackers-new-super-weapon-adds-firepower-to-ddos.aspx?admgarea=TC_SECCYBERSSEC

44. *October 24, Softpedia* – (International) **'Download Microsoft Windows License' spam used as launchpad for malware attack.** GFI Labs experts issued an alert to warn users about a spam campaign that's being used as a launchpad for a Blackhole-Cridex malware attack. It starts with an email entitled "Re:Fwd: Order 321312" which reads: Welcome, You can download your Microsoft Windows License here. Microsoft Corporation." Microsoft has nothing to do with the emails and the emails have nothing to do with Windows licenses. Instead, when users click on the link that's behind "here," they are taken to a Web site hosted on a Russian domain, which contains and obfuscated JavaScript that is designed to load another Web page. While the victim is viewing a message that reads "Please wait a moment. You will be forwarded," in the background, the Blackhole exploit kit is working on trying to find a security hole to push malware onto the victim's computer.
Source: http://news.softpedia.com/news/Download-Microsoft-Windows-License-Spam-Used-as-Launchpad-for-Malware-Attack-301923.shtml

45. *October 24, The Register* – (International) **US-CERT warns DKIM email open to spoofing.** The U.S. Computer Emergency Response Team (US-CERT) issued a warning that DomainKeys Identified Mail (DKIM) verifiers that use low-grade encryption are open to being spoofed and need to be upgraded to combat attackers wielding contemporary quantities of computing power. This problem has been found to affect some of the biggest names in the tech industry, including Google, Microsoft, Amazon, PayPal, and several large banks. The DKIM system adds a signature file to messages that can be checked to ascertain the domain of the sender by checking with DNS. It also takes a cryptographic hash of the message, using the SHA-256 cryptographic hash and RSA public key encryption scheme, so it cannot be altered en route. The problem stems from the very weak key lengths that are being used by the companies.
Source: http://www.theregister.co.uk/2012/10/24/uscert_dkim_spoofing_flaw/

46. *October 24, Threatpost* – (International) **Attackers turn to open DNS resolvers to amplify DDoS attacks.** A recent tactic adopted by distributed denial-of-service (DDoS) attackers is the use of open DNS resolvers to amplify their attacks. This technique, while not novel, is beginning to cause serious problems for the organizations that come under these attacks. In a new report, researchers associated with Host Exploit, a volunteer organization that tracks malicious activity among hosting providers, said attackers have been making good use of the numerous poorly configured open DNS resolvers in recent months. These machines were plentiful, but it was not just open resolvers in and of themselves that represented a problem. The issue arose when they were misconfigured, allowing attackers to take advantage of weaknesses in the open resolvers to use them as amplifiers for their attacks.

Source: http://threatpost.com/en_us/blogs/attackers-turn-open-dns-resolvers-amplify-ddos-attacks-102412

For another story, see item **33**

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

47. *October 24, Flint Journal* – (Wisconsin, Indiana, Michigan) **Cut fiber cables in Wisconsin, Indiana responsible for Genesee County phone outages.** Cut fiber cables in Wisconsin and a computer card failure in Indiana led to the interruption of Windstream phone service to several schools and other customers across the region, the Flint Journal reported October 24. Fiber cables near Milwaukee, Wisconsin and Greencastle, Indiana, were cut, Windstream said in an email. There also was a computer card failure at a switching station in Fishers, Indiana. Windstream, a communications company based in Little Rock, Arkansas, said service was restored to Flint, Farmington Hills, and Grand Rapids in MIchigan. The company did not say how many customers were affected.
Source:
http://www.mlive.com/news/flint/index.ssf/2012/10/cut_fiber_cables_responsible_f.html

[Return to top]

Commercial Facilities Sector

48. *October 25, Los Angeles Daily News* – (California) **Canyon Country apartment explosion leads to pot grow, 'extraction' lab.** An apartment that was the source of an explosion October 24 in Canyon Country, California, displacing two neighboring families, was being used as a "marijuana grow house and a THC extraction laboratory," the Sheriff's Department said October 25. The blast severely burned one man, whose name and condition were not immediately available. Another man was arrested on suspicion of cultivation of marijuana and manufacturing a controlled substance. Deputies at the sheriff's Santa Clarita Valley station said there was significant damage to the three-unit building. The building was "red tagged," meaning residents could not return until it is found to be safe. Deputies responding to the explosion found drugs and fireworks inside the apartment. The entire east side of the complex, the Mountain View apartments, was evacuated in the immediate aftermath. The Los Angeles County fire and sheriff's departments, including a HAZMAT squad and arson investigators,

checked the scene before allowing residents in other buildings back to their homes.
Source: http://www.dailynews.com/ci_21849359/canyon-country-apartment-explosion-leads-discovery-drugs-fireworks?source=most_viewed

49. *October 25, WMUR 9 Manchester* – (New Hampshire) **2 boys arrested in connection with fire at popular ski shop.** Two juveniles were arrested in connection with a fire at a ski shop in North Conway, New Hampshire. Fire officials said fire broke out the evening of October 24 at Joe Jones Ski and Sports Shop on Route 16. Fire crews found heavy smoke billowing from the showroom and flames working their way up the outside of the building. Witnesses said they could see smoke for a number of blocks. Firefighters from across the Mount Washington Valley area responded to the fire. North Conway's fire chief said the fire caused at least $200,000 in damage. The business was closed at the time of the fire, fire officials said. The State fire marshal's office and the Conway Police Department are investigating the fire.
Source: http://www.wmur.com/news/nh-news/Suspicious-fire-damages-popular-North-Conway-ski-shop/-/9857858/17124554/-/srhdy7z/-/index.html

50. *October 25, CNN* – (California) **United States Fire Protection shooting: Three relatives killed at Downey, California business.** An unknown suspect gunned-down five members of a family — killing three — at their Los Angeles-area fire extinguisher business and a nearby home October 24, police said. The suspect was on the loose and considered to be armed and dangerous, said a Downey Police spokesman. The shootings started at United States Fire Protection in Downey, about 10 miles southeast of downtown Los Angeles, with a 9-1-1 call, police said. Of the three people shot there, two died. Five minutes after the first call, a 9-1-1 call came from the family's nearby home, where a person was fatally shot and a second person was wounded, police said. The gunman fled in a car owned by one of the victims, according to police. The two survivors were at a hospital in critical condition October 24. All five victims are members of a family that runs the fire extinguisher business, though it was not clear whether all five were involved in the business, police said. The relationship between the gunman and the victims, if any, was not immediately clear.
Source: http://www.wptv.com/dpp/news/national/united-states-fire-protection-shooting-three-relatives-killed-at-downey-california-business

51. *October 24, North County Times* – (California) **3-alarm blaze damages several Carlsbad apartments.** A three-alarm blaze at a Carlsbad, California apartment complex damaged about eight units and prompted at least two dozen tenants to evacuate October 24, authorities said. The fire broke out in a three-story building at The Grove apartments. Flames burned through the roof when firefighters and police arrived on the scene. Firefighters requested additional trucks from Vista, Oceanside, Encinitas, and Rancho Sante Fe Fire Protection District, a Carlsbad city spokeswoman said. It took firefighters about 1 hour and 15 minutes to control the blaze, which spread through the attic and damaged about eight third-floor units. Additional apartments sustained smoke and water damage. Residents of 36 units were displaced, either by damage to their apartments or because the utilities were shut off for fire safety. The Red Cross was called to assist 20 tenants, while others found their own places to spend the night.

Source: http://www.nctimes.com/news/local/carlsbad/alarm-blaze-damages-several-carlsbad-apartments/article_99bec013-b034-5e32-9a68-cd3dffaed435.html

52. *October 24, KNSD 7 San Diego* – (California) **Marijuana device found at Mercedes dealership.** A marijuana pipe that looked like an explosive device was found at a Mercedes Benz dealership in Kearny Mesa, California, according to the San Diego Fire Department (SDFD). Police said an employee reported the item after a customer brought the device into the dealership. The man found the device 2 miles from the storefront, picked it up, put it in his car and brought it to the dealership out of curiosity, according to a SDFD spokesperson. Officials originally believed it was a pipe bomb, but after further investigation determined it was a marijuana device. A robot investigated the item and determined it was a marijuana pipe. The device was attached to bottom of car, as a way to transport the marijuana, and happened to fall off from underneath the car at that intersection. The customer who brought the device to the shop was not considered a suspect, according to officials. Roughly 300 employees at the dealership were evacuated for 2 hours while the bomb squad investigated.
Source: http://www.nbcsandiego.com/news/local/Suspicious-Device-Found-at-Mercedes-Dealership-175621141.html

53. *October 24, CNN* – (Georgia) **Authorities arrest man suspected of killing 1 at Georgia megachurch.** The man suspected of killing one person at the World Changers Church International in suburban Atlanta was arrested October 24, U.S. Marshals said. Police named the suspect and described him as armed and dangerous. Authorities said marshals and Fulton County Police arrested the suspect at Lenox Mall in the Buckhead community of Atlanta, about 25 miles from the church. There were about 25 people in the church when the shooting happened, a police spokeswoman said. The megachurch, which claims about 30,000 members, is led by well-known prosperity minister. The victim died at a hospital. He was leading a prayer when he was shot, police said. The suspect was a former volunteer at the church who resigned in August. The spokeswoman said police do not know whether the victim was targeted specifically.
Source: http://www.cnn.com/2012/10/24/justice/georgia-church-shooting/index.html?hpt=ju_c2

54. *October 24, Charlotte Business Journal* – (North Carolina) **High-rise floors at Charlotte Plaza evacuated.** The upper floors at the Charlotte Plaza building in uptown Charlotte, North Carolina, were evacuated October 24 and would be unavailable to tenants until October 25 due to a "building emergency" that caused a loss of power, according to its owner. Floors 15 through 27 were closed to tenants. A Hines representative said the cause was an electrical short. The building's management team is assessing the problem and estimated tenants would be allowed back on the upper floors October 25, according to real estate firm Hines, which owns the property. The lower floors can be accessed but "may experience comfort issues, in regards to air, resulting from the building emergency," the firm said.
Source: http://www.bizjournals.com/charlotte/blog/real_estate/2012/10/high-rise-floors-at-charlotte-plaza.html

55. *October 24, KRCG 13 New Bloomfield* – (Missouri) **Gas leak leads to evacuations in Ashland.** A natural gas leak forced several evacuations and shut down most of downtown Ashland, Missouri, October 24. Street crews accidentally broke a 6-inch gas line while working near the Southern Boone County Middle School. With the smell of gas spreading throughout a four block area, emergency crews evacuated Southern Boone County High School, Middle School, and Preschool Kindergarten. Authorities blocked off nearby streets and closed more than a dozen businesses including the Ashland Post Office. Ameren crews shut off the leak about 90 minutes after the gas line broke. No one was hurt and nothing was damaged. After Ameren crews repaired the broken natural gas line, they checked every customer's house for any problems, and re-lit pilot lights. Southern Boone County firefighters, Boone County Sheriff's Deputies, Ashland Police, and the Missouri State Highway Patrol responded to the leak.
Source:
http://www.connectmidmissouri.com/news/story.aspx?id=816801#.UIlg2K7kGol

For another story, see item **11**

[Return to top]

National Monuments and Icons Sector

56. *October 24, Associated Press* – (Colorado) **Wildfire forces evacuation of southern Colorado town, destroys at least dozen homes.** A wildfire that forced the evacuation of hundreds of people in and around a small southern Colorado town has damaged at least 14 homes, authorities said October 24. The 3 1/4 square-mile fire was burning near Wetmore, Colorado. About 380 people were evacuated after the fire broke out October 23 and quickly grew in winds gusting up to 79 mph. The fire continued to spread through the night, forcing authorities to go door-to-door to evacuate seven more homes in neighboring Pueblo County. The Federal Emergency Management Agency authorized federal funds to fight the fire. The cause of the Wetmore Fire was still under investigation, but wind may be to blame. A Custer County Sheriff told the Denver Post that colliding power lines apparently created sparks that ignited dry brush.
Source:
http://www.therepublic.com/view/story/29ad64ad3f764476a5dbdc9e8c11fab7/US--Wildfire-Town-Evacuated

[Return to top]

Dams Sector

57. *October 25, Cape Girardeau Southeast Missourian* – (Missouri; Illinois) **Flood projects progressing on both sides of Mississippi River.** Progress is steadily being made with flood-recovery projects on both sides of the Mississippi River, the Cape Girardeau Southeast Missourian reported October 25. Cairo, Illinois, will be the beneficiary of a $7.8 million contract awarded by the U.S. Army Corps of Engineers for its flood-control projects, and officials in the Missouri counties of Mississippi and New Madrid are pleased with efforts to repair levees that were intentionally breached

during 2011's massive flooding. The contract for Cairo was awarded October 19, and the money will go toward construction of two landside earthen berms and a 4,200-foot slurry trench expected to reduce water seepage under the Ohio River levee. The funding is part of the ongoing $46 million recovery project performed under Corps supervision for the city that saw record flooding in 2011. In addition to the new slurry trench and berm projects, Cairo already had a 7,200-foot slurry trench under construction along its Mississippi River levee that is expected to be completed in January 2013. It has seen the completion of 28 relief wells along the same levee designed to further reduce water seepage, and another set of 30 relief wells near the city's floodwall were scheduled to be operational by September 2012.
Source: http://www.semissourian.com/story/1907364.html

58. *October 25, Pittsburgh Post-Gazette* – (Pennsylvania) **Bill would increase funding for locks, dams.** Legislation that would provide increased federal money for long-delayed repairs to crumbling locks and dams on the Monongahela River will be introduced in the U.S. Senate, the Pittsburgh Post-Gazette reported October 25. A Tennessee senator said October 24 his proposal would raise the diesel tax that barge operators pay to help fund major river infrastructure improvements. It would also make an Ohio River project plagued by more than $2 billion in cost overruns ineligible to receive money from a trust fund supported by the tax. New locks and a dam being built on the Ohio River near Olmsted, Illinois, currently receive $147 million of the $170 million in federal funding that the U.S. Army Corps of Engineers is allotted each year to build new facilities or make major repairs to existing infrastructure. That leaves little money for other projects, including building new locks on the Monongahela River at Charleroi, Pennsylvania, so that a 105-year-old lock and dam upriver at Elizabeth can be demolished. More than 200 locks and the dams located alongside them make it possible to move about 550 million tons of coal, grain, and other commodities annually on the country's 11,000-mile river system. More than half of the facilities are older than the 50 years they were designed to last, with Pittsburgh having some of the oldest locks and dams in the country.
Source: http://www.post-gazette.com/stories/business/news/bill-would-increase-funding-for-locks-dams-659103/

59. *October 24, Bakersfield Now* – (California) **Final impact study ready on Isabella Dam modification.** The final environmental impact statement for the Safety Modification Study of Isabella Dam in California was released by the U.S. Army Corps of Engineers, Bakersfield Now reported October 24. The Corps also scheduled three public meetings on the plan. New concerns about the two dams first came to light in 2006. Since then, the Corps studied how to deal with three main issues. The study detailed how engineers proposed to "reduce the risk of dam failure or catastrophic downstream flooding during a large storm," according to a Corps statement. Earlier in 2012, Corps engineers announced the main points of their repair plan. They want to raise the crests of both the main and auxiliary dams by 16 feet to prevent over-topping in extreme flood events. On the auxiliary dam, they want to make modifications to increase stabilization and reduce risk during an earthquake. Also, they intend to add a filter and drain system to the auxiliary dam for quake safety, and to control "seepage" of water through the earth-filled structure. Engineers also want to add a second

emergency spillway and realign the Borel Canal through a tunnel in the auxiliary dam. As of August, engineers put the cost of the modification at $400- $600 million. The Corps hopes to start construction on the dam project in 2015 and be done in 2022. Source: http://kernrivervalley.bakersfieldnow.com/news/environment/74453-final-impact-study-ready-isabella-dam-modification

[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/IPDailyReport

Contact Information

Content and Suggestions:	Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703)387-2273
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@hq.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