Daily Open Source Infrastructure Report
23 April 2012

Top Stories

- The California Public Utilities Commission said Pacific Gas and Electric will be fined nearly $17 million for irregularities in its gas pipeline safety testing in Contra Costa County. – *Bay City News Service* (See item **4**)
- A court issued $14 million in fines against a Chicago trading firm, two Dutch companies, and three officers for manipulating the price of oil on the New York Mercantile Exchange. – *U.S. Commodity Futures Trading Commission* (See item **13**)
- A Connecticut farm business where a fire had burned for 9 days as of April 20 was cited by state regulators for illegal construction of a solid wood waste facility. – *New Haven Register* (See item **23**)
- Farmers, ranchers, and woodlands in the southwest, southeast, and California could face problems from worsening drought conditions through July, according to federal forecasters. – *MSNBC* (See item **24**)
- All Kansas prison inmates were moved back to a state facility after four escaped from a county jail, the department of corrections said April 19. – *Associated Press* (See item **38**)
- The U.S. Cyber Emergency Response Team warned cyber criminals are attempting highly targeted social engineering attacks on operators of industrial control systems. – *Network World* (See item **42**)

Fast Jump Menu

Energy Sector

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

1. *April 20, Buffalo News* – (New York) **Poor fuel storage records may cost county $800,000.** The failure of Erie County, New York, to keep proper records of gasoline and diesel storage tanks on its property and to ensure several of the tanks were not leaking could cost the county more than $800,000, Buffalo News reported April 20. Earlier in April, the county paid a $275,000 fine for violating two federal environmental laws that regulate the way the county must maintain and monitor above-ground and underground oil storage tanks at its parks, public works facilities, and other properties. County officials also expect to spend as much as $465,000 on additional work to make sure its tanks meet federal environmental standards under the Clean Water Act and other laws. The county legislature voted April 19 to extend a contract to complete a second phase of a project to bring the county's fuel tanks into compliance. The federal penalties lodged against the county stemmed from inspections done by the U.S. Environmental Protection Agency in 2008 of oil storage tanks on county-owned property.
   Source: http://www.buffalonews.com/city/communities/erie-county/article819512.ece

2. *April 20, Middletown Journal* – (Ohio) **Massive fire at oil company poses environmental threat.** A massive fire at an oil company in Pike Township, Ohio, took firefighters 6 hours to get under control April 19 and will require an extensive environmental cleanup. More than 50 agencies responded, including every fire department in Clark County, to the fire at the R.D. Holder Oil Co. The fire produced flames that shot 200 feet up, black smoke that could be seen as far away as Dayton and Butler County, with the plume even showing up on weather radar. Ohio Environmental Protection Agency officials at the scene determined oil spilled into a tributary of Donnels Creek, which feeds into Mad River. Officials used vacuum equipment and

other techniques to remove environmental contaminants, according to the Bethel Township and Wright-Patterson Air Force Base fire chief. Public and private HAZMATs teams contained petroleum-based contaminants to no more than a quarter mile downstream. The cause of the fire is still under investigation, but a fire spokesman believed it ignited while workers transferred a fluid from one tank to another. The company supplies diesel fuel, heating oil, gasoline, Dragon racing fuel, bio-diesels, and lubricants.
Source: http://www.middletownjournal.com/news/massive-fire-at-oil-company-poses-environmental-threat-1362530.html

3. *April 19, azfamily.com* – (Arizona) **Fuel tanker rollover closes highway near Heber, Ariz.** A long section of highway near Heber, Arizona, was closed for more than 8 hours after a fuel tanker crash the morning of April 19. According to a spokesman with the Arizona Department of Public Safety, a 45-mile stretch of Highway 260 was shut down as a result of the crash. The tanker went off the road and rolled over, spilling 7,700 gallons of diesel fuel.
Source: http://www.azfamily.com/news/Fuel-tanker-rollover-closes-highway-near-Heber-Ariz-148190625.html

4. *April 19, Bay City News Service* – (California) **PG&E to pay $17 million for safety violations.** The California Public Utilities Commission (CPUC) confirmed April 19 Pacific Gas and Electric (PG&E) will be fined nearly $17 million for irregularities in the utility's gas pipeline safety testing in Contra Costa County. In January, the CPUC issued a $16.76 million citation for the utility's failure to conduct gas safety tests on more than 13 miles of gas distribution pipelines in several cities in Contra Costa County, including Danville, Antioch, Pittsburg, and Concord. Some stretches of pipeline had not been tested for leaks since 1993, a violation of federal and state pipeline safety regulations, according to the CPUC. PG&E appealed the citation in February. The appeal was denied by a CPUC administrative law judge, and the panel re-ordered the utility to pay the citation.
Source: http://pinole.patch.com/articles/pge-to-pay-17-million-for-safety-violations

5. *April 18, Victoria Advocate* – (Texas) **Oil well compressor on fire; homes evacuated.** Fire and oil field officials are waiting for natural gas to burn off from pipes leading to a compressor on fire near Mission Valley in Victoria County, Texas, April 18. The fire burned for 10 to 11 hours. The pipelines leading into the compressor were closed shortly after the fire started. Representatives from Valerus, which owns the gas compressor, were on site for several hours. The Houston-based company asked the Valerus district manager to respond because of the value of the equipment in danger. "The compressor is about a $1.2 million piece of equipment. But believe it or not, this is not an uncommon occurrence in our business." The company intends to investigate the fire along with the Texas Railroad Commission. Residents of homes within a quarter mile of the equipment were evacuated but have since returned.
Source:
http://www.victoriaadvocate.com/news/2012/apr/18/ep_dreyer_lane_fire_041912_173908/?breaking&local-business

For more stories, see items **13** and **42**

[Return to top]

Chemical Industry Sector

6. *April 17, KPAX 8 Missoula* – (Montana) **Libby man pleads guilty to stealing, detonating explosives.** A convicted felon pleaded guilty in federal court in Missoula, Montana, to stealing explosives from his former employer and then detonating them near Libby. The man was charged with being an "unlawful drug user in possession of explosive materials." Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) agents said he worked for Genesis Mine in Troy for nearly a year. During that time he started stealing explosive materials from the company. Then in December 2011, the man and six other people, including his son tied the stolen explosive to a tree and detonated it in an area outside of Libby. In an interview with ATF agents, the convict admitted stealing a variety of explosives, including detonating cords, high explosive boosters, and pole igniters. He also told federal agents he was a meth addict.
Source: http://www.kpax.com/news/libby-man-pleads-guilty-to-stealing-detonating-explosives/

For more stories, see items **1** and **31**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

7. *April 19, Pottstown Mercury* – (Pennsylvania) **Electrical problem forces 'scram' at Limerick nuke plant.** Exelon Nuclear's Limerick Generating Station in Limerick, Pennsylvania, had to shut down one of its nuclear reactors because of an electrical problem April 19. Unit 1 was shut down due to a malfunction that caused a temporary loss of power to the plant's main generator cooling pumps, according to a communications manager for the site. A Nuclear Regulatory Commission spokesman said the cause of the shutdown was under review, but it appeared to be related to an electrical breaker failure.
Source: http://www.pottsmerc.com/article/20120419/NEWS01/120419333/electrical-problem-forces-scram-at-limerick-nuke-plant&pager=full_story

For another story, see item **42**

[Return to top]

Critical Manufacturing Sector

8. *April 19, U.S. Department of Labor* – (Alabama) **U.S. Department of Labor's OSHA cites metal fabricator in Atmore, Ala., for 11 safety and health violations.** April 19, the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) cited Escofab Inc. for 11 safety and health — including 1 willful — violations

at the company's metal fabrication shop in Atmore, Alabama. The willful safety violation was for failing to correct overhead gantry crane deficiencies. Escofab had the cranes inspected by a private consultant in 2008 and 2011, but failed to correct problems identified, including electrical hazards, and missing and broken parts. Nine serious and one other-than-serious violations were also cited.
Source:
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=22197

For another story, see item **42**

[Return to top]

Defense Industrial Base Sector

9. *April 19, U.S. News & World Report* – (National) **Scientists reprogram plant DNA to identify counterfeit military parts.** A new technology that uses plant genes to track even the most miniscule computer parts is being considered to make sure sophisticated U.S. military equipment such as bomb guidance kits, airplane electronics, and radars are not being made with counterfeit components, according to an April 19 report by U.S. News & World Report. By reprogramming plants' genetic material, Stony Brook, New York-based Applied DNA Sciences can create a tiny marker that can be embedded on computer chips, mixed in with the ink used to print cash, or woven into clothing. The military can then use a device similar to a barcode scanner to instantly "read back" that DNA, verifying the parts are authentic. Experts have warned the electrical components inside some of the most sophisticated military computers are faulty and fraudulent, prompting Congress to pass a law in late 2011 requiring military contractors to guarantee the parts they use in military systems. The new tracking technology uses plant DNA because plants thrive in sunlight, whereas animals' DNA can break down from ultraviolet rays. In 2011, the U.S. military reported more than 1,300 counterfeit parts in their weapons — more than 4 times the 2009 number — to IHS iSuppli, a company that monitors the industry.
Source: http://www.usnews.com/news/articles/2012/04/19/scientists-reprogram-plant-dna-to-identify-counterfeit-military-parts

[Return to top]

Banking and Finance Sector

10. *April 20, Pocono Record* – (Pennsylvania; New Jersey) **Did Pocono Mountain cops catch 'Silent Bandit' bank robber?** Police arrested a suspect in a Mount Pocono, Pennsylvania bank robbery April 19, and authorities are investigating whether he is the FBI's "Silent Bandit," suspected in a wave of robberies in eastern Pennsylvania and New Jersey. April 19, a man entered the ESSA Bank at Weis Markets in Mount Pocono, threatened tellers, and demanded money, but he did not display a weapon, Pocono Mountain Regional Police said. Minutes after the robbery, the suspect was spotted driving near the state police barracks in Swiftwater. He was stopped and

arrested. The FBI has been investigating five bank robberies in the Lehigh Valley, Bucks County, and New Jersey since April 3. A sixth, unsuccessful, robbery reported April 18 at a PNC Bank branch in Flemington, New Jersey, was also believed to be linked to the "Silent Bandit." All of the robberies occurred at banks inside grocery stores.
Source:
http://www.poconorecord.com/apps/pbcs.dll/article?AID=/20120420/NEWS/204200325/-1/news

11. *April 20, International Business Times* – (National; International) **SEC accuses British twins of running 'stock picking robot' scam.** The U.S. Securities and Exchange Commission (SEC) April 20 accused a pair of British twins of duping American investors into paying $1.2 million for subscription to a newsletter featuring a phony stock-picking robot. The two were hit with a SEC suit in a New York federal court accusing them of touting a sophisticated trading program dubbed "Marl" that could pick out penny stocks poised to jump in value. "The 'stock picking robot' was a work of fiction," the SEC said. "The defendants' story was persuasive. Approximately 75,000 investors, the vast majority of whom lived in the United States, paid ... for annual subscriptions to the Doubling Stocks newsletter and copies of the robot software." The brothers' tips actually came from stock promoters that paid them more than $1.8 million in fees, none of which was disclosed to investors, the SEC alleged. Investors would pay $47 for annual newsletter subscriptions, plus an additional $97 for a download version of the stock-picking robot, the complaint said. The software, however, was designed to take stocks from a database compiled by the brothers. The SEC said the cam was a pump-and-dump scheme to generate trading volume for thinly-traded stocks.
Source: http://www.ibtimes.com/articles/331212/20120420/sec-investment-scheme-robot.htm

12. *April 20, Boston Herald* – (Massachusetts) **SEC fines MIT prof and son $5M in hedge fund fraud.** A Massachusetts Institute of Technology professor and his son must shell out nearly $5 million and have been barred from the securities industry in connection with U.S. Securities and Exchange Commission (SEC) fraud charges that claim the pair and their hedge fund firms mislead investors about their investment strategy and past performance, the Boston Herald reported April 20. An SEC investigation found that a Sloan School of Management professor and his son raised millions for their hedge funds through GMB Capital Management LLC and CMB Capital Partners LLC by falsely telling investors they had a lengthy track record of success based on actual trades using real money, when in reality, the pair knew the track record was based on back-tested hypothetical simulations. They also misled investors in certain funds to believe they used quantitative optimal pricing models devised by the professor to invest in exchange-traded funds and other liquid securities, the SEC said. Instead, they merely invested the money almost entirely in other hedge funds. GMB Capital Management later provided false statements to SEC staff examining the firm's claims in marketing materials of a successful track record. The father and son agreed to be barred from the securities industry and pay $4.8 million. The SEC said that over 3 years they raised more than $500 million for eight hedge

funds and various managed accounts while making representations to investors.
Source:
http://www.bostonherald.com/business/general/view.bg?articleid=1061125890&srvc=rss

13. *April 19, U.S. Commodity Futures Trading Commission* – (New York; Illinois; International) **Federal court orders $14 million in fines and disgorgement stemming from CFTC charges against Optiver and others for manipulation of NYMEX crude oil, heating oil, and gasoline futures contracts and making false statements.** The U.S. Commodity Futures Trading Commission (CFTC) April 19 announced it obtained $14 million in civil monetary penalties and disgorgement pursuant to a federal court consent order against defendants Optiver Holding BV, a global proprietary trading company headquartered in the Netherlands, and two subsidiaries — Optiver US, LLC (Optiver), a Chicago-based corporation, and Optiver VOF, a Dutch company, as well as against three former company officers responsible for the unlawful trading. The CFTC's complaint charged the defendants with engaging in manipulation and attempted manipulation of New York Mercantile Exchange (NYMEX) Light Sweet Crude Oil, New York Harbor Heating Oil, and New York Harbor Gasoline futures contracts in March 2007. The complaint further charged Optiver and one of the individuals with concealing the manipulation by making false statements in response to an inquiry from NYMEX. The consent order requires the defendants to pay a $13 million civil monetary penalty and $1 million in disgorgement. The CFTC's complaint alleged that in at least 19 instances in March 2007 the defendants attempted to manipulate prices, and in at least 5 instances were successful in causing artificial prices. In each instance, defendants intentionally accumulated a large position in Trading at Settlement (TAS) contracts. As alleged, the defendants offset their large TAS position by trading futures contracts shortly before and during the closing period in a manipulative manner.
Source: http://www.cftc.gov/PressRoom/PressReleases/pr6239-12

14. *April 19, Federal Bureau of Investigation* – (Virginia) **Hampton Roads businessman indicted for alleged $11 million historic tax credit fraud scheme.** A Chesapeake, Virginia man was indicted by a federal grand jury accused of engaging in a 6-year historic tax credit fraud scheme that cost the United States and Virginia more than $11 million and enriched him and others by about $8 million, according to an April 19 FBI press release. The man "is accused of cheating taxpayers and investors out of millions intended to preserve historic properties in Virginia," a U.S. attorney said. The man was charged in a 14-count indictment that included 1 count of conspiracy to commit wire fraud, 7 counts of wire fraud, and 6 counts of unlawful monetary transactions. According to the indictment, from January 2006 through March 2012, the man and his business partner allegedly borrowed funds from financial institutions to purchase and renovate properties that could qualify for historic rehabilitation tax credits. They had no personal use for the credits, but intended to sell them to investors in need of reducing their own tax liability. The man and his partner are accused of fraudulently increasing the federal and state historic tax credits for which they were eligible by inflating the amounts spent on renovating the properties, fabricating other necessary documents, and making other material misstatements. He and his business partner also allegedly sold

these fraudulently obtained tax credits to corporate investors for millions of dollars by fabricating additional documents and representing that investor funds would be used to support the renovation projects.
Source: http://www.fbi.gov/norfolk/press-releases/2012/hampton-roads-businessman-indicted-for-alleged-11-million-historic-tax-credit-fraud-scheme

15. *April 18, U.S. Commodity Futures Trading Commission* – (Colorado) **Federal court orders Colorado defendants Flint-McClung Capital LLC to pay over $6 million in CFTC action charging them with running forex Ponzi scheme.** The U.S. Commodity Futures Trading Commission (CFTC) April 18 announced a Colorado district court entered an order against defendants Flint-McClung Capital LLC (FMC) of Englewood, Colorado, and one individual requiring them jointly and severally to pay restitution of $1,701,250 and a $4.3 million civil monetary penalty. The order also imposes permanent trading and registration bans against the defendants. The court's order of default judgment and permanent injunction stems from a June 2011 CFTC enforcement action that charged FMC and the individual with fraud and misappropriation in an off-exchange foreign currency (forex) Ponzi scheme. The order finds that, beginning around March 2010, the defendants fraudulently solicited and received at least $2.4 million from 20 customers by touting their success in trading forex. In their solicitations, the individual and FMC falsely represented FMC had about $300 million in pool participant funds, which were segregated and in reserve, and used about $500 million in FMC proprietary funds to trade forex. However, according to the order, the defendants engaged in little, if any, trading on behalf of pool participants. Of the funds solicited and received, the defendants misappropriated at least $1,701,250 for personal expenses.
Source: http://www.cftc.gov/PressRoom/PressReleases/pr6236-12

For another story, see item **19**

[Return to top]

Transportation Sector

16. *April 20, Associated Press; KTWV 94.7 FM Los Angeles* – (California) **Big-rig crash blocks key freeway corridor to port.** A big-rig crash blocked a southern California freeway corridor to the Port of Long Beach, the Associated Press reported April 20. The California Highway Patrol said a trucker swerved to avoid a vehicle on the southbound Interstate 710 and flipped, slamming into the concrete center divider. The truck was hauling an empty shipping container. Wreckage and debris littered both sides of the Long Beach Freeway in the Carson area north of I-405, shutting down most lanes in both directions for hours. KTWV 94.7 FM Los Angeles said all but one northbound lane was reopened before the April 20 morning commuter rush.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/04/20/state/n045319D24.DTL

17. *April 20, Reuters* – (New York) **Birds force Delta emergency landing at Kennedy Airport.** A bird strike forced a Delta Air Lines flight bound for Los Angeles to make

an emergency return to New York's John F. Kennedy International Airport 10 minutes after takeoff April 19, authorities said. The pilot of Delta Flight 1063 reported an engine-related problem and landed the Boeing 757 safely at the airport from which it departed, said a spokeswoman for the Federal Aviation Administration (FAA). The Port Authority of New York and New Jersey, which oversees airports in metropolitan New York, said the pilot reported the "engine issue" 10 minutes into the flight. Such strikes are not uncommon. The FAA maintains a page on its Web site dedicated to wildlife strikes and said there were 121,000 strikes, mostly birds, between 1990 and 2010, averaging 26 strikes a day in recent years.
Source: http://www.reuters.com/article/2012/04/20/uk-usa-plane-birds-idUSLNE83J01V20120420

18. *April 19, Los Angeles Times* – (Florida) **Plane crash off Florida coast: Navy, Coast Guard search for pilot.** U.S. Coast Guard (USCG) and Navy forces were dispatched to the scene of a plane crash off the coast of Florida, the Los Angeles Times reported April 19. There was no word April 20 about the fate of the pilot believed to have become incapacitated at the controls. The small aircraft circled in the skies for hours over the Gulf of Mexico as air traffic controllers watched. They apparently tried for hours to make contact, but all attempts failed, pointing to the likelihood the pilot had perhaps fallen unconscious at the controls, or suffered a heart attack. The prospect of an unresponsive plane flying out of control sent up alarms: Two F-15 fighters under the direction of North American Aerospace Defense Command out of 159th Fighter Wing in New Orleans reached the aircraft. They also were unable to make contact with the pilot, said an April 19 statement. The USCG said the crash took place about 120 miles west of Tampa, in the gulf. The plane was completely submerged, no longer visible from the surface, officials said.
Source: http://www.latimes.com/news/nation/nationnow/la-na-nn-florida-plane-crash-pilot-fate-unknown-20120419,0,5245736.story

For more stories, see items **3**, **4**, and **5**

[Return to top]

Postal and Shipping Sector

19. *April 20, Sacramento Bee* – (California) **Sacramento man indicted for bank fraud, identity theft.** A Sacramento, California man was indicted April 20 by a federal grand jury for bank fraud and identity theft. He was charged with multiple counts of bank fraud, submitting false documents to an agency of the United States, obtaining U.S. mail by fraud, aggravated identity theft, and credit card fraud, said a Department of Justice news release. He allegedly submitted, in the names of numerous victims, false U.S. mail forwarding forms to obtain U.S mail by fraud. With the contents of the misdirected mail and other unlawfully obtained victim identification and financial information, he allegedly committed many acts of bank and credit card fraud. He also is charged with posing as a victim on multiple occasions, and with purchasing and obtaining by fraud, car parts, debit cards, and more than a dozen iPads and iPhones. He was arrested April 9 at his Sacramento apartment by U.S. Postal Service inspectors.

Source: http://www.loansafe.org/sacramento-man-indicted-for-bank-fraud-identity-theft

20. *April 19, WAVE 3 Louisville* – (Kentucky) **Recluse spiders shut down Fairdale post office.** The United States Postal Service temporarily shut down the post office in the Fairdale section of Louisville, Kentucky, because of the presence of recluse spiders. The Fairdale location was expected to reopen April 23 after the spiders' removal. Postal officials said customers with post office boxes can get their mail at the Hillview branch.
Source: http://www.wave3.com/story/17578365/recluse-spiders-shut-down-fairdale-post-office

[Return to top]

Agriculture and Food Sector

21. *April 20, Food Safety News* – (Illinois) **Felony indictment charges four in tainted cheese conspiracy.** A federal grand jury in Chicago returned a 6-count indictment against four individuals, alleging they were involved in a 2007 scheme to ship more than 110,000 pounds of contaminated Mexican-style cheese, Food Safety News reported April 20. The indictment does not claim the cheese caused human illnesses or other public health consequences, according to a U.S. attorney for the Northern District of Illinois. However, lab analysis showed the cheese was adulterated with Salmonella, E. coli, and other illness-causing bacteria, he said. One defendant owned an Illinois company that imported the dried Mexican cheese, and another defendant owned a Wisconsin company with a facility in Elmhurst, Illinois, that distributed cheese nationwide. The indictment charges the defendants with illegally distributing cheese, which had been returned by dissatisfied customers, after scraping off mold and fungus so it could be resold. They are also charged with lying to inspectors from the U.S. Food and Drug Administration by creating and sending the agency false documentation. From the Elmhurst facility, the cheese was distributed to retail stores in Illinois, Indiana, Michigan, Georgia, and Texas under the Queso Cincho De Guerrero brand name. The dry hard Mexican cheese was the subject of a recall in September 2007.
Source: http://www.foodsafetynews.com/2012/04/felony-indictment-charges-four-in-cheese-conspiracy/

22. *April 20, Associated Press* – (National) **FDA: Gulf seafood safe despite oil spill concerns.** Photos of fish with sores may raise concern about long-term environmental effects of the massive BP oil spill, but federal health officials say the Gulf seafood that is on the market is safe to eat, the Associated Press reported April 20. After all, diseased fish are not allowed to be sold, said a doctor who heads the U.S. Food and Drug Administration's Gulf Coast Seafood Laboratory. "It's important to emphasize that we're talking about a low percentage of fish," he said. "It doesn't represent a seafood safety hazard." Two years after the oil spill, scientists cite lesions and other deformities in some Gulf fish as a sign of lingering environmental damage. They can not say for sure what is causing the fish ailments or if there really are more sick fish now than in the past.

Source: http://health.usnews.com/health-news/news/articles/2012/04/20/fda-gulf-seafood-safe-despite-oil-spill-concerns

23. *April 20, New Haven Register* – (Connecticut) **Connecticut DEEP slaps violation notice on North Haven/North Branford farm business where fire has burned for 9 days.** The Connecticut Department of Energy and Environmental Protection (DEEP) issued a notice of violation to a farm business where a fire had been burning on the North Haven-North Branford line for 9 days April 20. DEEP mailed the notice to the business April 18, saying it appears as if the farm built or created a solid waste facility where more than 10 cubic yards of wood waste — which includes tree limbs, trunks, branches, and other vegetative matter — was disposed of without a plan or permit issued by DEEP. Meanwhile, North Haven and North Branford officials, including those from the Quinnipiack Valley and East Shore District health departments, received air quality complaints from residents who were bothered by the smoke. Also, Eight-Mile Brook which runs through Rimmon Road in North Haven, was darkened as a result of the fire. Berms must be built so there will be no more runoff, the North Branford fire chief said. He said the DEEP took samples of water from a North Haven watercourse. There were dead fish in a pond, and the fire is being blamed for that.
Source: http://www.nhregister.com/articles/2012/04/20/news/doc4f91431b7ba43305912353.txt

24. *April 19, MSNBC* – (National) **Drought forecast for southwest, California 'not optimistic'.** Most of the southwestern region of the United States as well as parts of California and the southeast can expect drought conditions to worsen through July, federal forecasters said April 19. "Overall, the current Drought Outlook is not optimistic," the National Weather Service said in summarizing its forecast. Besides affecting farmers and ranchers, drought means a greater risk of wildfires, especially in areas expecting a warmer than average spring. "May – July is expected to be warmer than normal" in the southwest and west, the service added in a more detailed report. "For most of the southwestern and western part of the country, drought is expected to persist in most locations and expand into the central Rockies," it added. "In addition, mountain snowpack, the source of a lot of the region's moisture, is starting off below normal, and as a result, summer streamflows are expected to be abnormally low," forecasters noted. Most of California and Nevada, as well as parts of Colorado, Oregon, Texas, Utah, and Washington state, are also forecast to see drought persisting or intensifying. On the East Coast, most of Georgia and South Carolina, as well as parts of Alabama, Delaware, and Maryland, are expected to see continued or worse drought conditions.
Source: http://usnews.msnbc.msn.com/_news/2012/04/19/11288192-drought-forecast-for-southwest-california-not-optimistic?lite

25. *April 19, Bloomberg* – (National) **Freeze damages grape juice crop.** An April freeze damaged grape crops from Michigan to New York that in 2011 supplied about two-thirds of the U.S. fruit used to make grape juice, government and industry officials said, Bloomberg reported April 19. About 90 percent of juice-grape crops were damaged in Michigan, the third-largest U.S. grower, and as much as 50 percent were hurt in New York, the No. 2 producer, and in Pennsylvania and Ohio, said the director of member

relations for the National Grape Cooperative Inc., the owners of Welch's juices and jellies. Cold weather destroyed the primary buds on plants, and secondary buds will produce 35 percent of normal output. Apples, grapes, and cherries were the hardest hit when temperatures fell below 32 degrees Fahrenheit from April 6 to April 14 across the Midwest, especially in Michigan, said South Dakota's climatologist, who led a media briefing by telephone for the National Oceanic and Atmospheric Administration. The cold spell followed unusually warm weather in March that led to an early start to growing season.
Source: http://www.sltrib.com/sltrib/world/53952621-68/grape-april-crops-michigan.html.csp

For another story, see item **48**

[Return to top]

Water Sector

26. *April 20, Quincy Patriot Ledger* – (Massachusetts) **Leak sends untreated sewage into Weymouth's Back River.** Between 80,000 and 100,000 gallons of untreated sewage ended up in the Back River after a pipe carrying waste from a pumping station cracked, the water and sewer superintendent of Weymouth, Massachusetts said April 19. The spill was discovered April 18. The pumping station could not be shut off until the town had set up an emergency bypass, which took nearly 24 hours. A spokesman for the department of environmental protection said the agency is assessing the spill's effect on the river.
Source: http://www.patriotledger.com/topstories/x513712295/Leak-sends-untreated-sewage-into-Weymouth-s-Back-River

27. *April 19, WTOL 11 Toledo* – (Ohio) **City making emergency water system repairs.** The city of Toledo, Ohio, is in the process of making emergency repairs to a critical component of its water system at the facility which feeds water to the Collins Park treatment plant, Toledo's Department of Public Utilities engineer said April 19. If this problem had occurred during the summer, a water restriction alert would have been issued, and the city is hoping to finish repairs on two of the four pumps that broke down April 14 at the low service pump station before peak season arrives. Each pump has a capacity of 45 million gallons per day, and daily usage is running over 60 million gallons. The facility currently has no back-up in case a working pump breaks down. "We are getting proposals to have some temporary bypass pump, it will bypass the low service pump one and two in order to augment our demands if needed or provide redundancy if needed," the engineer said. The mayor's office has signed emergency purchase orders. The city hopes to return the facility to full capacity within the next 2 months.
Source: http://www.wtol.com/story/17589793/city-making-emergency-water-system-repairs

28. *April 19, Wilmington Star-News* – (North Carolina) **Utility's mistake spills sewage.** The Cape Fear Public Utility Authority (CFPUA) in North Carolina made a

mistake during construction work 6 months ago that started a spill of an estimated 386,000 gallons of sewage, officials said April 19. The leak was found April 12 when personnel from Wilmington's stormwater department reported an odor at manmade wetlands near St. James Place, according to the city's stormwater services manager. A permanent fix will be completed in 3 weeks, said CFPUA's chief operating officer. He said the leak is believed to have started when crews rebuilt a sewer line there and failed to connect a privately owned wastewater pipe connecting a bakery and a deli to the wastewater system. The contractor and project inspectors believed the line was abandoned, said the services superintendent. Some of the wastewater entered Burnt Mill Creek, which drains into the Cape Fear River, according to a CFPUA news release. The city will issue a notice of violation, the city's stormwater services manager said.
Source: http://www.starnewsonline.com/article/20120419/ARTICLES/120419596/-1/sports03?Title=Nearly-400-000-gallons-of-sewage-spilled-near-South-Kerr-Avenue

29. *April 18, Homeland Security News Wire* – (Arizona; International) **Water vulnerability in U.S. border region.** A team of bilingual and binational researchers from the University of Arizona and the Colegio de Sonora in Hermosillo, Sonora, Mexico, issued a casebook that depicts the water vulnerability and potential adaptation to climate change throughout the Arizona-Sonora region, a University of Arizona release reported April 16. For the last 3 years, the research team has worked closely with water managers, disaster relief planners, and other decision-makers in Arizona and Sonora to assess the capacity that governments, private enterprises, and individuals might have to better prepare for, or adapt to, such changes. Researchers found increased vulnerability of urban water users to climatic changes because of factors such as aging or inadequate water-delivery infrastructure, over-allocation of water resources within the region, and the location of poor neighborhoods in flood-prone areas or other areas at risk. Adding to vulnerability issues, agriculture was noted as consuming approximately 70 to 80 percent of available water in the Arizona-Sonora region.
Source: http://www.homelandsecuritynewswire.com/dr20120418-water-vulnerability-in-u-s-border-region

For more stories, see items **1**, **2**, **23**, and **42**

[Return to top]

Public Health and Healthcare Sector

30. *April 20, Watertown Daily Times* – (New York) **Grand jury charges two Carthage Area Hospital nurses with stealing drugs.** A Carthage Area Hospital nurse was indicted in New York on 69 charges, including 9 felonies of first-degree falsifying business records to steal drugs from the hospital, while a grand jury charged a second nurse with 24 misdemeanors for similar activities, the Watertown Daily Times reported April 20. Other charges include 20 misdemeanor counts each of obtaining a controlled substance by fraud, fifth-degree criminal possession of stolen property, and petit larceny. The charges were contained in a grand jury indictment handed up April 19. It is alleged that from April 11, 2011 to October 26, 2011, the registered nurse made false

entries into the Carthage hospital's automated medication dispensing system by entering an invalid reason for dispensing controlled substances in an attempt to conceal that she was stealing the drugs. It was further alleged she dispensed more controlled substances from the system than called for in valid dispensing orders.
Source: http://www.watertowndailytimes.com/article/20120420/NEWS07/704209859

31. *April 20, U.S. Environmental Protection Agency* – (Georgia; National) **EPA orders a stop sale of Zep, Inc. disinfectant for use in hospitals.** The U.S. Environmental Protection Agency (EPA) issued a Stop Sale, Use, or Removal Order (SSURO) to Zep, Inc., located in Atlanta, Georgia, to stop the sale of "ZEP Formula 165," a disinfectant intended for use in hospitals. Under EPA's antimicrobial testing program, ZEP Formula 165 was evaluated, and it was determined that contrary to labeling claims, the product was ineffective against Mycobacterium Tuberculosis.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/1e674fdccbf8dcfc852579e60050663d?OpenDocument

32. *April 20, Occupational Health & Safety* – (National) **Hospital-linked infections down, CDC says.** Occupational Health & Safety reported April 20 that a new Centers for Disease Control and Prevention (CDC) state-by-state breakdown of health care-associated infections showed reductions in infection rates across the country. The CDC report also pinpointed that some medical procedures will require stronger infection prevention efforts to maximize patient safety. The report includes a summary measure called a standardized infection ratio, which allows tracking of prevention efforts over time. The data in the report were submitted by hospitals to the CDC's National Healthcare Safety Network, the agency's infection tracking system used by more than 7,800 health care facilities nationwide. This is the first time that CDC has released a standardized infection ratio for central line-associated bloodstream infections for each of the 50 states. As seen in the report, 21 states had significant decreases in central line-associated bloodstream infections between 2009 and 2010.
Source: http://ohsonline.com/articles/2012/04/20/hospital-linked-infections-down-cdc-says.aspx?admgarea=news

33. *April 19, Security News Daily* – (National) **Wearable firewall stops pacemaker hacking.** Security News Daily reported April 19 that researchers from Purdue and Princeton universities have developed a solution to what could be catastrophic problem for millions of people who use insulin pumps, pacemakers, and other personal medical devices that rely on wireless communication to function: MedMon — a signal-jamming personal firewall for medical devices that detects potentially malicious communications going into, or coming from, a wearable or implanted device. After identifying malicious signals, MedMon employs electronic jamming, similar to technology used in military systems, to prevent any potentially harmful wireless commands from getting through to the device and causing it to falter or accept instructions that could cause its wearer harm. The research team highlighted the need for its prototype by replicating, in the lab, an attack on a diabetes monitoring system, which consists of a continuous glucose monitor and an insulin pump that communicate wirelessly with each other. Analyzing a commercially available glucose monitor, the scientists were able to

eavesdrop on the wireless communication sent to the device — they used off-the-shelf software and hardware — and to reverse-engineer the communication protocol, discover the device PIN, and send their own malicious data to it, including instructions to start and stop insulin injection.
Source: http://www.securitynewsdaily.com/1753-firewall-prevent-pacemaker-hacking.html

34. *April 18, U.S. Food and Drug Administration* – (New Jersey; National) **U.S. Marshals seize ultrasound gel product at a New Jersey company.** U.S. Marshals, acting at the request of the Food and Drug Administration (FDA), seized Other-Sonic Generic Ultrasound Transmission Gel located at Pharmaceutical Innovations Inc. in Newark, New Jersey, April 18 after an FDA analysis found product samples contained dangerous bacteria. The seizure included all lots of the gel product manufactured between June 2011 and December 2011. Until they were seized, the products were held under embargo by the New Jersey Department of Health and Senior Services at the FDA's request. Under the Federal Food, Drug, and Cosmetic Act, the seized gel is adulterated, because product samples were contaminated with two strains of bacteria, Pseudomonas aeruginosa and Klebsiella oxytoca. The gel is also misbranded because it is dangerous to health when used in the manner suggested in the labeling. These bacteria pose serious risks of infection to individuals exposed to the product.
Source: http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm300838.htm

[Return to top]

Government Facilities Sector

35. *April 20, WANE 15 Fort Wayne* – (Indiana) **Meth lab found in Trine student's apt.** A housing complex at Trine University, located in Angola, Indiana, had to be evacuated early April 19 after an alleged methamphetamine lab was found in the apartment of a student. A university villa had to be cleared after a smell of chemicals was detected and police were called. "Due to the inhalation hazards and fire hazard, the building was evacuated," said a Steuben Circuit Court probable cause affidavit. Students were allowed back in their apartments later the same day. One student was arrested and logged into jail early April 19. Two students, apparently roommates of the arrested student, were taken to the hospital for observation. The student under arrest faced a charge of Class D felony possession of precursors or reagents, Class D felony maintaining a common nuisance, and Class A misdemeanor possession of paraphernalia.
Source: http://www.wane.com/dpp/news/crime/meth-lab-found-in-trine-students-apt

For more stories, see items **1**, **9**, and **18**

[Return to top]

Emergency Services Sector

36. *April 19, Salt Lake Tribune* – (Washington) **Dispatcher in murder-suicide reprimanded.** A Washington state dispatcher who took a social worker's 9-1-1 call just before a man killed his children and himself in a house fire has been reprimanded for allowing 22 minutes to lapse before help arrived, the Salt Lake Tribune reported April 19. The dispatcher violated four law enforcement support agency policies in his handling of the call, though he did correctly assign the call a priority that indicated an "imminent danger to life or property." The dispatcher took the 9-1-1 call February 5 after the man locked out a social worker who was supposed to supervise a visit with his sons at his rental home in Graham, Washington. The dispatcher asked the social worker seemingly unimportant questions and failed to grasp the situation: when the social worker said she smelled gas, the dispatcher assumed she smelled the fumes of her own idling car, according to a letter obtained by the Salt Lake Tribune. The house was doused with gasoline, and the man hit both boys in the head with a hatchet before he set the house on fire.
Source: http://www.sltrib.com/sltrib/news/53942610-78/call-powell-lovrak-dispatcher.html.csp

37. *April 19, Niles Daily Star* – (Michigan) **Hackers attack Berrien County website.** Computer hackers gained access to the Berrien County, Michigan Web site April 15 and executed a plan the hackers called, "SSS = Shoot the Sheriff Sunday." Anonymous IRC, the name of the hacker group, placed material on the Berrien County Sheriff's Department Web site, including profanity and the group's views toward government agencies. After authorities learned of the cyber attack they quickly shut down the Web site. The Berrien County undersheriff said the county network was not compromised, and no personal information was obtained by the group beyond what was available on the county site and the sheriff's department site. Both Web sites are stored off site by an independent company and are separate from the county network. The county Web site returned to service April 17, and the sheriff's department's site was back online April 18. The hackers gained access to password information for a select few county employees who had access to update and make changes to the Web site. Those passwords have been changed.
Source: http://www.nilesstar.com/2012/04/19/hackers-attack-berrien-county-website/

38. *April 19, Associated Press* – (Kansas) **Kansas removes all inmates from county jail after 4 escape; 2 remain at large.** All Kansas prison inmates were moved back to a state facility after four escaped from a county jail, including a convicted murderer who remains at large, the department of corrections said April 19. The remaining 18 prison inmates who were being held in the Ottawa County Jail because of prison overcrowding were returned to the state prison in Ellsworth, a department spokesman told the Associated Press. Twenty-two inmates were transferred from Ellsworth in January to help alleviate overcrowding. Overcrowding in Kansas' prisons has been exacerbated in recent years by closures and budget cuts. Inmate counts earlier in 2011 showed male prisons are housing 8,635 inmates, 266 over capacity. The spokesman also said the department had informal internal discussions about providing supplemental training to staffers at county jails that house state inmates.

Source: http://www.foxnews.com/us/2012/04/19/2-kan-jail-inmates-at-large-1-in-custody-in-neb/?test=latestnews

For more stories, see items **18** and **52**

[Return to top]

Information Technology Sector

39. *April 20, Help Net Security* – (International) **Fake 'Steam Cracker' steals user credentials.** Users of Valve's Steam game sales and distribution platform are being targeted by malware peddlers; the lure is a "Steam Cracker." It is being offered on YouTube and on many gamer forums, and it supposedly gives the users access to all games for free. The scammers offer simple instructions for installing the software: disable antivirus software and firewall, then replace the original steam.exe file with the downloaded, cracked one. "The file in question is a fake Steam client, which uses aspects of the real thing but just falls short of being 100 percent convincing (file size, file, and of course the fact that this file isn't digitally signed unlike the real Steam executable)," a GFI researcher said. If the user runs Windows Vista or later versions of the platform, the file runs and shows the fake client that looks legitimate. The creators even included the legitimate store.steampowered(dot)com pages inside the user interface and links to the genuine Playstation Network ID log-in page, the researcher said, but he warned that even though the phishing of credentials is not obvious, it does not mean the users' log-in credentials are safe. The fake Steam client looks for the serial codes of games along with more general programs such as design packages, movie players, system defraggers, code tweakers, and iPod converters, the researcher explained. The malware employs keylogging to accomplish this task.
Source: http://www.net-security.org/malware_news.php?id=2079&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

40. *April 20, H Security* – (International) **Ruby 1.9.3 update fixes RubyGems security problem.** The Ruby development team published an update to the 1.9.3 series of its open source programming language to fix a vulnerability found in the RubyGems package management framework. The maintenance release of the scripting language, labeled 1.9.3-p194, updates RubyGems to close a security hole that caused SSL server verification to fail for remote repositories. This was addressed by disallowing redirects from https to http connections and by enabling the verification of server SSL certificates in an updated version of RubyGems, 1.8.23; more details on these issues are provided in the latest RubyGems History file. The developers encouraged those who use https source in .gemrc or /etc/gemrc to upgrade as soon as possible.
Source: http://www.h-online.com/security/news/item/Ruby-1-9-3-update-fixes-RubyGems-security-problem-1544248.html

41. *April 20, H Security* – (International) **New version of OpenSSL closes security holes in ASN1 parser.** A member of Google's Security Team told the OpenSSL developers

of a security hole in the current version of their open source library. The errors occur when parsing ASN1 data via the asn1_d2i_read_bio() function. According to the OpenSSL advisory and the member's message, the issue affects applications that process external X.509 certificates or public RSA keys. The OpenSSL developers released versions 1.0.1a, 1.0.0i, and 0.9.8v to fix the "ASN1 BIO" problem but the advisories did not state whether the update was urgent. The OpenSSL team discussed a "potentially exploitable vulnerability" and the Google Security Team member provided further details by saying the issue "can cause memory corruption," but neither spoke about potential consequences. The full scope of the problem will most likely only be revealed once a Metasploit module is released. However, the OpenSSH project's own SSH server was unaffected. A researcher wrote that sshd verifies RSA keys with the custom openssh_RSA_verify() function which, he said, already helped avoid eight exploitable bugs in the ASN1 parser. Fixed OpenSSL packages for Ubuntu and OpenBSD were already released. Fixes for Red Hat Enterprise Linux and Fedora will be issued soon.
Source: http://www.h-online.com/security/news/item/New-version-of-OpenSSL-closes-security-holes-in-ASN1-parser-1543932.html

42. *April 19, Network World* – (International) **US-CERT: Social engineers target utilities with fake Microsoft support calls.** The U.S. Cyber Emergency Response Team recently warned that cyber criminals are attempting highly targeted social engineering attacks on operators of industrial control systems. These utility companies are receiving phone calls warning of infected PCs. The utilities receive a call from a representative of a large software company — allegedly, the one that sold them the operating system on their computers — warning them their PCs have viruses and to take a series of steps so the caller can help the operator fix the problem. The calls purport to be from the "Microsoft Server Department" informing the utilities they have a virus. The caller tries to convince the utility operators to start certain services on their computer (likely, those services would allow unauthorized remote access).
Source: http://www.networkworld.com/community/node/80337

43. *April 19, Threatpost* – (International) **Analysis: Flashback spread via social engineering, then Java exploits.** Kaspersky Lab's latest analysis of the Mac OS X Flashback botnet revealed its malware was spread via drive-by downloads on hacked WordPress Web sites. From September 2011 until February 2012, the Flashback creators distributed the trojan through compromised WordPress sites that prompted users to download various iterations of a fake Adobe Flash Player update that was, in actuality, the Mac trojan. The attacks started using social engineering lures, and it was not until February that Flashback authors began using exploits to grow the botnet. They exploited known Java vulnerabilities, at least two of which date back as far as June 2009. More importantly, though, Flashback's creators took advantage of the window of exposure between Oracle and Apple's patch schedules. A Kaspersky researcher said Apple creates its own patches to fix Java vulnerabilities instead of using Oracle's. So, the bugs were already patched by Oracle, but Apple had not yet deployed patches. The researcher noted that on average, historically speaking, there was a 2-month delay between Oracle's fixes, which come first, and Apple's. In March 2012, Flashback's authors started making use of a Russian partner program that somehow injected redirect

scripts into legitimate Web sites. The researcher said tens of thousands of WordPress sites were infected in late February and early March and notes that other estimates had the number as high as 100,000 infected sites. It was unclear how the sites became infected, but the researcher believed bloggers were either using vulnerable versions of WordPress or installed the ToolsPack plugin.
Source: http://threatpost.com/en_us/blogs/analysis-flashback-spread-social-engineering-then-java-exploits-041912

44. *April 19, Security News Daily* – (International) **New Android malware spreads by text message.** Criminals targeting smartphones crafted a clever text-message-based attack that removes the middleman and delivers its malicious payload directly to its Android targets. The malware, identified by researchers at NQ Mobile as "UpdtBot," disguises its malicious intentions by appearing as a text message telling recipients "their systems is at risk and they need to install the latest system upgrade." It is a typical scareware tactic, tricking would-be victims into believing they need to fix their phone or computer to stave off imminent harm. However, UpdtBot takes the traditional scam a step further. While most Android malware uses text messages to communicate with an attack server or to sign the victim up for text-message subscription services, this text-based threat contains a link in the message; when the user clicks on the link contained in the text, he/she is taken to a site that automatically uploads the malware. From there, UpdtBot can make calls, send texts, download new apps, and install corrupt software onto infected Android phones. So far, the malware infected more than 160,000 Android devices, according to NQ Mobile.
Source: http://www.securitynewsdaily.com/1754-android-malware-text-messages.html

For more stories, see items **33** and **37**

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

45. *April 19, WLUC 6 Marquette* – (Michigan) **Cell service restored.** The phone outage in Schoolcraft County, Michigan, and a portion of Delta County has been fixed, WLUC 6 Marquette reported April 19. The fiber optic cable was damaged near Cooks. The Michigan State Police were asked to investigate the area, as the damages to the line led the repair crews to believe the cable may have been intentionally tampered with.
Source: http://www.uppermichiganssource.com/news/story.aspx?list=~\home\lists\search&id=744017#.T5FikdkwJI5

46. *April 19, Cerritos-Artesia Patch* – (California) **Thieves targeting amplifiers and connectors inside Charter Communication cable boxes in Cerritos.** A crime alert was issued April 19 in response to a spate of thefts targeting amplifiers and connectors found inside cable boxes belonging to Charter Communications in Cerritos, California, over the past few weeks. More than 1,000 of the gray or brown colored cable boxes, which are located along residential sidewalks and on arterial streets in parkways, are required to delivery digital cable signals to Charter customers. However, when the targeted parts are removed, cable service is interrupted. "We've had more than 20 stolen over the past 3 weeks," a Cerritos Sheriff's Station detective sergeant said. The thefts also appear to be occurring in close proximity to one another. Earlier the week of April 16, five cases were reported in residential neighborhoods. The detective sergeant said the amplifiers are worth between $300 to $600 a piece, and the connectors are valued at roughly $40. "Whoever is taking them knows exactly what they're doing because they're clean cut at the connector sites," the sergeant said, adding that these items are being stolen within minutes. When one of these items is tampered with or taken, cable service is immediately disrupted and an alert is sent to Charter.
Source: http://cerritos.patch.com/articles/cerritos-crime-alert-issued-for-flurry-of-charter-communication-cable-box-thefts-targeting-amplifiers-and-connectors

For another story, see item **44**

[Return to top]

Commercial Facilities Sector

47. *April 19, Los Angeles Times* – (California) **Car crashes into Valley dental office; three critically injured.** At least six people were injured April 19 when a car careened into a dental office in the Lake Balboa section of Los Angeles, leaving three people critically injured and two pinned by the vehicle, Los Angeles fire officials said.
Source: http://latimesblogs.latimes.com/lanow/2012/04/car-careens-into-dental-office-injurying-six-three-critical-1.html

48. *April 19, KTVX 4 Salt Lake City* – (Utah) **Refrigerant leak forces evacuations at Gateway Mall.** An evacuation was ordered April 18 at the Gateway Mall in Salt Lake City after a refrigerant leak was discovered at a restaurant. Employees noticed a gas plume near the restaurant's refrigeration unit and called the fire department. The restaurant and the nearby food court were evacuated. Crews discovered that it was a refrigerant leak and not a natural gas leak as originally believed. One employee and one security guard were taken to a hospital with minor respiratory issues. Officials said patrons would be allowed back inside once the restaurant is aired out.
Source: http://www.abc4.com/content/news/slc/story/Refrigerant-leak-forces-evacuations-at-Gateway/STgoD3iyU0-2wI_qIZc3Gw.cspx

49. *April 19, Stockton Record* – (California) **California three-alarm fire destroys three businesses.** A three-alarm fire April 19 destroyed three businesses in a strip mall in Stockton, California. The fire required nine fire engines and three fire trucks to control. Some 40 residents from a neighboring apartment complex were evacuated to a school

for shelter.
Source: http://www.firehouse.com/news/10703331/california-three-alarm-fire-destroys-three-businesses

50. *April 19, WAVE 3 Louisville* – (Kentucky) **Firefighters: Explosion due to marijuana drying operation.** An explosion at an apartment building in Louisville, Kentucky, April 19 was found to be caused by a marijuana drying operation. Firefighters said a resident was drying marijuana with butane cans. "At one point he piled too many clothes next to those cans and the flare caught the clothes on fire, causing this haze," a fire captain said. It was later confirmed the "haze" was burning marijuana, rather than fumes from a meth lab as first suspected. The building sustained damage, and the potential for structural damage meant residents could not return to their apartments.
Source: http://www.wave3.com/story/17584548/explosion-reported-at-apartment-building-near-butchertown

51. *April 19, WOOD 8 Grand Rapids* – (Michigan) **Pipe bomb explodes at apt. complex.** The FBI was among the agencies investigating a pipe bomb that exploded at the office of an apartment complex in Benton Harbor, Michigan, April 18. Benton Harbor police found what appeared to be fragments of a pipe bomb near the office window of the Cogic Village Apartments. The blast blew out the front office window. The explosion also blew fragments about 75 yards through the window of another apartment. No one was injured when that device went off. Police said the apartment was owned by the Church Of God In Christ. Authorities were not yet sure if this explosion was aimed at that organization.
Source: http://www.woodtv.com/dpp/news/local/sw_mich/pipe-bomb-explodes-in-benton-harbor

For another story, see item **5**

[Return to top]

National Monuments and Icons Sector

52. *April 19, KXAN 21 Austin* – (Texas) **Officials: Fires overwhelmed resources.** Emergency officials could have tripled the manpower devoted to battling the late summer wildfires in 2011 in Bastrop, Texas, and it still would not been enough to stem the devastation, a legislative panel was told April 19. "There's not enough resources in Texas to prevent something like this happening," said the chief of emergency management for the Texas Department of Public Safety in testimony before the state house agriculture committee. Two people died from the fires that began swirling over the 2011 Labor Day weekend. More than 34,000 acres of pine forest and ranch land was scorched, an estimated 1,670 homes were destroyed, and 5,000-plus people were uprooted from their homes. More than 1,000 firefighters from across Texas and beyond the state's borders assisted in the effort to stop the flames. The Texas Air National Guard dumped 1.4 million gallons of water on the flames, but it was of little use given the parched landscape and the buffeted winds. A major who commands the Texas National Guard, said the strained resources could be made worse the next

time. He said the federal government is considering moving the state's fleet of eight C-130 heavy transport planes used in disasters to Montana.
Source: http://www.kxan.com/dpp/news/local/bastrop/resources-were-no-match-for-bastrop-fire

For another story, see item **14**

[Return to top]

Dams Sector

Nothing to report

[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)387-2267
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer