Daily Open Source Infrastructure Report
19 October 2012

Top Stories

- A Bangladeshi man snared in an FBI terror sting considered targeting the U.S. President and the New York City Stock Exchange before plotting a car bomb attack on the Federal Reserve, an official told the Associated Press October 18. – *Associated Press* (See item 7)
- BB&T Corp. acknowledged October 17 that its Web site was suffering from intermittent outages related to a distributed denial-of-service (DDoS) attack. The institution is the ninth U.S. bank to be affected by a DDoS strike in the last 5 weeks. – *BankInfoSecurity* (See item 9)
- California pharmacy regulators began an investigation of reports of irregularities in prescription refills at CVS pharmacies. Investigators are probing complaints that CVS renewed doctors' prescriptions and billed insurers without customers' consent, and in some cases enrolled the customers in automatic refill programs without their knowledge. – *United Press International* (See item 28)
- Cherryville, North Carolina's police chief and a police captain were suspended after investigators found they allegedly used their credentials and legal authority to let trucks full of stolen goods pass through Gaston County. – *WBTV 3 Charlotte* (See item 33)
- Police provided the name of the gunman who stormed into a Casselberry, Florida salon October 18 and shot four women — killing three — before driving away and committing suicide. – *Orlando Sentinel* (See item 48)

Fast Jump Menu

Energy Sector

1. *October 18, WMC 5 Memphis* – (National) **Severe storms leave behind trail of damage in the mid-south.** Storms swept through the mid-south October 17. In Millington, Tennessee, many families at the Westside Mobile Home Park were evacuated and were assisted by the Red Cross. About six or seven mobile homes suffered damage. However, no one was injured. There were also reports of a possible tornado touchdown in Crittenden County, Arkansas, which resulted in damage and injuries. Northern Mississippi was also hit hard. At least 15,000 outages were reported, but those decreased as crews worked to restore power. October 18, the National Weather Service had survey teams in the Mid-South to confirm any tornado touchdowns.
   Source: http://www.wmctv.com/story/19848946/severe-storms-leave-trail-of-damage-in-the-mid-south

2. *October 17, Associated Press* – (New York) **Cops: Ex-NY town official stole 8K gals. of fuel.** New York State police charged a former highway superintendent with stealing thousands of gallons in municipal diesel fuel and using it for his own vehicles, the Associated Press reported October 17. Investigators said they believe the former superintendent may have stolen more than 8,000 gallons of fuel from the town of Wright before he left office in January. Police said the former superintendent directed town highway department employee's to stop filling out fuel logs in order to conceal the thefts. The accused was charged with falsifying business records, official misconduct, and petit larceny. He was issued an appearance ticket.
   Source: http://online.wsj.com/article/AP93652540014e4f8eaa0ec2be4f348887.html

For another story, see item **52**

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials and Waste Sector

3. *October 18, Phys.Org* – (International) **Nuclear power plants located in tsunami risk zones.** Scientists have highlighted "potentially dangerous" areas that are home to completed nuclear plants or those under construction. The study is the first to look into the location of nuclear power plants and correlate them to areas at risk of tsunamis. "We are dealing with the first vision of the global distribution of civil nuclear power plants situated on the coast and exposed to tsunamis," explained a co-author of the study and researcher at the Centre for Research on the Epidemiology of Disasters of the Catholic University of Leuven in Belgium. To inform their analysis, the authors used historical, archaeological, geological, and instrumental records as a base for determining tsunami risk. Their study presented a map of the world's geographic zones that are more at risk of large tsunamis. Based on these data, 23 nuclear power plants with 74 reactors have been identified in high-risk areas. One of them includes Fukushima I. Of these, 13 plants with 29 reactors are active; another 4, that now have 20 reactors, are being expanded to house 9 more; and there are 7 new plants under construction with 16 reactors. Despite the fact that the risk of these natural disasters threatens practically the entire western coast of the American continent.
   Source: http://phys.org/news/2012-10-nuclear-power-tsunami-zones.html

4. *October 17, Carbondale Southern Illinoisan* – (Illinois) **Honeywell must improve safety before reopening.** The U.S. Nuclear Regulatory Commission (NRC) has given orders to Honeywell on what safety measures must be in place before the company's Metropolis, Illinois uranium conversion plant can restart operations, the Carbondale Southern Illinoisan reported October 17. Uranium conversion at the Honeywell Metropolis Works plant have been shut down since May, after NRC officials found problems within the facility that could cause public harm in the event of a natural disaster. Officials worried an earthquake or tornado could breach the plant, causing the release of the chemical uranium hexafluoride. The agency is requiring Honeywell to revise its emergency response plans to natural disasters, as well as make necessary facility modification to make it more earthquake and wind resistant. The company is cooperating with the agency in making the changes. Company officials said needed upgrades could take between 9 and 12 months to complete.
   Source: http://thesouthern.com/news/local/honeywell-must-improve-safety-before-reopening/article_6248b858-1816-11e2-b699-001a4bcf887a.html

[Return to top]

Critical Manufacturing Sector

5. *October 17, WSEE 35/WICU 12 Erie* – (Pennsylvania) **Worker killed in DonJon shipyard accident.** A man was killed October 17 while working inside the DonJon shipbuilding yard on Erie's Bayfront in Pennsylvania. A maintenance worker was servicing a crane about 100 feet from the ground. He got caught in the machinery and was killed instantly. It took Erie firefighters 2 hours to recover the man's body from the crane. Representatives from the Occupation Safety and Health Administration are conducting an investigation of the death.
Source: http://www.erietvnews.com/story/19846605/worker-killed-in-donjon-shipyard-accident

6. *October 17, U.S. Department of Labor* – (Ohio) **US Department of Labor's OSHA cites auto parts supplier TFO Tech for exposing workers to amputation hazards at Jeffersonville, Ohio, facility.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited TFO Tech Co. Ltd with 13 safety violations at the company's auto parts manufacturing facility in Jeffersonville, Ohio, according to an October 17 news release. The violations include a lack of machine guarding and allowing workers to perform maintenance on machinery without first isolating the equipment's energy source. OSHA opened an inspection in July under the agency's National Emphasis Program on Amputations after receiving a complaint alleging hazards. Proposed fines total $51,000. Twelve serious violations involve a lack of guarding for the points of operation on automated mechanical forging presses, not having machine-specific lockout/tagout procedures, a damaged metal guard on a conveyor, inadequate strain relief and insulation for electrical cords, a lack of periodic inspections, unguarded floor openings, failing to train workers, and failing to lock out the energy sources of machinery during servicing and maintenance.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23142

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

7. *October 18, Associated Press* – (New York) **U.S. President was considered potential target.** A Bangladeshi man snared in an FBI terror sting considered targeting the U.S. President and the New York City Stock Exchange before plotting a car bomb attack on the Federal Reserve, a law enforcement official told the Associated Press October 18. The official stressed that the suspect never got beyond the discussion stage in

considering an attack on the U.S. President. In a September meeting with an undercover agent posing as a fellow jihadist, the suspect explained he chose the Federal Reserve as his car bomb target "for operational reasons," according to a criminal complaint. The suspect also indicated he knew that choice would "cause a large number of civilian casualties, including women and children," the complaint said. FBI agents grabbed the man — armed with a cellphone he believed was rigged as a detonator — after he made several attempts to blow up a fake 1,000-pound the bomb inside a vehicle parked next to the Federal Reserve October 17 in lower Manhattan, the complaint said. The suspect appeared in federal court October 17 to face charges of attempting to use a weapon of mass destruction and attempting to provide material support to a terrorist group.
Source: http://abcnews.go.com/US/wireStory/feds-indicted-plot-attack-federal-reserve-17502296#.UIAqjK74LxM

8. *October 17, Reuters* – (New Jersey) **SEC charges Yorkville with securities fraud.** Securities regulators October 17 sued Yorkville Advisors LLC and its top executives, accusing the New Jersey hedge fund of reporting false and inflated values for some of its investments. The Securities and Exchange Commission (SEC) lawsuit targeted Yorkville, which has been one of the largest funds specializing in thinly traded micro-cap and small-cap companies, the founder and president, and the chief financial officer. The firm misreported values as the financial crisis hit in 2008 and 2009 and market conditions deteriorated, and its returns during the period consisted mostly of unrealized gains from marked-up investments, the SEC said. The scheme let Yorkville improperly boost its management fees and led it to improperly receive more than $10 million in unearned fees, the SEC said. The SEC accused Yorkville, which once managed more than $1 billion in assets, of creating and providing false and misleading documents to its auditors to further the scheme. The firm also made false and misleading statements to its investors between April 2008 and January 2010 about the value of its investments and other matters, the SEC said. The "false portrayal of Yorkville as a firm that employed 'robust' internal controls caused pension funds and funds of funds to invest over $280 million in the Funds," the SEC said.
Source: http://www.reuters.com/article/2012/10/17/us-sec-yorkville-idUSBRE89G14L20121017

9. *October 17, BankInfoSecurity* – (National) **BB&T site outages linked to DDoS.** BB&T Corp. acknowledged October 17 that its Web site was suffering from intermittent outages related to a distributed denial-of-service (DDoS) attack. The $178.5 billion institution is the ninth U.S. bank to be affected by a DDoS strike in the last 5 weeks. "BB&T is experiencing intermittent outages on BBT.com due to a 'Denial of Service' event," a bank spokesman said October 17. BB&T's site outage is the second attack apparently waged by a hacktivist group the week of October 15. October 16, Capital One's online banking and corporate sites suffered outages believed to be caused by a second attack aimed at the bank by the same group. Capital One's Web site was back up and running by October 17, said a spokeswoman, although some customers may continue to suffer from periodic glitches linked to ongoing system upgrades.
Source: http://www.bankinfosecurity.com/bbt-site-outages-linked-to-ddos-a-

5208?rf=2012-10-18-eb&elq=f35dac9ed1d9430aad0f418cc8491d5f&elqCampaignId=4861

10. *October 17, Bloomberg News* – (Georgia) **Former American United Bank officers, directors sued by FDIC.** Former American United Bank officers and directors were sued by the Federal Deposit Insurance Corporation (FDIC) for $45.2 million over their alleged negligence in managing the bank's lending operations. The lawsuit, filed October 17 in federal court in Atlanta, names the defendants as the former president and chief executive officer, former senior vice president, and the chief lending officer. "Rather than manage the bank's lending function in a sound and responsible manner, the defendants took unreasonable risks with the bank's loan portfolio," the FDIC said in the complaint. American United Bank, based in Lawrenceville, Georgia, was closed by State regulators in 2009. Ameris Bank of Moultrie, Georgia, agreed to assume all American United Bank's deposits, the FDIC said in 2009.
Source: http://www.bloomberg.com/news/2012-10-17/former-american-united-bank-officers-directors-sued-by-fdic.html

[Return to top]

Transportation Sector

11. *October 17, St. Louis Post-Dispatch* – (Missouri) **Highway littered with soup cans after crash near Pacific reopens.** Cans of soup and boxes of salad dressing were strewn along the westbound lanes of Interstate 44 near Pacific, Missouri, after three tractor-trailers crashed and lost their loads October 17. The Missouri Highway Patrol said no one was injured, but the crash shut down the highway for about 8 hours. All westbound lanes were shut down for more than 3 hours. After another hour, traffic was being allowed to sneak by in a single lane while the two lanes remained closed. Traffic was backed up about 3-1/2miles, according to the Missouri Department of Transportation. The Missouri Highway Patrol responded to the crash, which happened at the 256-mile marker.
Source: http://www.stltoday.com/news/local/crime-and-courts/highway-littered-with-soup-cans-after-crash-near-pacific-reopens/article_503ed126-1855-11e2-84da-001a4bcf6878.html

For another story, see item **20**

[Return to top]

Postal and Shipping Sector

Nothing to report

[Return to top]

Agriculture and Food Sector

12. *October 18, U.S. Food and Drug Administration* – (National) **The Raymond-Hadley Corporation expands allergy alert on undeclared milk contamination in Wegmans 17.2 oz. Gluten Free Double Chocolate Brownie Mix to include 3 additional enjoy by date codes.** October 18, The Raymond-Hadley Corp. of Spencer, New York, expanded the recall of Wegmans Gluten Free Double Chocolate Brownie Mix 17.2-ounce, UPC 077890283363, to include enjoy by dates from October 30, 2013 through March 17, 2013. The mixes may be contaminated with the undeclared allergen milk. The product was distributed nationwide through Wegmans retail stores, and are packaged under the Wegmans brand in chipboard boxes. As of October 12, two reports of rash have been received.
Source: http://www.fda.gov/Safety/Recalls/ucm324405.htm

13. *October 17, U.S. Food and Drug Administration* – (National) **Kasel Associated Industries recalls Boots & Barkely Roasted American Pig Ears and Boots & Barkley American Variety Pack Dog Treats because of possible Salmonella health risk.** October 17, Kasel Associated Industries of Denver voluntarily recalled its Boos & Barkley Roasted American Pig Ears and Boots & Barkley American Variety Pack dog treats because they may be contaminated with Salmonella. Humans are at risk for Salmonella poisoning from handling contaminated pet products. The recalled Roasted Pig Ears and Variety Pack Dog Treats were distributed nationwide through Target retail stores August 2012.
Source: http://www.fda.gov/Safety/Recalls/ucm324279.htm

14. *October 17, U.S. Food and Drug Administration* – (National) **Bucks Ice Cream recalls Iskream Brand Peanut Butter and Jelly No Sugar Added Ice Cream because of possible health risk.** October 17, Buck's Ice Cream of Milford, Connecticut, co-pack manufacturer for Iskream, Inc., voluntarily recalled all lot codes of Iskream Brand Peanut Butter and Jelly No Sugar Added Ice Cream. The product is potentially contaminated with Salmonella due to ingredients sourced from Sunland. The ice cream was distributed to retail customers through several wholesale distributors in the northeast between March 1, 2012 and October 17, 2012. The product is labeled as "Reduced Fat No Sugar Added Peanut Butter and Jelly with the UPC 858452020554.
Source: http://www.fda.gov/Safety/Recalls/ucm324348.htm

15. *October 17, U.S. Food and Drug Administration* – (National) **Dole Fresh Vegetables announced precautionary recall of limited number of salads.** October 17, Dole Fresh Vegetables of Monterey, California, voluntarily recalled a limited number of cases of Dole American Blend salad in 12-ounce bags, coded A275208A or B, with a use by date of October 17, and UPC 7143000933. The product may be contaminated with Listeria monocytogenes. The salads were distributed in Illinois, Indiana, Maine, Missouri, New Jersey, New York, Ohio, Pennsylvania, Tennessee, and Wisconsin. The recall is due to a sample of Dole American Blend salad which yielded a positive result for Listeria in a random sample test.
Source: http://www.fda.gov/Safety/Recalls/ucm324315.htm

16. *October 16, Publix* – (National) **Publix issues recall for Premium Frozen Tempura Shrimp.** Publix Super Markets issued a voluntary recall for 11-ounce Publix Premium Frozen Tempura Shrimp, the company announced October 16. The dipping sauce packet included with the product contains soy that is not declared on the packaging. Publix discovered this during internal product evaluations.
Source: http://www.publix.com/about/newsroom/recalls/Recall.do?id=3762&lang=en

17. *October 16, California Department of Public Health* – (California) **CDPH warns consumers not to eat three preserved plum products.** The director of the California Department of Public Health (CDPH) warned consumers October 16 not to eat three preserved plum products after tests found that all three exceed State standards for lead. Chemical analysis found that the Red Lantern Plum Candy, Chan Pui Mui Preserved Plum, and Sanh Yuan Preserved Plum products all contained over 6.0 micrograms of lead per serving. The three California importers of the products issued a voluntary recall. The Red Lantern Plum Candy, from China and imported by K.Y.L. Trading Co, Inc. in Brisbane, is sold in a 3-ounce clear plastic package that has red and gold lanterns and red Chinese characters on the front of the package. K.Y.L. Trading Company recalled both the Red and the White varieties of the product. Chan Pui Mui Preserved Plum, from Hong Kong and imported by QFCO, Inc. in Burlingame, is sold in a 14-ounce clear plastic package that has red and blue labeling and contains a large white circle in the middle of the package. Sanh Yuan Preserved Plum, from Taiwan and imported by CHO Fuku Group (USA), Inc. in El Monte, is sold in a 5-ounce clear plastic package that has a green border with various fruits shown at the bottom and Chinese characters appear throughout the package.
Source: http://www.cdph.ca.gov/Pages/NR12-054.aspx

18. *October 16, U.S. Food and Drug Administration* – (National) **Trifecta Foods, LLC announces voluntary recall of Fresh Pak and Energy Club brands of In-Shell Roasted Salted and Unsalted Peanuts due to potential health risk.** October 16, Trifecta Foods, LLC in Pacoima, California, voluntarily recalled products containing In-Shell Roasted Salted and Unsalted Peanuts supplied by Sunland, Inc. because they may be contaminated with Salmonella. The recalled products were available to retail customers under the Fresh Pak and Energy Club labels distributed nationally to independent stores, grocery, and retail chains. The products have best by/expiration dates from November 23, 2012, through April 10, 2013.
Source: http://www.fda.gov/Safety/Recalls/ucm324331.htm

19. *October 15, U.S. Food and Drug Administration* – (National; International) **Natural Selection Foods recalls Earthbound Farm Baby Spinach Grab & Go Salad Kit with Peanuts due to possible health risk associated with Sunland Inc. peanut products (no risk associated with spinach).** Natural Selection Foods voluntarily recalled Earthbound Farm Baby Spinach Grab & Go Salad Kits with Peanuts October 15. The product was sold in a 3.5-ounce clamshell with UPC 0-32601-08875-0; all use by dates are affected. The peanuts in the packets were chopped by Sunland and are potentially contaminated with Salmonella. The salad kits were distributed to retail supermarkets and foodservice operators in 14 States as well as British Columbia and

Ontario, Canada.
Source: http://www.fda.gov/Safety/Recalls/ucm324324.htm

[Return to top]

Water Sector

20. *October 18, Hawaii News Now* – (Hawaii) **Water main break closes roads, school in Hawaii Kai.** Parents of students at Kamilo'iki Elementary School in Hawaii were called to pick up their children ahead of schedule October 17 after a water main break knocked out service to the school and closed roads in the area. According to Honolulu Police, Hawaii Kai Drive was closed between Ahukini Street and Lunalilo Home Road because of the incident. Town-bound traffic was rerouted onto Ahukini Street to bypass the main break site. According to the Honolulu Board of Water Supply, the break appeared to be in an area where an 8-inch water main connects to a 12-inch water main. Crews were in the process of excavating and would be able to pinpoint the break once they reach the main. The Board of Water Supply also said that more than 200 homes were estimated to be without water as a result of the water main break.
Source: http://eastoahu.hawaiinewsnow.com/news/news/109990-water-main-break-closes-roads-school-hawaii-kai

21. *October 17, Chesterfield Village News* – (Virginia) **Water restrictions remain in place.** Lake Chesdin Reservoir in Virginia, even with a fair amount of rain recently, remains 27 inches below its typical water level, even though better than the late August low of minus 56 inches, the Chester Village News reported October 17. The Appomattox River Water Authority (ARWA) monitors Lake Chesdin reservoir and treats the water so residents and businesses can safely consume the water. The ARWA and Lake Chesdin serves the southern area of Chesterfield, Colonial Heights, Dinwiddie, Prince George Counties, and the City of Petersburg. "Until the trees lose their leaves and reducing evaporation as the days become shorter, the reservoir level will remain low," said the ARWA executive director. "The watershed that supplies Chesdin reaches as far as Farmville and includes 133,000 square miles." According to the director, it would take a tropical rain-event that will dump about four inches of rain on the watershed to restore the reservoir to normal levels. Water restrictions affected the entire county. The assistant director of Chesterfield's utility department said that in some cases, restrictions can be lifted in November, but it remained undecided until ARWA meets. October 18, the board, which controls water restrictions and other reservoir concerns, will meet to discuss and decide on whether mandatory water restriction should remain in place.
Source: http://www.villagenewsonline.com/node/10031

22. *October 16, Tampa Bay Times* – (Florida) **Tampa Bay Water draining C.W. Bill Young Reservoir for repairs.** Tampa Bay Water has begun draining its 15.5 billion-gallon C.W. Bill Young Reservoir in Florida to get ready for repair work on its persistent cracking problem, a utility official said October 15. Tampa Bay Water sends 45 million gallons of water a day out of the reservoir to its customers, which means it will be completely dry by the end of December, she said. Repair work on the reservoir,

was scheduled to begin in January 2013 and last 22 months. To make up for idling the reservoir, Tampa Bay Water began running its idled desalination plant. The plant, which has a maximum capacity of about 25 million gallons per day, has been producing 12 million a day since August, so far with no signs of trouble. The utility also takes water from the Hillsborough and Alafia rivers and the Tampa Bypass Canal, as well as pumping millions of gallons of water from underground. The reservoir's walls consist of an earthen embankment as wide as a football field at its base, averaging about 50 feet high. An impermeable membrane buried in the embankment prevents leaks. The embankment's top layer, a mixture of soil and concrete to prevent erosion, began cracking in December 2006. Some cracks were up to 400 feet long and up to 15 1/2 inches deep. Workers patched the cracks, but the patches did not last.
Source: http://www.tampabay.com/news/environment/water/tampa-bay-water-draining-cw-bill-young-reservoir-for-repairs/1256497

[Return to top]

Public Health and Healthcare Sector

23. *October 18, GovInfoSecurity* – (National) **FDA tackling medical device security.** The U.S. Food and Drug Administration (FDA) is looking for ways to improve how it tracks medical device safety and security issues, such as malware risks, GovInfoSecurity reported October 18. The FDA has taken into account the findings of a recent Government Accountability Office report that recommended the FDA develop a plan to improve post-market surveillance of information security issues in medical devices. "We are reviewing all our processes and procedures and will come out with a plan," said the deputy director of the FDA's division of electrical and software engineering. For example, the FDA is considering whether to toughen requirements related to reporting safety and security issues. The FDA is also reaching out to other federal agencies, including the Department of Homeland Security, to coordinate the tracking of security issues.
Source: http://www.govinfosecurity.com/fda-tackling-medical-device-security-a-5210

24. *October 18, Watertown Daily Times* – (New York) **Former Carthage hospital employee forged patient information on 300 surveys.** About 300 of northern New York's Carthage Area Hospital patients' signatures were forged on recent alcohol and drug surveys, according to a village police chief. While hospital officials said they could not comment on the number of people affected, they said in a news release issued October 17 that "a former employee of the hospital made up information on an alcohol and drug survey with patients' names on it and forged the patients' signatures without the hospital's consent or knowledge." That employee has since been fired. The crime was found by a data collection person at Jefferson County Community Services, the local agency overseeing a $1.5 million, 5-year national Substance Abuse and Mental Health Services Administration grant that aims to identify the early onset of alcohol abuse in county residents and avoid associated hospital readmissions. The grant focused on emergency room patients, he said. The news release issued by Carthage Area Hospital indicated the surveys were sent to the Department of Social Services. An internal hospital investigation revealed no other patient personal contact information

besides names was provided, according to the news release. A Community Services director said the forgery will not affect the grant, for which the Community Services office recently was given approval for its second year of funding.
Source: http://www.watertowndailytimes.com/article/20121018/NEWS07/710189849

25. *October 17, Milwaukee Journal Sentinel* – (Wisconsin) **Oak Creek man convicted of Medicaid fraud.** An Oak Creek, Wisconsin man was convicted October 17 of Medicaid fraud for submitting false records for home care services that were never provided, an attorney general's office announced. A jury found him guilty on 17 counts of medical assistance fraud, according to State court records. In December 2008, the man became a participant in the Medicaid-financed "Include, Respect, I Self-Direct" (IRIS) program, which allowed him to submit timesheets for hours worked by home care providers, according to a statement from attorney general's office. According to the statement, between April 2009 and February 2010, he submitted timesheets for a man and a woman who he claimed provided him with home care services. That man told investigators that he never provided care, and the woman said she only worked for two days, for which she was never paid, the statement said.
Source: http://www.jsonline.com/news/crime/oak-creek-man-convicted-of-medicaid-fraud-tg791j5-174670181.html

26. *October 17, Associated Press* – (Louisiana) **La. woman arrested on Medicaid fraud charges.** A Ponchatoula, Louisiana woman was arrested on charges she submitted false timesheets to her employer for her work as a personal care attendant for Medicaid recipients. A Louisiana attorney general office said she was booked into the East Baton Rouge Parish jail October 16 on 5 counts of Medicaid fraud, 10 counts of filing or maintaining false public records, and 7 counts of forgery. The attorney general's office said the timesheets stated that she provided caregiver services to a Medicaid patient on the same dates and times when she actually worked for a second employer.
Source: http://www.sfgate.com/news/crime/article/La-woman-arrested-on-Medicaid-fraud-charges-3958436.php

27. *October 17, Ars Technica* – (National) **Hospitals' computer hardware also suffers from infection.** MIT's Technology Review reported October 17 that hospitals' computerized equipment—such as patient monitoring systems, MRI scanners, and nuclear medicine systems—are dangerously vulnerable to malware, and many systems are in fact heavily infected with viruses. Due to many of these systems running on older versions of Windows, such as Windows 2000, medical equipment manufacturers often will not support security patches or operating system upgrades for their systems, largely out of concern about whether such changes would require them to resubmit their systems to the Food and Drug Administration for certification. The scope of the problem was the topic of a panel discussion at a National Institute of Standards and Technology Information Security and Privacy Advisory Board October 11. The chief information security officer at Boston's Beth Israel Deaconess Medical Center told attendees that malware had infected fetal monitors in his hospital's high-risk pregnancy ward to the point where they were so slow they could not properly record data. The systems have since been replaced with new ones based on Microsoft's Windows XP.

Source: http://arstechnica.com/security/2012/10/hospitals-computer-hardware-also-suffers-from-infection/

28. *October 17, United Press International* – (California) **California investigates CVS pharmacies.** California pharmacy regulators have begun an investigation of reports of irregularities in prescription refills at CVS pharmacies. The executive officer of the California Board of Pharmacy said October 16 investigators are probing complaints that CVS Caremark Corporation renewed doctors' prescriptions and billed insurers without customers' consent, and in some cases enrolled the customers in automatic refill programs without their knowledge. A spokesman for CVS said the company's policy requires a patient's consent "be obtained before a prescription is filled," and added the company would provide the pharmacy board with any information needed. The week of October 8, the U.S. Department of Health and Human Services began another investigation of CVS into allegations the company billed Medicare for medication patients had not ordered or picked up, and in 2011 the company agreed to pay $17.5 million to resolve allegations it falsified prescription drug claims for Medicaid programs in California and nine other States, the Los Angeles Times reported October 17.
Source: http://www.upi.com/Top_News/US/2012/10/17/California-investigates-CVS-pharmacies/UPI-57311350501834/

[Return to top]

Government Facilities Sector

29. *October 18, Associated Press* – (Idaho) **Idaho man convicted in attack on federal property.** A western Idaho man was convicted in federal court of using Molotov cocktails to torch a business where he stole firearms. After a 5-day jury trial the man was convicted in U.S. District Court in Boise October 16 of carrying the fiery devices during and in relation to a federal crime of violence in May 2011. He was also found guilty of conspiracy to maliciously use explosive materials, conspiracy to maliciously damage federal property and theft. Prosecutors alleged the man and an accomplice used Molotov cocktails to destroy a U.S. Department of Agriculture truck, an all-terrain vehicle, as well as other properties. Prosecutors said the man faces at least 35 years in prison.
Source: http://www.ctpost.com/news/crime/article/Idaho-man-convicted-in-attack-on-federal-property-3958594.php

30. *October 17, Manchester Patch* – (New Jersey) **High school will reopen Thursday following bomb threat.** Manchester Township High School in New Jersey was scheduled to reopen October 18, a day after authorities said a threat was made against the building. Students were dismissed October 17 after an undisclosed threat on the building was discovered. "We've taken precautionary measures and evacuated the school," said the Manchester chief of police. He added that the threat did not appear to be credible and declined to comment on how it was made. K-9 units from the Monmouth County Sheriff's Department and the Joint Base Task Force conducted "a thorough search of the building," said a Manchester Police captain. Police continued to

investigate the incident. The afternoon middle school session at the building was canceled October 17, according to the district. Also responding to the scene were the Manchester and Ridgeway volunteer fire departments and the township's Office of Emergency Management.
Source: http://manchester-nj.patch.com/articles/high-school-evacuated-following-bomb-threat

For another story, see item **20**

[Return to top]

Emergency Services Sector

31. *October 18, Memphis Commercial Appeal* – (Tennessee) **Grenade brought to Tenn. station prompts evacuations.** A man October 17, took a grenade he found on a south Memphis, Tennessee lot to Memphis Fire Station No. 14. He feared that if he turned the grenade in to the police, they might keep him all day. He parked in front of the fire station, leaving the grenade in the truck when he told firefighters about it. The fire department took him to a back room, away from the fire station windows. A fire department battalion chief made a bomb threat report to Memphis police. Nearby residences, about two dozen of them, were evacuated if people were at home; police blocked off the street for about two blocks, and the police bomb squad arrived to safely cart the grenade away. A police report described it as an old military-grade grenade with a rusted pin and the handle still intact. The man had found it stuck in the ground of a lot where a house had been demolished days earlier. Police determined that the grenade was hollowed out and not a "live" grenade that could have exploded.
Source: http://www.firehouse.com/news/10815852/grenade-brought-to-tenn-station-prompts-evacuations

32. *October 18, McClatchy-Tribune News Service* – (Oklahoma) **Two Oklahoma firefighters arrested on arson charges.** Two volunteer firefighters in Warner, Oklahoma, were arrested October 17 on arson complaints. The Warner police chief said the two were arrested in connection with several fires allegedly set in Muskogee and possibly McIntosh counties. He said the fires were all set in areas where the two assumed no one would be injured. It is unknown how many fires were set. The two were booked on seven counts of first-degree arson, embezzlement, and the unauthorized use of a credit card. The joint investigation between the Warner Police Department and the Muskogee County Sheriff's Office began in July. The police chief said the investigation into the fires is ongoing.
Source: http://www.firehouse.com/news/10815847/two-oklahoma-firefighters-arrested-on-arson-charges

33. *October 18, WBTV 3 Charlotte* – (North Carolina) **Cherryville police chief, officer suspended due to FBI probe.** Cherryville, North Carolina's police chief and a police captain were suspended after investigators found they allegedly let trucks full of stolen goods pass through Gaston County, WBTV 3 Charlotte reported October 18. Two federal indictments unsealed in U.S. District Court in Charlotte, charge a reserve

deputy sheriff with the Gaston County Sheriff's Office and police officers with the Cherryville Police Department with multiple counts related to the misuse of their official position to provide protection for the transportation of goods they believed to be stolen, announced a U.S. Attorney for the Western District of North Carolina. Two non-law enforcement defendants were also charged for their role in the conspiracy. According to allegations contained in the two indictments, on multiple occasions, the men used their credentials and legal authority to assist with the transfer or transport of stolen goods and/or cash proceeds from the sale of stolen goods, in exchange for monetary bribes.
Source: http://www.wbtv.com/story/19843917/cherryville-police-chief-officer-suspended-due-to-fbi-probe

34. *October 17, Wyandotte Patch* – (Michigan) **2 police guns stolen from cruiser during break-in at Wyandotte DPS.** The Wyandotte, Michigan police department is changing its weapons policy after two police-issued guns were stolen recently out of a cruiser. The car was at the Wyandotte Department of Public Services (DPS) for routine service when someone broke into the DPS October 4. The thief stole a rifle, a shotgun, and several ammunition magazines from the police car. Thousands of dollars worth of tools also were stolen from the DPS. The stolen police weapons, which contain some identifiable marks, have been reported to the State and to the National Crime Information Center. The chief said the investigation is ongoing.
Source: http://wyandotte.patch.com/articles/2-police-guns-stolen-from-cruiser-during-break-in-at-wyandotte-dps

35. *October 17, Worcester Telegram & Gazette* – (Massachusetts) **Mass. fire chief allegedly stole drugs from ambulance.** The Princeton, Massachusetts fire chief was arraigned October 15 on two drug charges in Worcester District Court for allegedly stealing narcotics from the town ambulance. He was arraigned on one count of larceny of a drug, and one count of obtaining drugs by fraud. He was released on personal recognizance, and scheduled to return to court December 3. The investigation into the alleged theft began earlier in 2012, when pharmacists at St. Vincent Hospital in Worcester, and Heywood Hospital in Gardner, notified State police that "excessive amounts of narcotics were being dispensed to the Princeton Fire Department," according to a State police report included in court records. State police conducted an audit of the narcotics being dispensed to the Princeton Fire Department, and found that varying amounts of Fentanyl, morphine, Valium, and Versed were unaccounted for. The fire chief was the primary record keeper of narcotics for the Princeton Fire Department and had signed out the drugs that were dispensed from the two hospitals, the report said.
Source: http://www.firehouse.com/news/10815354/mass-fire-chief-allegedly-stole-drugs-from-ambulance

36. *October 17, WAFB 9 Baton Rouge* – (Louisiana) **10 arrested for trying to smuggle drugs into prison.** The arrest of two people for trying to smuggle narcotics into the Livingston Parish Detention Center in Louisiana, October 3 has led to eight more arrests. Members of the Livingston Parish Sheriff's Office (LPSO) Narcotics Division and Detention Center had information about a plan to smuggle drugs into the

Livingston Parish Detention Center. October 3, the LPSO team saw a woman drop off a man along the road. The man, carrying a package, entered a nearby wooded area. The LPSO team saw the man step onto Detention Center property and head toward the outer perimeter fence of the Detention Center. The man was stopped, but resisted arrest. He was taken into custody. The woman later returned to the area in order to pick up the man she dropped off. She was arrested and charged. October 15, following an extensive investigation, eight inmates were charged for their efforts to attempt to get the seized package of narcotics inside the detention center.
Source: http://www.wafb.com/story/19843731/10-arrested-for-trying-to-smuggle-drugs?hpt=ju_bn5

[Return to top]

Information Technology Sector

37. *October 18, The H* – (International) **Information leak in ZENworks Asset Management disclosed.** The Metasploit developers discovered an information leaking vulnerability in Novell ZENworks Asset Management 7.5 that allows a remote attacker to read files that have system-level privileges and extract all information stored by the application. A researcher from Rapid7 explained that the Web console of ZENworks Asset Management provides two maintenance calls that can be used with hard-coded credentials. One of the calls allows remote attackers to gain access to the filesystem, while the other call gives details of the software's backend database credentials in clear text. The researcher discovered the vulnerability in August and immediately wrote a Metasploit module to exploit it. He then disclosed it to Novell and the U.S. Computer Emergency Readiness Team, and now published the exploit and corresponding Metasploit module.
Source: http://www.h-online.com/security/news/item/Information-leak-in-ZENworks-Asset-Management-disclosed-1732130.html

38. *October 18, The H* – (International) **Apple updates Java for older Mac OS X - kills browser plugin.** Following Oracle's CPU patch day, in which a large number of Java vulnerabilities were fixed, Apple released an update for Java 6 on Mac OS X 10.6.8, 10.7, and 10.8. The update brings Apple's Java 6 in line with Oracle's Java 6 Update 37, but also removes the Apple-provided Java applet plugin from all Web browsers. Apple previously modified its plugin to reduce unnecessary exposure to Java-based malware by disabling the plugin if it went unused for a period of time. This policy has apparently not been sufficient and now the update completely removes the plugin; browsers will display a "missing plugin" message, which, if clicked, will take the user to Oracle's site where they can download the latest Java applet plugin from Oracle.
Source: http://www.h-online.com/security/news/item/Apple-updates-Java-for-older-Mac-OS-X-kills-browser-plugin-1732089.html

39. *October 18, The Register* – (International) **One year on, SSL servers still cower before the BEAST.** The latest monthly survey by the SSL Labs project discovered that many secure sockets layer (SSL) sites remain vulnerable to the Browser Exploit Against SSL/TLS (BEAST) attack, more than a year after the underlying vulnerability

was demonstrated by security researchers. The stealthy piece of JavaScript works with a network sniffer to decrypt the encrypted cookies that a targeted Web site uses to grant access to restricted user accounts. October figures from SSL Pulse survey of 179,000 popular Web sites secured with the ubiquitous SSL protocol reveals that 71 percent (127,000) are still vulnerable to the BEAST attack. The latest statistics show little change from September figures, down just 1 percentage point from the 71.6 percent vulnerable to the BEAST attack recorded in September. Exposure to the so-called CRIME attack was also rife, 41 percent of the sample support SSL Compression, a key prerequisite of the attack. The so-called CRIME technique lures a vulnerable Web browser into leaking an authentication cookie created when a user starts a secure session with a Web site. Once the cookie is obtained, it can be used by hackers to log in to the victim's account on the site.
Source: http://www.theregister.co.uk/2012/10/18/ssl_security_survey/

40. *October 18, Softpedia* – (International) **Citadel trojan Rain Edition represents Fraud-as-a-Service at its best, RSA says.** The developers of the Citadel trojan recently released the 1.3.5.1 version, dubbed Rain Edition. The new variant costs more than its predecessor, but it also possesses new features. One of the most noteworthy new features is called "Dynamic Config." It allows botmasters to interact faster with their victims via browser injection technology. "This nifty function allows Trojan operators to create web injections and use them on the fly, pushing them to selected bots without the hassle of pushing/downloading an entire new configuration file," an RSA researcher explained. "Citadel-infected machines are going to have an instruction to reach out to the C&C every 2 minutes and update themselves with a predefined file where injection 'packs' will be ready to go. The whole system will be managed by a clever distribution mechanism dictating which injection(s) go to which bot or group of bots," he added. This new mechanism makes Citadel a representative for the Fraud-as-a-Service (FaaS) model. That is because botmasters are not forced to do all the work by themselves. Instead, they can hire up to five subordinates to help them create injections. They all have their own section on the administrator panel, which gives them only limited access to the entire operation. The advantage for the injection sellers in this case is that they can work with multiple botmasters.
Source: http://news.softpedia.com/news/Citadel-Trojan-Rain-Edition-Represents-Fraud-as-a-Service-at-Its-Best-RSA-Says-300441.shtml

41. *October 17, Threatpost* – (International) **Oracle leaves fix for Java SE zero day until February patch update.** Oracle will not patch a critical sandbox escape vulnerability in Java SE versions 5, 6, and 7 until its February Critical Patch Update (CPU), according to the researcher who discovered the flaw. The researcher, from security firm Security Explorations, told Threatpost that Oracle said it was deep into testing of another Java patch for the October CPU released October 16, and that it was too late to include the sandbox fix. The researcher said he plans to present technical details on the flaw November 14 at the Devoxx Java Community Conference in Belguim. The exploit relies on a user landing on a site hosting the exploit; an attacker would use a malicious Java applet or banner ad to drop the malware and ultimately have full remote control of a compromised machine.

Source: http://threatpost.com/en_us/blogs/oracle-leaves-fix-java-se-zero-day-until-february-patch-update-101712

42. *October 17, Softpedia* – (International) **Researcher finds denial of service vulnerability in Window 7.** A researcher claims to have identified a denial-of-service (DoS) vulnerability that affects fully updated versions of Windows 7 and possibly even Windows Vista. He revealed that a blue screen of death (BSOD) can be triggered by making a "very specific set of operating system calls." Although he has not been able to determine if the security hole can be used by an attacker to execute arbitrary code, he confirmed that it could be utilized to corrupt kernel memory and cause a DoS state.
Source: http://news.softpedia.com/news/Researcher-Finds-Denial-of-Service-Vulnerability-in-Window-7-300118.shtml

43. *October 17, Threatpost* – (International) **Nitol Botnet shares code with other China-based DDoS malware.** Microsoft learned that much of the code used by the Nitol malware family is copied from free malware resources hosted on Chinese Web sites. Microsoft posted portions of the code online the week of October 15, where similar lines used for denial-of-service (DoS) attack functionality are present in Nitol and on the sites in question. An antivirus researcher at Microsoft said that Nitol.A and Nitol.B also resemble malware used by the IMDDOS and Avzhan botnets, both of which, like Nitol, are used to carry out distributed denial-of-service (DDoS) attacks. Nitol.A and Nitol.B are the most active variants of the Nitol family. The Nitol botnet was recently taken down by Microsoft after it was given permission by the U.S. District Court for the Eastern District of Virginia to take control of the 70,000 sub-domains hosting malware on the 3322.org domain.
Source: http://threatpost.com/en_us/blogs/nitol-botnet-shares-code-other-china-based-ddos-malware-101712

44. *October 17, Softpedia* – (International) **Vodafone 'account update' notifications lead to phishing sites.** Vodafone phishing emails have been seen landing in inboxes in the past few days, informing customers that they need to update their accounts. Cybercriminals are not only after bank account details. The information stored in accounts that customers register on their mobile carrier's site could be just as valuable. Spammers have started sending out alerts entitled "Your Vodafone accounts update." The link does not point to the legitimate Vodafone site, but a Web page designed to trick users into disclosing their usernames and passwords. By gaining access to their victims' accounts, the scammers also gain access to billing information and other sensitive data that can be used to commit identity theft-related crimes.
Source: http://news.softpedia.com/news/Vodafone-Account-Update-Notifications-Lead-to-Phishing-Sites-300149.shtml

45. *October 17, SC Magazine* – (International) **Security beefed up in new Adobe Reader, Acrobat.** The week of October 15, Adobe released new versions of its flagship Reader and Acrobat products to include a number of new security capabilities. Reader XI extends previously introduced sandbox "Protected View" controls — in which PDFs are displayed in a confined environment to prevent malware from running elsewhere on the machine — to now include "read-only" activities so hackers are unable to steal data

via attacks, including so-called screen scrapes. The new Reader and Acrobat editions also include a built-in security feature known as Address Space Layout Randomization, or ASLR. Introduced with the release of Windows Vista in early 2007, ASLR randomizes memory space and significantly lowers the chances for certain code execution attacks to succeed. "Force ASLR improves the effectiveness of existing ASLR implementations by ensuring that all DLLs (dynamic-link libraries) loaded by Adobe Reader or Acrobat XI, including legacy DLLs without ASLR enabled, are randomized," a researcher with the Adobe Secure Software Engineering Team said October 17.
Source: http://www.scmagazine.com/security-beefed-up-in-new-adobe-reader-acrobat/article/264112/

Internet Alert Dashboard

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

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

[Return to top]

Communications Sector

46. *October 18, NorthEscambia.com* – (Florida; Alabama) **Frontier, Verizon customers report widespread telephone outages.** There was no immediate word October 17 on the cause of communications problems in North Escambia, Florida, that left many residents unable to make or receive phone calls. Frontier Communications customers from Molino, Florida north through Walnut Hill and Atmore into Monroe County, Alabama, reported that they were unable to make phone calls outside of Frontier exchanges and unable to receive phone calls from non-Frontier customers. Numerous Verizon Wireless customers also reported problems making and receiving calls or text messages, particularly in the Molino area.
Source: http://www.northescambia.com/2012/10/frontier-verizon-customers-report-widespread-telephone-outages

[Return to top]

Commercial Facilities Sector

47. *October 18, Associated Press* – (Colorado) **Police: 3 arrested for Denver bar killings, fire.** Three people have been arrested in connection with the killing of five people at a Denver bar that was set on fire, apparently to hide the crime, and the motive was robbery, police said October 18. The police commander said the suspects went to Fero's Bar & Grill bar to rob it before closing time October 17, but he did not go into details about how it turned into a murder case. An officer on routine patrol noticed a fire inside the bar. Inside, firefighters found the bodies of one man and four women, including the bar owner. The three suspects were all arrested in Denver. The Denver

medical examiner identified the victims, but did not release the cause of death.
Source: http://www.usatoday.com/story/news/nation/2012/10/18/denver-bar-fire-arrests/1640921/

48. *October 18, Orlando Sentinel* – (Florida) **Police ID gunman in Casselberry salon mass shooting.** Police provided the name of the gunman who stormed into a Casselberry, Florida salon October 18 and shot four women — killing three — before driving away and committing suicide. The suspect killed his ex-girlfriend, the salon manager, and several of her coworkers at the Las Dominicanas M & M Salon on Aloma Avenue. Both the salon manager and the owner of the salon filed domestic violence injunctions against the suspect in recent weeks. He was supposed to report to the Orange County Courthouse October 18 for a hearing in the domestic violence case. A fourth employee was taken to an area hospital, and her condition is unknown. Police said the suspect left the salon, located in a small strip mall near a Family Dollar store, and then shot himself several miles away at a home on Paradise Lane.
Source: http://www.orlandosentinel.com/news/local/breakingnews/os-casselberry-shooting-three-dead-20121018,0,289503,print.story

49. *October 18, WNBC 4 New York* – (New York) **Reported suspicious package in Home Depot not a bomb: Police.** A suspicious package reported inside a Home Depot store on Long Island, New York was not consistent with an explosive device, but police and bomb squad officers were continuing to sweep the premises as a precaution October 17. Police were called to the store on Hempstead Turnpike in Elmont, New York when an employee opened a returned box that was supposed to contain a jigsaw but instead contained other unspecified material. The worker and store managers, on alert after a pipe bomb was discovered inside another Home Depot store in Huntington October 15, called police. All businesses in the strip mall on Hempstead Turnpike, including Office Max and GNC, were evacuated as police and bomb squad responded. The stores were expected to re-open and employees returned to work when the all-clear is issued, police said.
Source: http://www.nbcnewyork.com/news/local/Home-Depot-Suspicious-Package-Elmont-New-York-Hempstead-Turnpike-174637561.html

50. *October 17, CBS News* – (New York) **Pipe bomb found in Long Island Home Depot, suspect arrested.** A suspect was arrested after a pipe bomb in a Long Island, New York Home Depot caused the store to be evacuated October 15, WCBS 2 New York reported October 17. The FBI has begun interviewing employees and combing through surveillance videos as part of their investigation. Sources said the bomb was believed to be part of a larger plot, perhaps an extortion attempt or a full-scale attack timed for the holidays, possibly on "Black Friday," November 23. A statement released by The Home Depot said, "We are cooperating with authorities on their investigation. The safety of our customers and associates is certainly of the utmost importance to us." Charges are pending against the person in custody, a source told WCBS 2 New York. Authorities are trying to decide if the person should be charged on a State or federal level.
Source: http://www.cbsnews.com/8301-504083_162-57534135-504083/pipe-bomb-found-in-long-island-home-depot-suspect-arrested/

51. *October 17, KSNW 3 Wichita* – (Kansas) **Gas leak contained, evacuations end in Goodland.** A major gas leak forced the evacuation of some businesses and homes in Goodland, Kansas. The leak was reported October 17 near the First National Bank. The sheriff said that it appears workers with a boring machine struck a gas line. Utility crews worked to repair the line and it was not until 5 hours later that officials reported the leak was contained and allowed people to return to their homes. "Some areas still remain blocked due to ongoing repair work and emergency crews remain on the scene at this time, however, emergency operations will be demobilizing shortly," said the emergency management director. The evacuated area included the blocks of Broadway, Clark, and Caldwell between 10th and 11th Streets.
Source: http://www.ksn.com/news/local/story/Gas-leak-contained-evacuations-end-in-Goodland/i8ik0O6_XUKv7LH_mptWvw.cspx

52. *October 17, Mississippi Press* – (Mississippi) **St. Martin hotel fire under control, facility heavily damaged.** A major structural fire at a Howard Johnson motel in Mississippi was brought under control. Firefighters from all over Jackson County were joined by units from the Biloxi Fire Department October 17 as the fire appeared to be on the verge of raging out of control. Winds, which hampered firefighting efforts died down and the fire was brought under control, but not before the tower above the elevator shaft collapsed, along with sections of the roof and park of the back wall on the north side of the hotel. Between the fire damage and huge amounts of water poured into the hotel to fight the blaze, the hotel would likely be a total loss.
Source: http://blog.gulflive.com/mississippi-press-news/2012/10/st_martin_motel_fire_under_con.html

[Return to top]

National Monuments and Icons Sector

54. *October 17, Associated Press* – (Colorado) **Fire near Mancos threatening dozens of homes.** The U.S. Forest Service called for evacuations of at least 30 to 40 homes threatened by a wildfire in southwestern Colorado. Fire officials said October 17 that the fast-moving fire 6 miles southeast of Mancos was burning on more than 100 acres near where the Weber Fire burned earlier in 2012. Meanwhile, crews tried to keep another fire in southwest Colorado from spreading toward houses at Vallecito Reservoir. Fire officials said high winds pushed the fire toward the reservoir, and about 20 homes have received pre-evacuation notices. Air and ground crews were not able to attack the fire directly October 17. It was estimated at 200 to 250 acres.
Source: http://www.noco5.com/story/19844723/copters-bulldozer-help-crews-at-sw-colo-wildfire

[Return to top]

Dams Sector

55. *October 17, Springfield Republican* – (Massachusetts) **Work begins to remove Amethyst Brook Dam in Pelham.** Workers removed the first stone from a 1820 dam on Amethyst Brook, Massachusetts, October 17 and opened up another 9 miles of upstream habitat for spawning fish. Work on the demolition began to the applause of State, municipal, and federal officials, who had gathered at the nearby HRD Press building to toast the $193,000 project. HRD Press occupies the site of the former Bartlett Rod Shop Co., which used power from the dam. A coalition that includes the U.S. Fish and Wildlife Service, the State Department of Fish & Game, and the Pelham and Amherst conservation commissions used money from a fund administered by the Holyoke Coal Tar Natural Resource Damages Trustee Council to dismantle the dam, a project that is expected to take about five weeks. The estimated repair cost is $300,000. The fund that is paying for the demolition of the Bartlett Rod Shop Co. dam was established through a 2004 consent decree that required the Holyoke Water Power Co. and the Holyoke Gas & Electric Department to remediate the effects of discharges into the Connecticut River by the former Holyoke Coal Tar, which they succeeded. There was a total of $395,000 in that fund, officials said.
    Source:
    http://www.masslive.com/news/index.ssf/2012/10/officials_fish_applaud_removal.html

56. *October 17, Adrian Daily Telegram* – (Michigan) **Court action to clear way for Red Mill Pond dam repairs.** A petition to establish a water level and special assessment district at Tecumseh's Red Mill Pond in Michigan was to be filed by the end of the week of October 15 in Lenawee county circuit court, the Adrian Daily Telegram reported October 17. Agreements giving the county ownership and right of way to access the dam are now in hand, said the Lenawee County drain commissioner. Signatures of all parties that could claim ownership of the property were needed to go forward with the court action, he said. The Tecumseh City council voted September 24 to grant an easement. Signatures were also collected from the former owner of the failed Red Mill Pond residential development and from the current owner, Kwest Group LLC of Ohio. Former owner Tecumseh Products Co. was also asked to sign off. The drain commission is set to oversee a repair project on the 105-year-old dam structure at Red Mill Pond. The county commission voted in June to authorize court action needed for the proposed $315,000 repair project.
    Source: http://www.lenconnect.com/article/20121017/NEWS/121019499/1001/NEWS

[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